

ABSTRACT

Systems and methods for a machine-learning driven fine-grained file access control approach are provided. According to one embodiment, a server associated with an enterprise network can obtain and store information regarding historical user behavior of users of the enterprise network by observing file access requests initiated by the users. The server receives a file access request initiated by a user, which relates to a file stored within the enterprise network in encrypted form. In response to receipt of the file access request, the server determines a risk score for the user based on multiple factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request so that based on the risk score, access to the file is permitted by returning a decryption key for the file or denied by withholding the decryption key.

CLAIMS:

What is claimed is:

1. A method comprising:

obtaining and storing, by one or more servers associated with an enterprise network, information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users;

receiving, by the one or more servers, a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the enterprise network in encrypted form;

responsive to receipt of the file access request, determining, by the one or more servers, a risk score for the first user based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request; and

based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key.

2. The method of claim 1, wherein said determining, by the one or more servers, a risk score for the first user comprises evaluating the file access request with reference to a model of user behavior developed by machine-learning.

3. The method of claim 1, wherein the information regarding historical user behavior includes for each user of the plurality of users:

historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time;

historical data regarding observed locations of the user; and

historical data regarding observed times at which the user accesses files.

4. The method of claim 1, wherein the observed data includes a current location of the first user as determined based on a source Internet Protocol (IP) address contained in the file access request.
5. The method of claim 1, wherein the observed data includes a status indicative of whether the connection through which the first user initiated the file access request is trusted or untrusted.
6. The method of claim 5, wherein the connection is trusted when the first user is on the enterprise network or accessing the enterprise network remotely via a secure connection.
7. The method of claim 5, wherein the connection is untrusted when the first user is not on the enterprise network or accessing the enterprise network remotely via an insecure connection.
8. The method of claim 1, wherein the encrypted form involves the file being encapsulated in a cryptographic wrapper.
9. The method of claim 1, wherein said permitting or denying further comprises when the risk score is less than a first threshold, returning the decryption key and providing full access to the file.
10. The method of claim 9, wherein said permitting or denying further comprises when the risk score is between the first threshold and a second threshold, returning the decryption key and providing limited access to the file.
11. The method of claim 10, wherein said permitting or denying further comprises when the risk score is greater than the second threshold, withholding the decryption key.

12. A non-transitory computer-readable storage medium embodying a set of instructions, which when executed by one or more processors of one or more servers associated with an enterprise network, causes the one or more processors to perform a method comprising:
- obtaining and storing information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users;
 - receiving a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the enterprise network in encrypted form;
 - responsive to receipt of the file access request, determining a risk score for the first user based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request; and
 - based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key.
13. The non-transitory computer-readable storage medium of claim 12, wherein said determining a risk score for the first user comprises evaluating the file access request with reference to a model of user behavior developed by machine-learning.
14. The non-transitory computer-readable storage medium claim 13, wherein the information regarding historical user behavior includes for each user of the plurality of users:
- historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time;
 - historical data regarding observed locations of the user; and
 - historical data regarding observed times at which the user accesses files.
15. The non-transitory computer-readable storage medium claim 13, wherein the observed data includes a current location of the first user as determined based on a source Internet Protocol (IP) address contained in the file access request.

16. The non-transitory computer-readable storage medium claim 13, wherein the observed data includes a status indicative of whether the connection through which the first user initiated the file access request is trusted or untrusted.
17. The non-transitory computer-readable storage medium claim 13, wherein the encrypted form involves the file being encapsulated in a cryptographic wrapper.
18. The non-transitory computer-readable storage medium claim 13, wherein said permitting or denying further comprises when the risk score is less than a first threshold, returning the decryption key and providing full access to the file.
19. The non-transitory computer-readable storage medium claim 18, wherein said permitting or denying further comprises when the risk score is between the first threshold and a second threshold, returning the decryption key and providing limited access to the file.
20. The non-transitory computer-readable storage medium claim 19, wherein said permitting or denying further comprises when the risk score is greater than the second threshold, withholding the decryption key.

Atty. Docket No.: FORT-031800
Fortinet Ref. No.: 18167

Patent Application

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

TITLE OF THE INVENTION

FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS

Inventors:

MATTHEW J. LITTLE, residing in:
Loanhead, Midlothian, Scotland
Mailing Address:
40 Torphichen Street
Edinburgh EH3 8JB
SCOTLAND

CARSON LEONARD, residing in:
Edinburg, Scotland
Mailing Address:
40 Torphichen Street
Edinburgh EH3 8JB
SCOTLAND

JAMIE R. GRAVES, residing in:
Edinburgh, Scotland
Mailing Address:
40 Torphichen Street
Edinburgh EH3 8JB
SCOTLAND

MILES GOULD, residing in:
Edinburgh, Scotland
Mailing Address:
40 Torphichen Street
Edinburgh EH3 8JB
SCOTLAND

Assignee: **FORTINET, INC.**
A Delaware Corporation

Entity: Regular Undiscounted

FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS

COPYRIGHT NOTICE

[0001] Contained herein is material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction of the patent disclosure by any person as it appears in the Patent and Trademark Office patent files or records, but otherwise reserves all rights to the copyright whatsoever. Copyright © 2019, Fortinet, Inc.

BACKGROUND

Field

[0002] Embodiments of the present invention generally relate to network security. In particular, embodiments of the present invention relate to an improved file access approach that provides access to an electronic file based on a machine-learning driven file access control mechanism including placing a cryptographic wrapper around the file to prevent access to data without performing an on-access validation of a user's rights to access the file and additionally calculating the current risk level of the user attempting to access the file based on their current and historical behavior, thereby facilitating fine-grained and dynamic access control to be applied to the user accessing the data.

Description of the Related Art

[0003] The rapid increase in implementation of network-based storage architectures have led to substantial concerns in the arena of network and information security. Major concerns relate to ensuring authentication, access control, and security of the stored data. One of the most widely used approaches to protect data within a network-based storage architecture is the use of encryption; however, encryption alone is insufficient as there are many known methods of circumventing encryption. For example, the data can be accessed by, among other things, finding an existing copy of the decryption key or a password, passcode or passphrase used to create the decryption key. See Kerr, Orin and Schneier, Bruce, *Encryption Workarounds*, 106 Georgetown L.J. 989 (2018).

[0004] Current file access control systems suffer from two key problems – either data is unprotected and individuals who have been given access once to a file are, effectively, granted

access in perpetuity or access is granted for a finite period of time (e.g., during employment with a particular organization) but this mechanism is policy-driven. Policy-driven approaches require all potential user behaviors of all users within the organization to be modeled and pre-calculated and policies to be correctly developed from the predicted behaviors (e.g., user access scenarios in terms of, among other things, the time of day, the location of the user, and/or privileges associated with the user and/or a user group with which the user is associated).

[0005] Policy-driven approaches have additional limitations, including the inherent inflexible nature of predefined rules and the requirement for constant configuration and management – typically by a network administrator – when circumstances change. For example, if an employee of an organization is granted access to sensitive company data, when that employee leaves the organization, his/her access must be revoked by altering the file access control policy. Similarly, when a employee joins the organization, policies must be added for the new employee. Therefore, the organization is burdened with the overhead and potential error prone process of adding, updating, and/or deleting numerous file access control policies the complexity of which increases as the number of employees grows, as the potential user access scenarios grow, as finer-grained levels of access are defined and as the number of employees grows.

[0006] In view of the foregoing technological limitations of policy-driven file access control approaches, there is a need for a more effective file access control mechanism.

SUMMARY

[0007] Systems and methods are described for a machine-learning driven fine-grained file access control approach. According to one embodiment, a server associated with an enterprise network can obtain and store information regarding historical user behavior of users of the enterprise network by observing file access requests initiated by the users. The server receives a file access request initiated by a user, which relates to a file stored within the enterprise network in encrypted form. In response to receipt of the file access request, the server determines a risk score for the user based on multiple factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request so that based on the risk score, access to the file is permitted by returning a decryption key for the file or denied by withholding the decryption key.

[0008] Other features of embodiments of the present disclosure will be apparent from accompanying drawings and detailed description that follows.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] In the Figures, similar components and/or features may have the same reference label. Further, various components of the same type may be distinguished by following the reference label with a second label that distinguishes among the similar components. If only the first reference label is used in the specification, the description is applicable to any one of the similar components having the same first reference label irrespective of the second reference label.

[00010] FIG. 1 is a simplified network architecture in which aspects of the present invention can be implemented in accordance with an embodiment of the present invention.

[00011] FIG. 2 illustrates an exemplary representation of functional components of a management server in accordance with an embodiment of the present invention.

[00012] FIG. 3A is a high-level flow diagram illustrating a portion of a file access control process in accordance with an embodiment of the present invention.

[00013] FIG. 3B is a flow diagram illustrating a user risk rating evaluation process in accordance with an embodiment of the present invention.

[00014] FIG. 4 is a sequence diagram illustrating interactions among various components of a network architecture in connection with a file access request in accordance with an embodiment of the present invention.

[00015] FIG. 5 illustrates an exemplary computer system in which or with which embodiments of the present invention may be utilized.

DETAILED DESCRIPTION

[00017] Systems and methods are described for a machine-learning driven fine-grained file access control approach. As noted above, current file access control systems suffer from two key problems – either data is unprotected and individuals who have been given access once to a file are, effectively, granted access in perpetuity or access is granted for a short period of time in accordance with a policy-driven approach that does not take into account the measured risk of a user's behavior. The policy-driven approach requires all potential user behaviors to be modelled and pre-calculated and policies to be correctly developed from these predicted behaviors. As described herein, a more effective method to protect data is to use measured (rather than modelled) user behavior to determine whether access should be granted to data.

[00018] According to embodiments of the present invention, the use of cryptographic wrappers encapsulating files to prevent access to data without an on-access validation of a user's rights to access the file is combined with a near real-time calculation of the current risk level of a user based on their current and historical behavior, thereby facilitating fine-grained and dynamic access control to be applied to the user attempting to access the data. An advantage of this approach is that risk is calculated in near real-time and the required access control determination for a specific file access can be made specific to a variety of factors which are used to calculate the risk of granting the requesting user access to the file in question.

[00019] In the following description, numerous specific details are set forth in order to provide a thorough understanding of embodiments of the present invention. It will be apparent to one skilled in the art that embodiments of the present invention may be practiced without some of these specific details.

[00020] Embodiments of the present invention include various steps, which will be described below. The steps may be performed by hardware components or may be embodied in machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor programmed with the instructions to perform the steps. Alternatively, steps may be performed by a combination of hardware, software, firmware and/or by human operators.

[00021] Embodiments of the present invention may be provided as a computer program product, which may include a machine-readable storage medium tangibly embodying thereon instructions, which may be used to program a computer (or other electronic devices) to perform a process. The machine-readable medium may include, but is not limited to, fixed (hard) drives,

magnetic tape, floppy diskettes, optical disks, compact disc read-only memories (CD-ROMs), and magneto-optical disks, semiconductor memories, such as ROMs, PROMs, random access memories (RAMs), programmable read-only memories (PROMs), erasable PROMs (EPROMs), electrically erasable PROMs (EEPROMs), flash memory, magnetic or optical cards, or other type of media/machine-readable medium suitable for storing electronic instructions (e.g., computer programming code, such as software or firmware).

[00022] Various methods described herein may be practiced by combining one or more machine-readable storage media containing the code according to the present invention with appropriate standard computer hardware to execute the code contained therein. An apparatus for practicing various embodiments of the present invention may involve one or more computers (or one or more processors within a single computer) and storage systems containing or having network access to computer program(s) coded in accordance with various methods described herein, and the method steps of the invention could be accomplished by modules, routines, subroutines, or subparts of a computer program product.

[00023] While embodiments of the present invention have been illustrated and described, it will be clear that the invention is not limited to these embodiments only. Numerous modifications, changes, variations, substitutions, and equivalents will be apparent to those skilled in the art, without departing from the spirit and scope of the invention, as described in the claims. For example, although embodiments of the present invention are described herein with reference to protecting access to a particular type of enterprise network resource, i.e., files, the methodologies described herein are thought to be applicable to enterprise network resources more generally (e.g., network resource or shared resource accessible via an enterprise network, such as defined portions of a storage device (e.g., a network share or a directory within a file system), databases, applications, and printers), albeit, without the use of a cryptographic wrapper as in the case of files.

Terminology

[00024] Brief definitions of terms used throughout this application are given below.

[00025] The phrase “endpoint device” generally refers to a network-capable computer hardware device, typically on a Transmission Control Protocol (TCP)/Internet Protocol (IP)

network. Non-limiting examples of endpoint devices include desktop computers, laptops, smart phones, tablets, thin clients, and Internet of Things (IoT) devices.

[00026] The phrase “endpoint protection system” generally refers a system that (i) focuses on protecting endpoint devices in a network from cyber threats and attacks by malicious internal and external threats, (ii) provides endpoint management functionality, for example, allowing a network administrator to identify and manage the users’ computers access over a corporate or enterprise network and/or (iii) protects the enterprise network by blocking access attempts and/or other risky activity at these points of entry to the enterprise network. An endpoint protection system may proactively defend endpoints with one or more of pattern-based anti-malware technology, behavior-based exploit protection, web-filtering, and an application firewall. For example, a network administrator may configure the endpoint protection system to restrict certain website access to specific users in order to maintain and comply with an organization’s policies and standards. Similarly, an endpoint protection system may provide antivirus/antimalware, sandbox protection and/or vulnerability management scanning and may additionally be configurable to remediate identified issues and/or automatically quarantine a suspicious or compromised endpoint in order to contain incidents and stem outbreaks. Non-limiting examples of endpoint protection systems include the FortiClient endpoint security solution (available from the assignee of the present invention), Cybereason, Sentinel. One endpoint security software, Stormshield SES, ForeScout CounterAct, Promisec PEM, CounterTack Sentinel, CrowdStrike Falcon Host, Guidance Software Encase, and Comodo Advanced Endpoint Protection.

[00027] The terms “connected” or “coupled” and related terms are used in an operational sense and are not necessarily limited to a direct connection or coupling. Thus, for example, two devices may be coupled directly, or via one or more intermediary media or devices. As another example, devices may be coupled in such a way that information can be passed there between, while not sharing any physical connection with one another. Based on the disclosure provided herein, one of ordinary skill in the art will appreciate a variety of ways in which connection or coupling exists in accordance with the aforementioned definition.

[00028] If the specification states a component or feature “may”, “can”, “could”, or “might” be included or have a characteristic, that particular component or feature is not required to be included or have the characteristic.

[00029] As used in the description herein and throughout the claims that follow, the meaning of “a,” “an,” and “the” includes plural reference unless the context clearly dictates otherwise. Also, as used in the description herein, the meaning of “in” includes “in” and “on” unless the context clearly dictates otherwise.

[00030] The phrases “in an embodiment,” “according to one embodiment,” and the like generally mean the particular feature, structure, or characteristic following the phrase is included in at least one embodiment of the present disclosure, and may be included in more than one embodiment of the present disclosure. Importantly, such phrases do not necessarily refer to the same embodiment.

[00031] Exemplary embodiments will now be described more fully hereinafter with reference to the accompanying drawings, in which exemplary embodiments are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. These embodiments are provided so that this invention will be thorough and complete and will fully convey the scope of the invention to those of ordinary skill in the art. Moreover, all statements herein reciting embodiments of the invention, as well as specific examples thereof, are intended to encompass both structural and functional equivalents thereof. Additionally, it is intended that such equivalents include both currently known equivalents as well as equivalents developed in the future (i.e., any elements developed that perform the same function, regardless of structure).

[00032] Thus, for example, it will be appreciated by those of ordinary skill in the art that the diagrams, schematics, illustrations, and the like represent conceptual views or processes illustrating systems and methods embodying this invention. The functions of the various elements shown in the figures may be provided through the use of dedicated hardware as well as hardware capable of executing associated software. Similarly, any switches shown in the figures are conceptual only. Their function may be carried out through the operation of program logic, through dedicated logic, through the interaction of program control and dedicated logic, or even manually, the particular technique being selectable by the entity implementing this invention. Those of ordinary skill in the art further understand that the exemplary hardware, software, processes, methods, and/or operating systems described herein are for illustrative purposes and, thus, are not intended to be limited to any particular named.

[00033] According to various embodiments of the present disclosure, files of an enterprise network are encapsulated in a cryptographic wrapper, which protects the files by preventing direct access by users who do not have associated cryptographic keys. When a user attempts to access a file, an access request is made to a server. The server analyzes various factors using a model of user behavior developed by machine-learning techniques to identify whether the access request at issue represents abnormal behavior (that is, represents an outlier with respect to a reference dataset) and quantifies the degree of abnormality in terms of a risk score. Further discussion regarding the collection of user behavior, although, from an endpoint device and in the context of identifying a user masquerading as another user is described in US Pub. Nos. 2018/0069881 and 2018/0351979, both of which are hereby incorporated by reference for all purposes.

[00034] In one embodiment, the various factors analyzed/evaluated by the server include information regarding historical behavior of the user, the file access request at issue and observed data associated with the file access request at issue to determine a risk score. Exemplary factors can include, but are not limited to, history of general file access by the user, current location of the user, history of location of the user, time of access request, time when the user typically accesses a file, whether the user is accessing from a trusted location or an untrusted location, behavior of the user's peer group as determined by either a list obtained from a directory services server or as measured by behavior of multiple users associated with the enterprise (where users with similar behavior may be deemed to be a part of the same group). On determination of the risk score, the server that maintains the decryption key of the requested file can provide or deny the access. For example, when the risk score is low, the user can be provided the decryption key to permit access; when the risk score is moderate, the user can be directed to access the file through a lower risk channel, e.g., a virtual private network (VPN); and when the risk score is high, the user can be blocked from accessing the file.

[00035] FIG. 1 is a simplified network architecture 100 in which aspects of the present invention can be implemented in accordance with an embodiment of the present invention. In the context of the present example, an improved file access approach is provided by using one or more servers, e.g., a management server 102, a permission server 104 and an analytics server 106. In an implementation, permission server 104 and analytics server 106 can be separate servers operatively coupled with management server 102, whereas, in an alternate embodiment, permission server 104 and analytics server 106 can be representative of functionality that is integrated within

management server 102. In one embodiment, the servers reside within an enterprise network 108 (which may be referred to simply as network 108 hereinafter). Further, client machines 110-1, 110-2 .. 110-N (which may be collectively referred to herein as client machines 110 and may be individually referred to herein as client machine 110) associated with network 108 represent endpoint devices through which users of the enterprise access various resources associated with network 108. Client machines 110 may include, but are not limited to, personal computers, smart devices, web-enabled devices, hand-held devices, laptops, mobile phones and the like and generally allow users to interact with network 108 as well as external resources associated with the Internet, for example.

[00036] Those skilled in the art will appreciate that, network 108 can include one or more wireless networks, wired networks or a combination thereof that can be implemented as one of the different types of networks, such as Intranet, Local Area Network (LAN), Wide Area Network (WAN), Internet, and the like. Further, network 108 can either be a dedicated network or a shared network, representing an association of the different types of networks that use a variety of protocols, for example, Hypertext Transfer Protocol (HTTP), Transmission Control Protocol/Internet Protocol (TCP/IP), Wireless Application Protocol (WAP), and the like.

[00037] In one embodiment, client machines 110 have installed thereon a file access control module (not shown) that intercepts or “hooks” certain system Application Programming Interface (API) calls in order to perform on-access validation of a user’s rights to access a file. In one embodiment, the file access control module runs in kernel mode and hooks low level operating system APIs to intercept various OS operations, such as file system input/output (I/O) activity. In this manner, the file access control module may perform appropriate user validation processing prior to performing the requested file access operation (e.g., delete, open, read, write, and/or rename) on the file. According to one embodiment, the file access control module may be integrated within an endpoint protection system installed on client machines 110. As described further below, in one embodiment, decryption keys for encrypted files stored within the enterprise network may be managed by a server associated with the enterprise network. In such an embodiment, the decryption key for a file is either returned or not responsive to the on-access validation of the file access request for the file. When the key is returned, the on-access validation process has authorized the requested file access and the file access control module uses the key to perform the requested file operation on the file. When the key is not returned, the on-access

validation process has denied the requested file access and the file access control module may forego performance of the requested file operation (whether or not the decryption key is required for the file operation at issue) on the file and may additionally cause the user to be notified regarding the fact that access to the file has been denied.

[00038] According to an embodiment, management server 102 serves as an interface between a file access control module running on client machines 110 and permission server 104 and analytics server 106. For example, management server 102 may manage a validation process for a file access request received from a file access control module running on a particular client machine 110 that initiated the file access request at issue. In one embodiment, management server 102 may first communicate information regarding the file access request to analytics server 106 to obtain a risk score for the user that initiated the request. Upon receiving the risk score, management server 102 may then request the decryption key for the file at issue from permission server 104 based on the risk score. If permission server 104 provides the requested decryption key, management server 102 returns it to the requesting file access control module; otherwise, management server 102 notifies the requesting file access control module that the file access request has been denied.

[00039] In one embodiment, management server 102 can obtain and store information regarding historical user behavior of users of network 108 by observing file access requests initiated by the users via their respective client machines 110. Alternatively, such information may be stored and processed by analytics server 106. For each user, the information regarding historical user behavior can include:

- Historical data regarding general file access, including one or more of:
 - A number of files accessed by the user over a predetermined or configurable time period,
 - Types of the files accessed over the time period, and
 - Applications used by the user over the time period;
- Current location of the user (as determined by the IP address of the client machine that initiated the file access request or by other means)
- Historical data regarding observed locations of the user;

- Time of day (local) where the file is requested; and/or
- Historical data regarding observed times at which the user typically accesses files.
- Whether the user is accessing data form a “trusted location” (e.g., via the corporate network or via a VPN) or from an “untrusted location” (e.g., via a public Internet hotspot)

[00040] In an embodiment, permission server 104 can receive information associated with a file access request initiated by a user, which can relate to a file stored within network 108 in encrypted form, for example, encapsulated in a cryptographic wrapper. In response to receipt of the file access request, analytics server 106 can determine a risk score for the user based on multiple factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request. The observed data can include a current location of user as determined based on a source IP address contained in the file access request and a status indicative of whether the connection through which the user initiated the file access request is trusted or untrusted. The connection can be trusted when the user is on network 108 or accessing network 108 remotely via a secure connection, while the connection can be untrusted when the user is not on network 108 or accessing network remotely 108 via an insecure connection.

[00041] In one embodiment, analytics server 106 applies machine learning techniques to the information regarding historical user behavior and the file access request at issue to determine a measure of abnormality or deviation from normal user behavior, which is referred to herein at times as a risk score. The machine learning algorithm employed by analytics server 106 may operate by building a model of user behavior. The model of user behavior may be formed in dependence on reference data (e.g., an example training set of input observations within the network environment at issue over a period of time). The model of user behavior may be formed in an unsupervised manner or may involve supervised learning with feedback. The model of user behavior may comprise a model of normal behavior, i.e., behavior which is not of a suspect nature, in dependence on normal reference data which reflects normal behavior of the users of the network environment at issue. The model of behavior may be formed in dependence on reference data collected relating to observed file access requests the network environment at issue and may be

updated based on ongoing observations regarding file access requests in the network environment at issue. The machine learning algorithm may comprise a clustering algorithm which is operative to perform clustering of the reference data.

[00042] As described further below a risk score calculation algorithm (e.g., a modified outlier detection algorithm) may be configured to apply a file access request at issue (including any optional observed data associated therewith) to the model of user behavior and to determine whether or not the file access request is in accordance with the model. If the file access request is outside of that represented within the model, then a degree to which it deviates from the model behavior, which may be expressed as a risk score, may be calculated. Where the model of user behavior comprises multiple sub-models, the risk score calculation algorithm may be operative to apply the file access request to an appropriate sub-model in dependence on an identifier associated with the file access request, such as a user identifier, the name or type of the file, or an IP address. Where the model is formed in dependence on normal reference data, the file access request not being in accordance with the model may be indicative of the file access request reflecting suspect behavior. For example, where the machine learning technique comprises a clustering algorithm the risk score calculation algorithm may be operative to determine whether or not the file access falls within the scope of at least one cluster formed by the clustering algorithm. Where the file access request is not in accordance with the model, the risk score calculation algorithm may be configured to output score representing a measure of deviation from normal user behavior.

[00043] The ongoing collection and analysis of user behavior within the network environment at issue may further comprise modifying the model in dependence on observed file access requests initiated by users for files associated with the network environment. The model may thus be modified in a supervised manner. More specifically the model may be modified in dependence on alerts provided to the network administrator responsive to denying file access requests, for example. It may be advantageous to have the network administrator periodically assess whether or not the file access requests that triggered alerts actually represent suspect behavior and provide for modification of the model in dependence on the network administrator's assessment.

[00044] The ongoing collection and analysis of user behavior may therefore provide for modification of the model by way of an input-output arrangement comprised in management server 102, permission server 104 and/or analytics server 106. More specifically the ongoing collection

and analysis of user behavior and/or the denial of access based on a risk score calculated based on the model of user behavior may further include prompting the network administrator by way of the input-output arrangement to modify the model. For example a message, alert or notification may be provided to the network administrator, such as on a visual display unit or an event log, and the user may be afforded an opportunity to re-classify file access requests identified as reflecting abnormal user behavior as relating to normal user behavior by way of a user operable part of the input-output arrangement such as a clickable area on the visual display unit.

[00045] The model formed by the risk score calculation algorithm may comprise multiple sub-models. Each sub-model may be separately formed from a different form of reference data. More specifically each sub-model may be formed from reference data relating to one or more of: a different file, a different type of file, a different user, a different IP address, a different location, a different timeframe.

[00046] The risk score calculation approach may comprise performing analysis in dependence on the file access request and more specifically upon application of the file access request (and associated observed data) to the model of user behavior. The analysis may provide for at least one determination to be made in respect of the nature of the suspect behavior. Analysis may determine, for example, that a file access request of the same form as the reference data, for example a file access request for the same file and by the same user, exhibits different behavior to the reference data. This may reflect the user account at issue has been compromised and is being used by someone other than the user. Alternatively, analysis may determine that a file access request fails to match or is insufficiently close to the reference data of any form in the model. This may reflect the presence of malware or may reflect the presence of an unauthorized user or an authorized user behaving in an inappropriate fashion.

[00047] In an embodiment, based on the risk score, permission server 104 can permit or deny access to the file by returning a decryption key for the file or by withholding the decryption key. In one embodiment, when the risk score is less than a first threshold, permission server 104 can return the decryption key to client machine 110 and provide full access to the file; when the risk score is between the first threshold and a second threshold, permission server 104 can return the decryption key to the client machine and provide limited access to the file; and when the risk score is greater than the second threshold, permission server 104 can withhold the decryption key.

Alternatively, there may simply be one threshold risk level. For example, when the risk score is less than or equal to the threshold risk level, full access to the file is permitted by returning the decryption key to the file access control module and when the risk score is greater than the threshold risk level, access is denied by withholding the decryption key. In addition to permitting or denying a file access request, permission server 104 may also responsive to denying the request providing an output (e.g., an alert or notification to the network administrator) indicating the detection of abnormal/suspect behavior. The output may comprise a human perceptible indication that suspect behavior has been performed by a particular user. Providing an output may comprise at least one of: operation of an output device, such as providing a message on a video display unit comprised in management server 102, permission server 104 or analytics server 106.

[00048] FIG. 2 illustrates an exemplary representation 200 of functional components of a management server 102 in accordance with an embodiment of the present invention. As illustrated, management server 102 can include one or more processor(s) 202. Processor(s) 202 can be implemented as one or more microprocessors, microcomputers, microcontrollers, digital signal processors, central processing units, logic circuitries, and/or any devices that manipulate data based on operational instructions. Among other capabilities, processor(s) 202 are configured to fetch and execute computer-readable instructions stored in a memory 206 of management server 102. Memory 206 can store one or more computer-readable instructions or routines, which may be fetched and executed to create or share the data units over a network service. Memory 206 can include any non-transitory storage device including, for example, volatile memory such as RAM, or non-volatile memory such as EPROM, flash memory, and the like. In an example embodiment, memory 206 may be a local memory or may be located remotely, such as a server, a file server, a data server, and the Cloud.

[00049] Management server 102 can also include one or more interface(s) 204. Interface(s) 204 may include a variety of interfaces, for example, interfaces for data input and output devices, referred to as I/O devices, storage devices, and the like. Interface(s) 204 may facilitate communication of management server 102 with various devices coupled to management server 102. Interface(s) 204 may also provide a communication pathway for one or more components of management server 102 and/or facilitate interaction with the network administrator. Examples of such components include, but are not limited to, processing engine(s) 208 and database 216.

[00050] Processing engine(s) 208 can be implemented as a combination of hardware and software or firmware programming (for example, programmable instructions) to implement one or more functionalities of engine(s) 208. In the examples described herein, such combinations of hardware and software or firmware programming may be implemented in several different ways. For example, the programming for the engine(s) may be processor executable instructions stored on a non-transitory machine-readable storage medium and the hardware for engine(s) 208 may include a processing resource (for example, one or more processors), to execute such instructions. In the examples, the machine-readable storage medium may store instructions that, when executed by the processing resource, implement engine(s) 208. In such examples, management server 102 can include the machine-readable storage medium storing the instructions and the processing resource to execute the instructions, or the machine-readable storage medium may be separate but accessible to management server 102 and the processing resource. In other examples, processing engine(s) 208 may be implemented by electronic circuitry. Database 216 can include data that is either stored or generated as a result of functionalities implemented by any of the components of processing engine(s) 208.

[00051] In an example, processing engine(s) 208 can include a permission engine 210, an analytics engine 212 and other engine(s) 214. Other engine(s) 214 can implement functionalities that supplement applications or functions performed by management server 102 or processing engine(s) 208.

[00052] In an aspect, information regarding historical user behavior of users of an enterprise network can be collected and stored in database 216 by observing file access requests initiated by the users. In an example, the file access requests can be initiated by the users using client machines and can include or be supplemented to include information such as an IP address and geographical location of the access, time of the access, a user identifier of the accessor or user, the name of the file attempting to be accessed, and the likes.

[00053] According to an example, for each user, the information regarding historical user behavior can include historical data regarding general file access which includes one or more of a number of files accessed by the user over a predetermined period of time, types of files accessed, and applications used by the user over the predetermined period of time. The information regarding historical user behavior can further include historical data regarding observed locations of the user,

as can be determined by the IP address of client machine or network device, and historical data regarding observed times at which the user accesses files, e.g., times when the file is requested, times when the user typically accesses a file, etc.

[00054] In an aspect, permission engine 210 can receive a file access request initiated by a user, which can relate to a file stored within the enterprise network in encrypted form. The encrypted form can include the file being wrapped within a cryptographic wrapper in order to prevent direct access to the file without a proper on-access validation process having been performed by the file access control module, involving validating the file access request by the file access control module via management server 102 (or one or more of management server 102, permission server 104 and analytics server 106) explicit permission is provided for authenticated access. Cryptographic keys can be stored in database 216 and can be provided by permission engine 210 for authenticated access by the user.

[00055] In response to receipt of the file access request, analytics engine 212 can determine a risk score for the user based on multiple factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request. For example, the analytics engine 212 can compare the observed data with the historical information of user behavior to determine the risk score so that the risk score can be provided to the permission engine 210. As described above, analytics engine 212 may perform the comparison by analyzes various factors using a model of user behavior developed by machine-learning techniques to identify whether the access request at issue represents abnormal behavior (that is, represents an outlier with respect to a reference dataset, such as a model of normal user behavior) and may also quantify the degree of abnormality in terms of a risk score.

[00056] According to an example, the observed data can include a current location of the user as determined based on an IP address contained in the file access request and a status indicative of whether the connection through which the user initiated the file access request is trusted or untrusted. The connection can be deemed trusted when the user is on the enterprise network or accessing the enterprise network remotely via a secure connection, e.g., via a VPN. On contrary, the connection can be deemed untrusted when the user is not on the enterprise network or accessing the enterprise network remotely via an insecure connection, e.g., a public internet hotspot.

[00057] In an aspect, based on the risk score, permission engine 210 can permit or deny access to the file by returning a decryption key for the file or by withholding the decryption key. For example, when the risk score is less than a first threshold, i.e., when the risk score is low, permission engine 210 can return the decryption key and provide full access to the file. Further, when the risk score is between the first threshold and a second threshold, i.e., when the risk score is moderate, permission engine 210 can return the decryption key and provide limited access to the file, thereby directing access to the file through a lower risk channel, e.g. a VPN. Furthermore, when the risk score is greater than the second threshold, i.e., when the risk score is high, permission engine 210 can withhold the decryption key, thereby blocking access to the file. In an implementation, the first threshold, the second threshold and the third threshold can be maintained by permission engine 210 and may be configurable by a network administrator via a browser based interface provided, for example, by management server 102. In addition to blocking access to the file, permission engine 210 may also generate an alert or notification to the network administrator regarding the detected abnormal user behavior to solicit feedback from the network administrator. In this manner, the ongoing collection and analysis of user behavior within the network environment at issue may further comprise modifying the model in dependence on observed file access requests initiated by users for files associated with the network environment and based on feedback received from the network administrator (e.g., confirming or overriding the abnormal user behavior determination regarding the file access request at issue), thus modifying the model in a supervised manner.

[00058] Those skilled in the art will appreciate that using various embodiments of the present disclosure, when any unusual or anomalous activity of the user is observed while accessing a file, the management server 102 can block the access or can provide limited access based on the risk associated with the activity. For example, if the user is accessing a file at 3:00 a.m. through a network other than the enterprise network, based on the historical user behavior, the activity can be determined to be highly risky and the user may not be provided the cryptographic key to access the file. Alternatively, when the user accesses the file during working hours using the enterprise network, the activity can be viewed as relatively normal and be assigned a low risk score and the user may be provided the cryptographic key associated with the file for full access by the user. A network administrator can simply configure permission server 104 or permission engine 210 with a rule defining under what conditions a requested decryption key is to be provided. For example,

the rule may specify the requested decryption key is to be provided when the risk score is less than or equal to a predefined or configurable threshold and withheld otherwise. Advantageously in the manner, the network administrator need not contemplate all possible user access scenarios and define policies for each of such scenarios as would be required by a policy-driven file access control approach. When defining the predefined or configurable threshold, the network administrator may take into consideration the fact that user behaviors vary in different environments. For example, in a more rigid or regimented environment, such as a private network of a bank or of a defense contractor, even a slight deviation from normal user behavior may not be tolerable and therefore the network administrator in such an environment may require user risk scores to meet a lower risk threshold in order for their file access requests to be granted. In contrast, in a more flexible environment, such as a private network of a game developer, a relatively high degree of deviation from normal user behavior may be acceptable and therefore the network administrator of such an environment may permit user risk scores to meet a higher risk threshold and still authorize their file access requests. In this manner, a fine-grained and dynamic file access control mechanism is provided that overcomes various disadvantages and limitations of typical policy-based file access control approaches.

[00059] FIG. 3A is a high-level flow diagram 300 illustrating a portion of a file access control process in accordance with an embodiment of the present invention. In the present example, it is assumed a user has initiated, via a client machine on which a file access control module is installed, a file access request relating to a file stored within an enterprise network in encrypted form. . The file access control module has intercepted the file access request and initiates performance of an on-access validation process to seek confirmation or denial of the user's rights to perform the requested file access request (e.g., perform a file operation, such as delete, open, read, write, and/or rename) on the file.

[00060] In context of the present example, information regarding historical user behavior of the users of an enterprise network can be stored in a database associated with the enterprise network by observing file access requests initiated by the users. At block 302, a permission server can receive a file access request for validation. The file access request may represent the file access request in its original form as initiated by the user or it may represent an augmented version thereof. For example, in one embodiment, an IP address contained within the original file access

request may be replaced with information regarding a geographic location associated with the IP address. Additionally, as noted above, the original file access request might be augmented to include, for example, status information indicative of whether the connection through which the user initiated the file access request is trusted or untrusted. In an example, the file can be stored in a separate server, say a file server associated with the enterprise network. In another example, the file can be stored in any network or computing device associated with the enterprise network.

[00061] In response to receipt of the file access request, at block 304, behavior analytics functionality (e.g., implemented in analytics server 106 or analytics engine 212) can determine a risk score for the user based on multiple factors, including, but not limited to information regarding historical user behavior, the file access request and observed data determined based on the file access request. The observed data can include current location of the user as determined by the IP address, a time at which the file access was requested, and information regarding whether the user is accessing the file from a trusted location or an untrusted location.

[00062] In an aspect, the analytics server can provide the risk score to the permission server, such that based on the risk score and one or more configured risk thresholds, at block 306, the permission server can cause the file access control module of the client machine to permit access to the file by returning a decryption key for the file or can cause the file access control module of the client machine to deny access to the file by withholding the decryption key.

[00063] FIG. 3B is a flow diagram 350 illustrating a user risk rating evaluation process in accordance with an embodiment of the present invention. In the context of the present example, access to the requested file can be provided by permission functionality (e.g., implemented in permission server 104 or permission engine 210) based on the risk score determined by the behavior analytics functionality by comparing the risk score with one or more risk threshold values (e.g., a first, a second and a third threshold value in this example). The threshold values can be predetermined, pre-configured or configurable by a network administrator via a command line interface or graphical user interface provided by the permission server or by the management server.

[00064] At block 352, the risk score can be compared with the first threshold value. If the risk score is less than the first threshold, at block 360, the permission server can provide full access to the file by returning the decryption key. However, if the risk score is greater than the first threshold,

at block 354, the risk score can be compared with the second threshold value. If the risk score is between first threshold value and the second threshold value, at block 362, the permission server can provide limited access to the file by returning the decryption key and specifying the limitations. If the risk score is not between the first threshold value and the second threshold value, that is, at block 356, if the risk score is greater than the second threshold value, at block 358, the permission server can block access to the file by withholding the decryption key.

[00065] FIG. 4 is a sequence diagram 400 illustrating interactions among various components of a network architecture in connection with a file access request in accordance with an embodiment of the present invention. In context of the present example, a file access request can be initiated by a user through a client machine 402 such that at step 1, the access request can be sent to a permission server 404 for validation. As noted above, the access request can pertain to a file stored with an enterprise network in encrypted form and can include an IP address (and/or geographical location information associated with the IP address) of the client machine from which the file access request originated, a time of the access, a user identifier of the user that initiated the file access request, a name of the file to be accessed, etc. At step 2, permission server 404 can send the access request to an analytics server 406 for processing.

[00066] At step 3, analytics server 406 can capture user behavior relating to the current file access request and incorporate that information into historical user behavior information maintained by analytics server 406, including historical data regarding general file accesses by the user, historical data regarding observed locations of the user when making such file access requests, and historical data regarding observed times at which the user typically accesses files. At step 4, analytics server 406, can determine a risk score associated with the user based on the historical user behavior information, the file access request and optional additional observed data determined based on the file access request. Upon determining the risk score by analytics server 406, at step 5, the risk score can be returned to permission server 404. As noted above, the ongoing collection and analysis of user behavior within the network environment at issue (e.g., step 3) may further comprise modifying the model in dependence on observed file access requests initiated by users for files associated with the network environment.

[00067] At step 6, permission server 404 can compare the risk score with one or more threshold values, for example, the first, second and third threshold values described above with

reference to FIG. 3B and permit the level of file access associated with the comparison results. For example, when the risk score is less than or equal to a particular risk threshold, a file access control rule defined by the network administrator may specify any requested file access is to be allowed. Alternatively, when the risk score is greater than the particular risk threshold, the file access control rule may specify any requested file access is to be blocked/denied. At step 7, the access right and/or the decryption key can be provided to client machine 402. In an example, when the risk score is low, indicating, for example, a low deviation from normal user behavior, full access can be provided to the file at issue; when the risk score is moderate, indicating, for example, a moderate deviation from normal user behavior, limited access can be provided to the file at issue and when the risk score is high, indicating, for example, a high deviation from normal user behavior, access to the file at issue can be blocked by withholding the decryption key.

[00068] As noted above, the denial of a file access request by permission server 404 based on a risk score indicative of abnormal user behavior may further include logging the denial or otherwise notifying the network administrator so as to provide the network administrator with an opportunity to provide feedback to the machine-learning algorithm by reclassifying file access requests identified as reflecting abnormal user behavior as relating to normal user behavior. In this manner, the model of user behavior can be modified so as to produce more accurate risk score outputs over time based on feedback provided by the network administrator.

[00069] FIG. 5 illustrates an exemplary computer system 500 in which or with which embodiments of the present invention may be utilized. Computer system 500 may represent a client machine (e.g., client machine 110 or client machine 402) or a server (e.g., management server 102, permission server 104 or analytics server 106).

[00070] As shown in FIG. 5, computer system includes an external storage device 510, a bus 520, a main memory 530, a read only memory 540, a mass storage device 550, a communication port 560, and a processor 570. Computer system may represent some portion of management server 102, management server 104 or analytics server 106.

[00071] Those skilled in the art will appreciate that computer system 500 may include more than one processor 570 and communication ports 560. Examples of processor 570 include, but are not limited to, an Intel® Itanium® or Itanium 2 processor(s), or AMD® Opteron® or Athlon MP® processor(s), Motorola® lines of processors, FortiSOC™ system on a chip processors or other

future processors. Processor 570 may include various modules associated with embodiments of the present invention.

[00072] Communication port 560 can be any of an RS-232 port for use with a modem based dialup connection, a 10/100 Ethernet port, a Gigabit or 10 Gigabit port using copper or fiber, a serial port, a parallel port, or other existing or future ports. Communication port 560 may be chosen depending on a network, such a Local Area Network (LAN), Wide Area Network (WAN), or any network to which computer system connects.

[00073] Memory 530 can be Random Access Memory (RAM), or any other dynamic storage device commonly known in the art. Read only memory 540 can be any static storage device(s) e.g., but not limited to, a Programmable Read Only Memory (PROM) chips for storing static information e.g. start-up or BIOS instructions for processor 570.

[00074] Mass storage 550 may be any current or future mass storage solution, which can be used to store information and/or instructions. Exemplary mass storage solutions include, but are not limited to, Parallel Advanced Technology Attachment (PATA) or Serial Advanced Technology Attachment (SATA) hard disk drives or solid-state drives (internal or external, e.g., having Universal Serial Bus (USB) and/or Firewire interfaces), e.g. those available from Seagate (e.g., the Seagate Barracuda 7200 family) or Hitachi (e.g., the Hitachi Deskstar 7K1000), one or more optical discs, Redundant Array of Independent Disks (RAID) storage, e.g. an array of disks (e.g., SATA arrays), available from various vendors including Dot Hill Systems Corp., LaCie, Nexsan Technologies, Inc. and Enhance Technology, Inc.

[00075] Bus 520 communicatively couples processor(s) 570 with the other memory, storage and communication blocks. Bus 520 can be, e.g. a Peripheral Component Interconnect (PCI) / PCI Extended (PCI-X) bus, Small Computer System Interface (SCSI), USB or the like, for connecting expansion cards, drives and other subsystems as well as other buses, such a front side bus (FSB), which connects processor 570 to software system.

[00076] Optionally, operator and administrative interfaces, e.g. a display, keyboard, and a cursor control device, may also be coupled to bus 520 to support direct operator interaction with computer system. Other operator and administrative interfaces can be provided through network connections connected through communication port 560. External storage device 510 can be any

kind of external hard-drives, floppy drives, IOMEGA® Zip Drives, Compact Disc - Read Only Memory (CD-ROM), Compact Disc - Re-Writable (CD-RW), Digital Video Disk - Read Only Memory (DVD-ROM). Components described above are meant only to exemplify various possibilities. In no way should the aforementioned exemplary computer system limit the scope of the present disclosure.

[00077] Thus, it will be appreciated by those of ordinary skill in the art that the diagrams, schematics, illustrations, and the like represent conceptual views or processes illustrating systems and methods embodying this invention. The functions of the various elements shown in the figures may be provided through the use of dedicated hardware as well as hardware capable of executing associated software. Similarly, any switches shown in the figures are conceptual only. Their function may be carried out through the operation of program logic, through dedicated logic, through the interaction of program control and dedicated logic, or even manually, the particular technique being selectable by the entity implementing this invention. Those of ordinary skill in the art further understand that the exemplary hardware, software, processes, methods, and/or operating systems described herein are for illustrative purposes and, thus, are not intended to be limited to any particular named.

[00078] As used herein, and unless the context dictates otherwise, the term "coupled to" is intended to include both direct coupling (in which two elements that are coupled to each other contact each other) and indirect coupling (in which at least one additional element is located between the two elements). Therefore, the terms "coupled to" and "coupled with" are used synonymously. Within the context of this document terms "coupled to" and "coupled with" are also used euphemistically to mean "communicatively coupled with" over a network, where two or more devices are able to exchange data with each other over the network, possibly via one or more intermediary device.

[00079] It should be apparent to those skilled in the art that many more modifications besides those already described are possible without departing from the inventive concepts herein. The inventive subject matter, therefore, is not to be restricted except in the spirit of the appended claims. Moreover, in interpreting both the specification and the claims, all terms should be interpreted in the broadest possible manner consistent with the context. In particular, the terms "comprises" and "comprising" should be interpreted as referring to elements, components, or steps

in a non-exclusive manner, indicating that the referenced elements, components, or steps may be present, or utilized, or combined with other elements, components, or steps that are not expressly referenced. Where the specification claims refers to at least one of something selected from the group consisting of A, B, C and N, the text should be interpreted as requiring only one element from the group, not A plus N, or B plus N, etc.

[00080] While the foregoing describes various embodiments of the invention, other and further embodiments of the invention may be devised without departing from the basic scope thereof. The scope of the invention is determined by the claims that follow. The invention is not limited to the described embodiments, versions or examples, which are included to enable a person having ordinary skill in the art to make and use the invention when combined with information and knowledge available to the person having ordinary skill in the art.

100

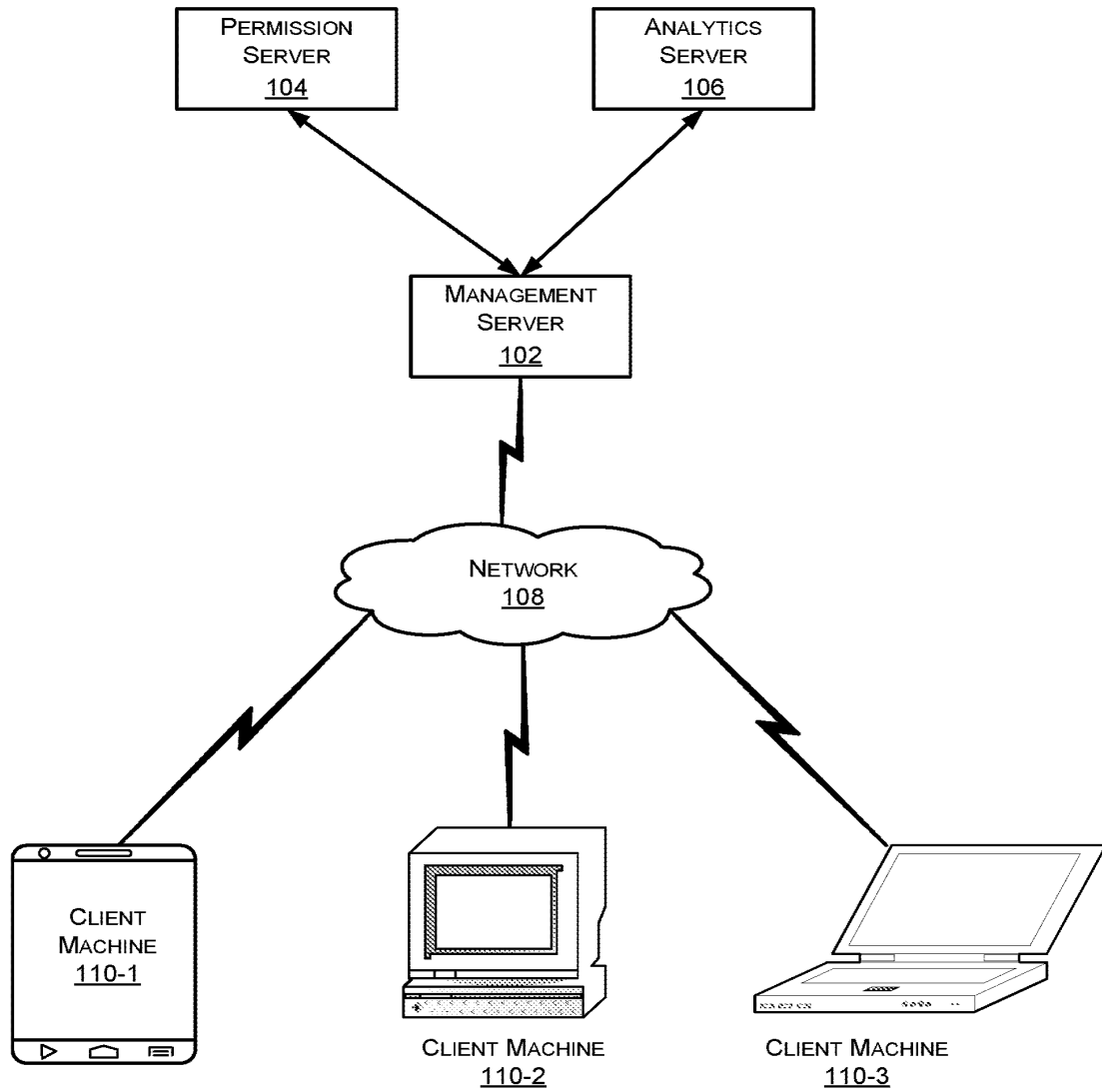


FIG. 1

200

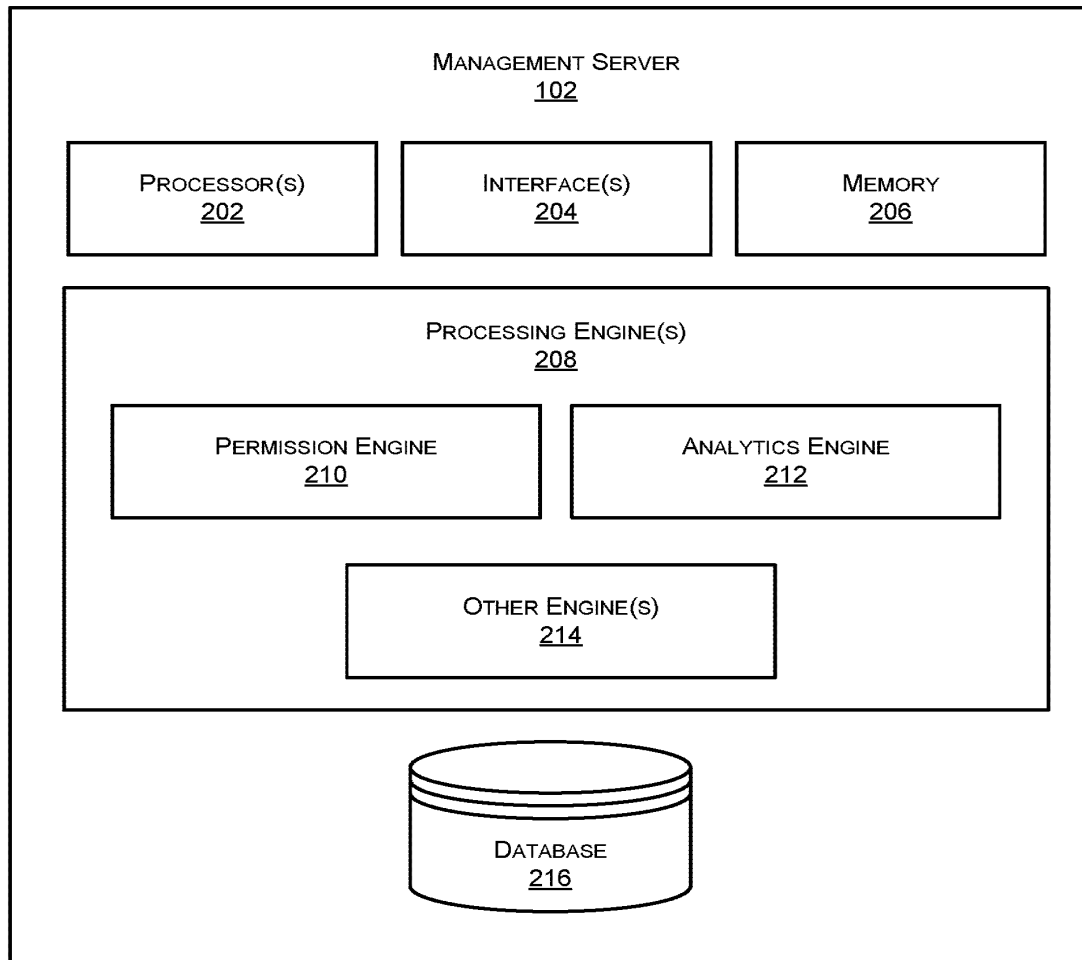


FIG. 2

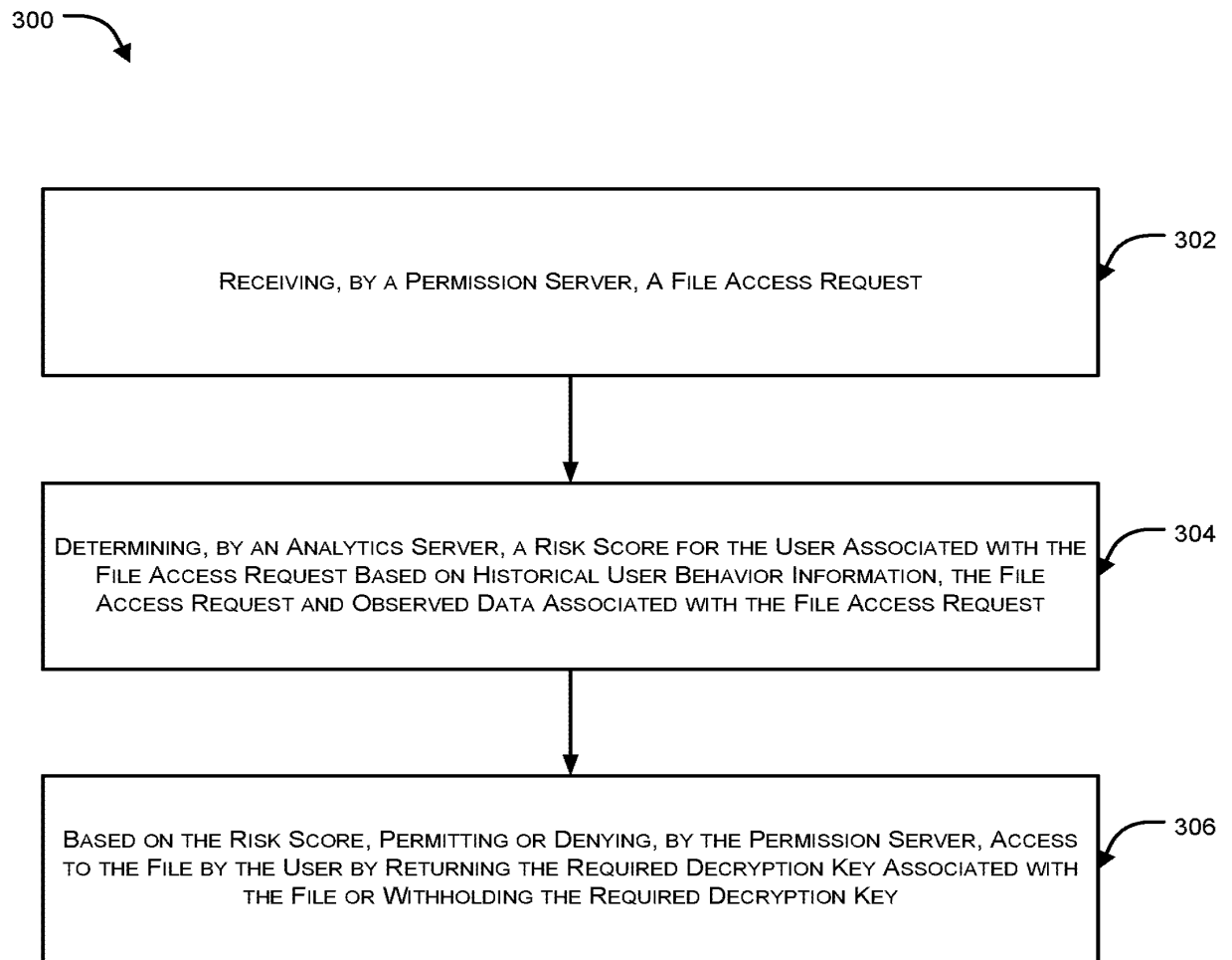


FIG. 3A

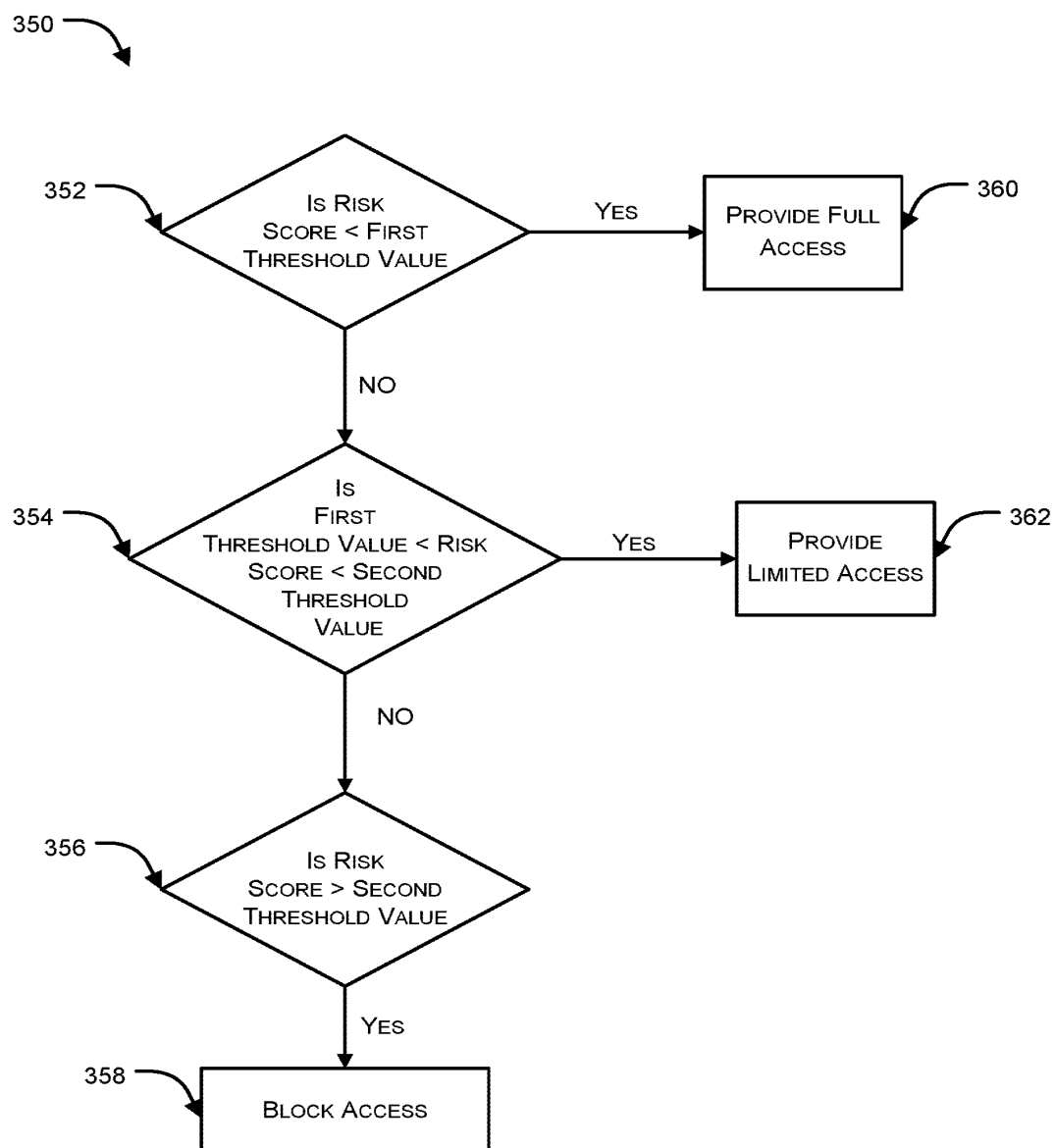


FIG. 3B

400

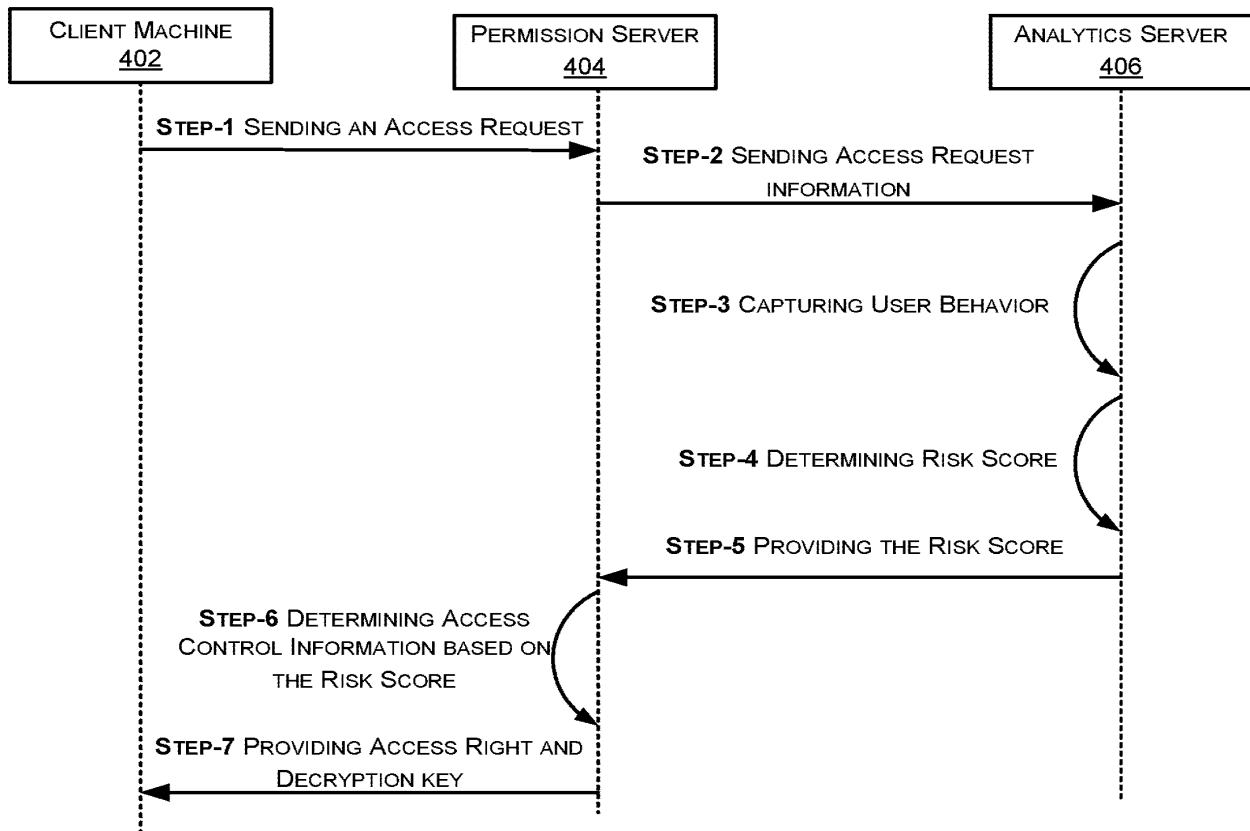


FIG. 4

500

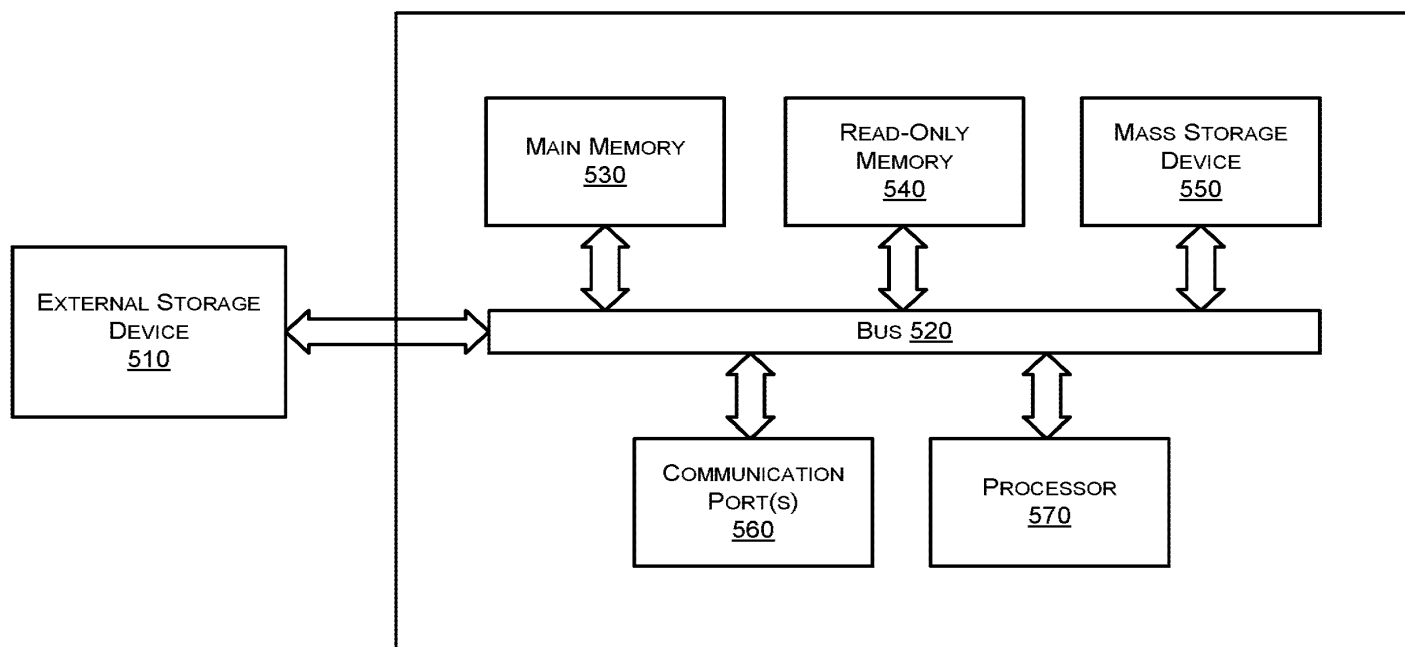


FIG. 5

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-031800
		Application Number	
Title of Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		
<small>The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.</small>			

Secrecy Order 37 CFR 5.2:

☐	Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)
--------------------------	---

Inventor Information:

Inventor	1				Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Matthew	J.	Little		
Residence Information (Select One) US Residency • Non US Residency Active US Military Service					
City	Loanhead		Country of Residence ⁱ	GB	
Mailing Address of Inventor:					
Address 1		40 Torphichen Street			
Address 2					
City	Edinburgh		State/Province		
Postal Code	EH3 8JB		Country ⁱ	GB	
Inventor	2				Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Jamie	R.	Graves		
Residence Information (Select One) US Residency • Non US Residency Active US Military Service					
City	Edinburgh		Country of Residence ⁱ	GB	
Mailing Address of Inventor:					
Address 1		40 Torphichen Street			
Address 2					
City	Edinburgh		State/Province		
Postal Code	EH3 8JB		Country ⁱ	GB	
Inventor	3				Remove
Legal Name					

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-031800
		Application Number	
Title of Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		

Prefix	Given Name	Middle Name	Family Name	Suffix
	Carson		Leonard	
Residence Information (Select One) US Residency ☒ Non US Residency Active US Military Service				
City	Edinburgh	Country of Residence ⁱ	GB	

Mailing Address of Inventor:

Address 1	40 Torphichen Street			
Address 2				
City	Edinburgh	State/Province		
Postal Code	EH3 8JB	Country ⁱ	GB	
Inventor	4	Remove		
Legal Name				

Prefix	Given Name	Middle Name	Family Name	Suffix
	Miles		Gould	
Residence Information (Select One) US Residency ☒ Non US Residency Active US Military Service				
City	Edinburgh	Country of Residence ⁱ	GB	

Mailing Address of Inventor:

Address 1	40 Torphichen Street			
Address 2				
City	Edinburgh	State/Province		
Postal Code	EH3 8JB	Country ⁱ	GB	
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.				
Add				

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).	
☐ An Address is being provided for the correspondence Information of this application.	
Customer Number	64128
Email Address	Add Email Remove Email

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-031800
		Application Number	
Title of Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		

Application Information:

Title of the Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		
Attorney Docket Number	FORT-031800	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	6	Suggested Figure for Publication (if any)	3A

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐ Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.			
Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	64128		

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-031800
		Application Number	
Title of Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78. When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	<input type="text"/>	<input type="button" value="Remove"/>	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			<input type="button" value="Add"/>

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)ⁱ the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ⁱ (if applicable)	<input type="button" value="Remove"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	
Additional Foreign Priority Data may be generated within this form by selecting the Add button.				<input type="button" value="Add"/>

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

- ☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
- NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-031800
		Application Number	
Title of Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-031800
		Application Number	
Title of Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.			
Applicant	1		<input type="button" value="Remove"/>
<p>If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.</p>			
<input type="button" value="Clear"/>			
☒ Assignee		Legal Representative under 35 U.S.C. 117	Joint Inventor
Person to whom the inventor is obligated to assign.		Person who shows sufficient proprietary interest	
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:			
<div style="border: 1px solid black; height: 20px; width: 100%;"></div>			
Name of the Deceased or Legally Incapacitated Inventor: <div style="border: 1px solid black; width: 400px; height: 20px;"></div>			
If the Applicant is an Organization check here. ☒			
Organization Name	Fortinet, Inc.		
Mailing Address Information For Applicant:			
Address 1	899 Kifer Rd.		
Address 2			
City	Sunnyvale	State/Province	CA
Country	US	Postal Code	94086
Phone Number		Fax Number	
Email Address			
Additional Applicant Data may be generated within this form by selecting the Add button. <input type="button" value="Add"/>			

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-031800
		Application Number	
Title of Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		

Assignee	1		
Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.			
<input type="button" value="Remove"/>			
If the Assignee or Non-Applicant Assignee is an Organization check here. ☒			
Organization Name	Fortinet, Inc.		
Mailing Address Information For Assignee including Non-Applicant Assignee:			
Address 1	399 Kifer Rd.		
Address 2			
City	Sunnyvale	State/Province	CA
Country i	US	Postal Code	94086
Phone Number		Fax Number	
Email Address			
Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. <input type="button" value="Add"/>			

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). However, if this Application Data Sheet is submitted with the **INITIAL** filing of the application and either box A or B is **not** checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Michael A DeSanctis/		Date (YYYY-MM-DD)	2019-03-22
First Name	Michael A.	Last Name	DeSanctis	Registration Number
				39957
Additional Signature may be generated within this form by selecting the Add button. <input type="button" value="Add"/>				

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-031800
		Application Number	
Title of Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		
First Named Inventor/Applicant Name:		Matthew J. Little		
Filer:		Michael A. DeSanctis		
Attorney Docket Number:		FORT-031800		
Filed as Large Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
UTILITY APPLICATION FILING	1011	1	300	300
UTILITY SEARCH FEE	1111	1	660	660
UTILITY EXAMINATION FEE	1311	1	760	760
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				1720

Electronic Acknowledgement Receipt	
EFS ID:	35507227
Application Number:	16362167
International Application Number:	
Confirmation Number:	6553
Title of Invention:	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS
First Named Inventor/Applicant Name:	Matthew J. Little
Customer Number:	64128
Filer:	Michael A. DeSanctis
Filer Authorized By:	
Attorney Docket Number:	FORT-031800
Receipt Date:	22-MAR-2019
Filing Date:	
Time Stamp:	16:37:02
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$1720
RAM confirmation Number	032519INTEFSW16372800
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Patent_Application.pdf	245011	yes	31
			98f7f567bac5257332adc0345377ddeff61a97b3		
	Multipart Description/PDF files in .zip description				
	Document Description		Start		End
	Abstract		31		31
	Claims		27		30
	Specification		1		26
Warnings:					
Information:					
2	Drawings-only black and white line drawings	Figures.pdf	78834	no	6
			ea82b7b1d0edf3d791c24aa0692950e2dafaad2b		
Warnings:					
Information:					
3	Application Data Sheet	ADS.pdf	1256169	no	9
			9cf1d0773ae4cfdfffb414008f364b1964843460		
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	34723	no	2
			fbd8a96fd7c60d4be6f20dc7ce8ceddf87f1a40b		
Warnings:					
Information:					
Total Files Size (in bytes):			1614737		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
16/362,167	03/22/2019	2139	1720	FORT-031800	20	2

CONFIRMATION NO. 6553

64128

MICHAEL A DESANCTIS
JAFFERY WATSON MENDONSA & HAMILTON LLP
7501 Village Square Drive, Ste. 206
Castle Pines, CO 80108

FILING RECEIPT



0000000107197314

Date Mailed: 04/09/2019

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Matthew J. Little, Loanhead, UNITED KINGDOM;
Jamie R. Graves, Edinburgh, UNITED KINGDOM;
Carson Leonard, Edinburgh, UNITED KINGDOM;
Miles Gould, Edinburgh, UNITED KINGDOM;

Applicant(s)

Fortinet, Inc., Sunnyvale, CA;

Assignment For Published Patent Application

Fortinet, Inc., Sunnyvale, CA

Power of Attorney: None

Domestic Applications for which benefit is claimed - None.

A proper domestic benefit claim must be provided in an Application Data Sheet in order to constitute a claim for domestic benefit. See 37 CFR 1.76 and 1.78.

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 04/05/2019

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 16/362,167**

Projected Publication Date: 09/24/2020

Non-Publication Request: No

Early Publication Request: No
Title

FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS

Preliminary Class

711

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

page 2 of 4

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 16/362,167			
APPLICATION AS FILED - PART I									
(Column 1)		(Column 2)		SMALL ENTITY		OTHER THAN SMALL ENTITY			
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)		
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	300		
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	660		
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	760		
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*			OR	x 100 =	0.00		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*				x 460 =	0.00		
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00		
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00		
			TOTAL			TOTAL	1720		
* If the difference in column 1 is less than zero, enter "0" in column 2.									
APPLICATION AS AMENDED - PART II									
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OTHER THAN SMALL ENTITY	
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)	RATE(\$)	ADDITIONAL FEE(\$)		
	Total (37 CFR 1.16(i))	*	Minus **	=	x =	OR	x =		
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x =	OR	x =		
	Application Size Fee (37 CFR 1.16(s))					OR			
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					OR			
			TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE			
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OTHER THAN SMALL ENTITY	
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)	RATE(\$)	ADDITIONAL FEE(\$)		
	Total (37 CFR 1.16(i))	*	Minus **	=	x =	OR	x =		
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x =	OR	x =		
	Application Size Fee (37 CFR 1.16(s))					OR			
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					OR			
			TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE			
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.									



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/362,167	03/22/2019	Matthew J. Little	FORT-031800

CONFIRMATION NO. 6553

FORMALITIES LETTER



OC000000107197315

64128

MICHAEL A DESANCTIS
JAFFERY WATSON MENDONSA & HAMILTON LLP
7501 Village Square Drive, Ste. 206
Castle Pines, CO 80108

Date Mailed: 04/09/2019

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing.

Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- Surcharge as set forth in 37 CFR 1.16(f) must be submitted.

The surcharge is due for any one of:

- late submission of the basic filing fee, search fee, or examination fee,
- late submission of inventor's oath or declaration,
- filing an application that does not contain at least one claim on filing, or
- submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of this Notice to avoid abandonment is/are itemized below. No entity status discount is in effect. If applicant is qualified for small entity status, a written assertion of small entity status must be submitted to establish small entity status. (See 37 CFR 1.27). If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- \$ 160 surcharge.
- \$(0) previous unapplied payment amount.
- \$ 160 TOTAL FEE BALANCE DUE.

Items Required To Avoid Processing Delays:

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):
Matthew J. Little
Jamie R. Graves
Carson Leonard
Miles Gould

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice".
<https://portal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html>

For more information about EFS-Web please call the USPTO Electronic Business Center at 1-866-217-9197 or visit our website at <http://www.uspto.gov/ebc>.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/fhadera/

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 04/19/2019

CVORACHA	ADJ #00000020	Mailroom Dt: 04/15/2019	
	Seq No: 7167	Sales Acctg Dt: 04/16/2019	16362167
	02 FC : 1464	-140.00 OP	

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 04/19/2019

CVORACHA	SALE	#00000027	Mailroom Dt:	04/15/2019	16362167
		01	FC : 1830	140.00	OP

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	16362167
	Filing Date	2019-03-22
	First Named Inventor	Matthew J. Little
	Art Unit	2139
	Examiner Name	
	Attorney Docket Number	FORT-031800

U.S.PATENTS							Remove	
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear		
	1	8595497		2013-11-26	Dogu et al.			
	2	8887274		2014-11-11	Buchanan et al.			
If you wish to add additional U.S. Patent citation information please click the Add button.							Add	
U.S.PATENT APPLICATION PUBLICATIONS							Remove	
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear		
	1	20180069881		2018-03-18	Graves et al.			
	2	20180351979		2018-12-06	Mandrychenko et al.			
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add	
FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ^{2,i}	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16362167
Filing Date	2019-03-22
First Named Inventor	Matthew J. Little
Art Unit	2139
Examiner Name	
Attorney Docket Number	FORT-031800

If you wish to add additional Foreign Patent Document citation information please click the Add button			Add
NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	Kerr, O.S., et al. "Encryption Workarounds." The Georgetown Law Journal. Vol. 106:989 2018. pgs 989-1019.	
	2	FinalCode. How FinalCode Works. http://www.finalcode.com/jp/english/about/mechanism/ . 2 pgs.	
If you wish to add additional non-patent literature document citation information please click the Add button			Add
EXAMINER SIGNATURE			
Examiner Signature			Date Considered
<p>*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.</p>			
<p>¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.</p>			

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16362167
Filing Date	2019-03-22
First Named Inventor	Matthew J. Little
Art Unit	2139
Examiner Name	
Attorney Docket Number	FORT-031800

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Michael A. DeSanctis/	Date (YYYY-MM-DD)	2019-04-12
Name/Print	Michael A. DeSanctis	Registration Number	39957

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt	
EFS ID:	35732536
Application Number:	16362167
International Application Number:	
Confirmation Number:	6553
Title of Invention:	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS
First Named Inventor/Applicant Name:	Matthew J. Little
Customer Number:	64128
Filer:	Michael A. DeSanctis
Filer Authorized By:	
Attorney Docket Number:	FORT-031800
Receipt Date:	15-APR-2019
Filing Date:	22-MAR-2019
Time Stamp:	21:28:13
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment		no			
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS_31800.pdf	1034449 a7dc34976fb167686a586707c67fdb887c3c2ae1	no	4
Warnings:					

Information:					
2	Non Patent Literature	NPL_1_31800.pdf	335305	no	31
			ff8e6f5a745acdf1c3998d1a90472866701ad4eb		
Warnings:					
Information:					
3	Non Patent Literature	NPL_2_31800.pdf	103799	no	2
			c15fbee4db65287a747cdfb1627741d8cb07bbff		
Warnings:					
Information:					
Total Files Size (in bytes):			1473553		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

☒ Practitioners associated with the Customer Number:

64128

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

☒ The address associated with Customer Number:

64128

OR

☐ Firm or Individual Name			
Address			
City	State	Zip	
Country			
Telephone	Email		

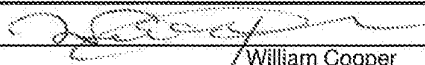
Assignee Name and Address:

Fortinet, Inc.
899 Kifer Rd.
Sunnyvale, CA 94086

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date	1-11-2018
Name	William Cooper	Telephone	(925) 984-3225
Title	Director of Litigation, Intellectual Property and Privacy		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-031800
		Application Number	
Title of Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		
<p>The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.</p> <p>This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.</p>			

Secrecy Order 37 CFR 5.2:

☐	Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)
--------------------------	---

Inventor Information:

Inventor 1					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Matthew	J.	Little		
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service					
City	Loanhead		Country of Residence ⁱ	GB	
Mailing Address of Inventor:					
Address 1		40 Torphichen Street			
Address 2					
City	Edinburgh		State/Province		
Postal Code	EH3 8JB		Country ⁱ	GB	
Inventor 2					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Jamie	R.	Graves		
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service					
City	Edinburgh		Country of Residence ⁱ	GB	
Mailing Address of Inventor:					
Address 1		40 Torphichen Street			
Address 2					
City	Edinburgh		State/Province		
Postal Code	EH3 8JB		Country ⁱ	GB	
Inventor 3					Remove
Legal Name					

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-031800
		Application Number	
Title of Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		

Prefix	Given Name	Middle Name	Family Name	Suffix
	Carson		Leonard	
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service				
City	Edinburgh	Country of Residence ⁱ	GB	

Mailing Address of Inventor:

Address 1	40 Torphichen Street			
Address 2				
City	Edinburgh	State/Province		
Postal Code	EH3 8JB	Country ⁱ	GB	

Inventor 4

Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Miles		Gould	
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service				
City	Edinburgh	Country of Residence ⁱ	GB	

Mailing Address of Inventor:

Address 1	40 Torphichen Street			
Address 2				
City	Edinburgh	State/Province		
Postal Code	EH3 8JB	Country ⁱ	GB	

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button.

Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ An Address is being provided for the correspondence Information of this application.

Customer Number	64128		
Email Address		Add Email	Remove Email

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-031800
		Application Number	
Title of Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		

Application Information:

Title of the Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		
Attorney Docket Number	FORT-031800	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	6	Suggested Figure for Publication (if any)	3A

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐	Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐	Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.			
Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	64128		

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-031800
		Application Number	
Title of Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78. When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status			
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)ⁱ the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	 Access Code ⁱ (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

☐ NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-031800
		Application Number	
Title of Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-031800
		Application Number	
Title of Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.			
Applicant 1			
If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.			
Clear			
☒ Assignee	☐ Legal Representative under 35 U.S.C. 117	☐ Joint Inventor	
☐ Person to whom the inventor is obligated to assign.		☐ Person who shows sufficient proprietary interest	
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:			
Name of the Deceased or Legally Incapacitated Inventor:			
If the Applicant is an Organization check here. ☒			
Organization Name	Fortinet, Inc.		
Mailing Address Information For Applicant:			
Address 1	899 Kifer Rd.		
Address 2			
City	Sunnyvale	State/Province	CA
Country	US	Postal Code	94086
Phone Number		Fax Number	
Email Address			
Additional Applicant Data may be generated within this form by selecting the Add button.			

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-031800
		Application Number	
Title of Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		

Assignee 1			
Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.			
If the Assignee or Non-Applicant Assignee is an Organization check here. ☒			
Organization Name	Fortinet, Inc.		
Mailing Address Information For Assignee including Non-Applicant Assignee:			
Address 1	899 Kifer Rd.		
Address 2			
City	Sunnyvale	State/Province	CA
Country ⁱ	US	Postal Code	94086
Phone Number		Fax Number	
Email Address			
Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.			

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).					
This Application Data Sheet must be signed by a patent practitioner if one or more of the applicants is a juristic entity (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, all joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of all joint inventor-applicants.					
See 37 CFR 1.4(d) for the manner of making signatures and certifications.					
Signature	/Michael A DeSanctis/			Date (YYYY-MM-DD)	2019-04-15
First Name	Michael A.	Last Name	DeSanctis	Registration Number	39957
Additional Signature may be generated within this form by selecting the Add button.					

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	FORT-031800
		Application Number	
Title of Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc Code: R48.REQ

Document Description: Request under Rule 48 correcting inventorship

PTO/AIA/40 (04-18)

Approved for use through 11/30/2020. OMB 0651-0031

U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**REQUEST FOR CORRECTION IN A
PATENT APPLICATION RELATING TO
INVENTORSHIP OR AN INVENTOR
NAME, OR ORDER OF NAMES, OTHER
THAN IN A REISSUE APPLICATION (37
CFR 1.48)**

Application Number	16/362,167
Filing Date	March 22, 2019
First Named Inventor	Matthew J. Little
Art Unit	2139
Examiner Name	TBD
Practitioner Docket Number	FORT-031800

To: Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Applicant hereby requests that the inventorship be corrected or changed, or that the name of the inventor or a joint inventor, or the order of the names of joint inventors, be changed, in the above-identified application. Note: 37 CFR 1.48 applies to any request to correct inventorship filed on or after September 16, 2012, regardless of the application filing date. Do not submit this form after payment of the issue fee or if the application has been patented. See 37 CFR 1.324 for correction of inventorship in a patent.

Please check the applicable box(es) below.

For a nonprovisional application:

- ☐ 1. This request is to correct or change the inventorship in a **nonprovisional** application (under 37 CFR 1.48(a)) and includes:
- ☐ An application data sheet (ADS) in accordance with 37 CFR 1.76(c) with the corrected or updated information shown with markings (e.g., underlining for insertions, strikethrough for deletions). See the Manual of Patent Examining Procedure (MPEP) section 601.05(a) for information about filing an ADS in an application filed on/after September 16, 2012. For information about filing a Supplemental ADS in an application filed before September 16, 2012, see MPEP 601.05(b).
- ☐ The processing fee set forth in 37 CFR 1.17(i). \$ _____
- ☐ An inventor is being added. An inventor's oath or declaration by any actual inventor who has not yet executed an oath or declaration is required (see 37 CFR 1.48(b)). See MPEP 602.01(a) for information about an inventor's oath or declaration for an application filed on/after September 16, 2012 (e.g., form PTO/AIA/01). For information about an inventor's oath or declaration for an application filed before September 16, 2012 (e.g., form PTO/SB/01), see MPEP 602.01(b).
- ☐ This request is being filed after the first Office action on the merits has been given or mailed (see 37 CFR 1.48(c) and 1.17(d)). Check one of the following:
- ☐ This request to correct or change the inventorship is due solely to the cancellation of claims in the application.
- OR
- ☐ The fee set forth in 37 CFR 1.17(d) is due (in addition to the fee set forth in 37 CFR 1.17(i)). \$ _____

[Page 1 of 2]

This collection of information is required by 37 CFR 1.48. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

**REQUEST FOR CORRECTION IN A PATENT APPLICATION RELATING TO INVENTORSHIP OR AN
INVENTOR NAME, OR ORDER OF NAMES, OTHER THAN IN A REISSUE APPLICATION
(37 CFR 1.48)**

- ☒ 2. This request is to correct or update the name of the inventor or a joint inventor, or the order of names of joint inventors, in a **nonprovisional** application (under 37 CFR 1.48(f)) and includes:

- ☒ An application data sheet in accordance with 37 CFR 1.76(c) identifying the complete inventive entity, including the corrected or updated name of the inventor, or the new order of names shown with markings (e.g., underlining for insertions, strikethrough for deletions). See the MPEP 601.05(a) for information about filing an ADS in an application filed on/after September 16, 2012. For information about filing a Supplemental ADS in an application filed before September 16, 2012, see MPEP 601.05(b).

- ☒ The processing fee set forth in 37 CFR 1.17(i). \$ 140

For a provisional application:

- ☐ This request is to change or correct the inventorship, or correct or update the name of the inventor or a joint inventor, in a **provisional** application (under 37 CFR 1.48(d)) and includes:

- ☐ Attached hereto is a document that is signed by a party set forth in 37 CFR 1.33(b) and identifies each inventor by his or her legal name, in the preferred order. Note: the document may be an application data sheet in accordance with 37 CFR 1.76(c) that identifies the changes with markings (underlining for insertions, strikethrough for deletions).

- ☐ The processing fee set forth in 37 CFR 1.17(q). \$ _____

Fee Payment Information:

- ☐ Applicant asserts small entity status. See 37 CFR 1.27.
- ☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously
- ☐ A check in the amount of the fee is enclosed.
- ☒ Payment by credit card. Form PTO-2038 is attached.
- ☐ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. _____.
- ☒ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

- ☐ Applicant* ☒ attorney or agent of record ☐ attorney or agent acting under 37 CFR 1.34
Registration number 39957 Registration number _____

Signature Michael A DeSanctis/

Typed or printed name Michael A. DeSanctis

Date April 15, 2019

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. *Juristic entities must be represented by a patent practitioner (See 37 CFR 1.31, applicable to any paper filed on or after September 16, 2012 that is presented on behalf of a juristic entity, regardless of application filing date). Submit multiple forms if more than one signature is required, see below**.

☒ ** Total of 1 forms are submitted.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal				
Application Number:		16362167		
Filing Date:		22-Mar-2019		
Title of Invention:		FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		
First Named Inventor/Applicant Name:		Matthew J. Little		
Filer:		Michael A. DeSanctis		
Attorney Docket Number:		FORT-031800		
Filed as Large Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
LATE FILING FEE FOR OATH OR DECLARATION	1051	1	160	160
Petition:				
PETITION FEE- 37 CFR 1.17(H) (GROUP III)	1464	1	140	140
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				300

Electronic Acknowledgement Receipt	
EFS ID:	35732051
Application Number:	16362167
International Application Number:	
Confirmation Number:	6553
Title of Invention:	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS
First Named Inventor/Applicant Name:	Matthew J. Little
Customer Number:	64128
Filer:	Michael A. DeSanctis
Filer Authorized By:	
Attorney Docket Number:	FORT-031800
Receipt Date:	15-APR-2019
Filing Date:	22-MAR-2019
Time Stamp:	21:26:14
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$ 300
RAM confirmation Number	041619INTEFSW21264100
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Applicant Response to Pre-Exam Formalities Notice	Response_Missing_Parts_31800.pdf	16151	no	1
			83f211712ace3937bd926ce88636f1edfdcecb4		
Warnings:					
Information:					
2	Oath or Declaration filed	Executed_Declarations_31800.pdf	159748	no	3
			ebd06213513225214222ef9e50e6b95c9abebda2		
Warnings:					
Information:					
3	Assignee showing of ownership per 37 CFR 3.73	Statement_31800.pdf	117659	no	3
			ff77b6d203ec3ed9b9433d9da3984fbae7364f6e		
Warnings:					
Information:					
4	Assignee showing of ownership per 37 CFR 3.73	Executed_Assignment_31800.pdf	77251	no	2
			4ab008565c4fde75a8aa8045b482b06cb38a9021		
Warnings:					
Information:					
5	Power of Attorney	Executed_POA.pdf	474709	no	1
			90c012816ba61c3524f930194f96b062ec0f98ca		
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
6	Application Data Sheet	ADS_substitute_31800.pdf	152249	no	9
			682f01bd832400315b8f7bbc4f746874c192634b		
Warnings:					

Information:					
This is not an USPTO supplied ADS fillable form					
7	Request under Rule 48 correcting inventorship	Request_Correction.pdf	1161416 2215402996ab54943068a6bb94cd0758b59ce5e2	no	3
Warnings:					
Information:					
8	Fee Worksheet (SB06)	fee-info.pdf	32031 eb4fad05f9653ea52e33f5c5e3f19f8edac75423	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			2191214		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Matthew J. Little	Examiner:
App. No.: 16/362,167	Group Art Unit: 2139
Filed: March 22, 2019	Conf. No.: 6553
For: FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS	Docket No.: FORT-031800

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

RESPONSE TO THE NOTICE TO FILE MISSING PARTS

Sir:

In response to the Notice to File Missing Parts dated April 9, 2019, enclosed for filing are a Substitute Application Data Sheet, a Statement Under 3.73(c), a Power of Attorney and the Executed Declarations in connection with the above-mentioned matter. Payment in the amount of \$160 is being submitted via EFS-Web concurrently with the filing of this paper.

If the Examiner has any questions, please telephone the undersigned at 303-856-7155.

Respectfully submitted,

Jaffery Watson Mendonsa & Hamilton LLP

Date: April 15, 2019

by /Michael A. DeSanctis/
Michael A. DeSanctis, Esq.
Reg. No. 39,957
Customer No. 64128
Ph: (303) 856-7155

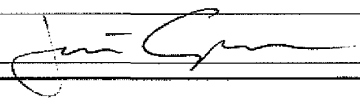
**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)**

Title of Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS
<p>As the below named inventor, I hereby declare that:</p> <p>This declaration is directed to: ☒ The attached application, or ☐ United States application or PCT international application number _____ filed on _____.</p> <p>The above-identified application was made or authorized to be made by me.</p> <p>I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.</p> <p>I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.</p> <p style="text-align: center;">WARNING:</p> <p>Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.</p>	
<p>LEGAL NAME OF INVENTOR</p> <p>Inventor: <u>Matthew J. Little</u> Date (Optional) <u>26/03/2019</u></p> <p>Signature: </p>	
<p><small>Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.</small></p>	

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)**

Title of Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS
<p>As the below named inventor, I hereby declare that:</p> <p>This declaration is directed to: ☒ The attached application, or ☐ United States application or PCT international application number _____ filed on _____</p> <p>The above-identified application was made or authorized to be made by me.</p> <p>I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.</p> <p>I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.</p> <p style="text-align: center;">WARNING:</p> <p>Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.</p> <p>LEGAL NAME OF INVENTOR</p> <p>Inventor: <u>Jamie R. Graves</u> Date (Optional): <u>25/3/19</u></p> <p>Signature: <u></u></p> <p>Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.</p>	

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS
---------------------------	--

As the below named inventor, I hereby declare that:

This declaration is directed to:

☒

The attached application, or

☐

United States application or PCT international application number _____

filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

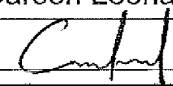
WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Carson Leonard

Date (Optional): 25/3/19

Signature: 

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Fortinet, Inc.

Application No./Patent No.: 16/362,167

Filed/Issue Date: March 22, 2019

Titled: FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS

Fortinet, Inc., a corporation

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☒ The assignee of the entire right, title, and interest.
2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):
- ☐ The extent (by percentage) of its ownership interest is ____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.
- ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

- A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.
- B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____
- The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.
2. From: _____ To: _____
- The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

[Page 1 of 2]

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☒ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Michael A DeSanctis/

Signature

Michael A. DeSanctis

Printed or Typed Name

April 15, 2019

Date

39957

Title or Registration Number

[Page 2 of 2]

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ASSIGNMENT

WHEREAS, We, **Matthew J. Little, Jamie R. Graves, and Carson Leonard**, have invented certain new and useful improvements for which an application entitled

"FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS"

is about to be made for Letters Patent of the United States, the application having been executed on even date herewith, and which may be identified in the United States Patent and Trademark Office by Application No. 16/362,167, filed on March 22, 2019 and further identified as Atty. Docket No. FORT-0318000.

WHEREAS, **Fortinet, Inc.**, a Corporation of the State of Delaware, and having its principal offices at 899 Kifer Rd., Sunnyvale, CA 94086 (hereafter "Assignee"), is desirous of acquiring the entire right, title and interest in and to the application, any inventions or discoveries described therein and in, to and under any and all Letters Patents to be obtained therefor;

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, we have sold, assigned and transferred, and by these presents do hereby sell, assign and transfer unto the Assignee, its successors and assigns:

1. the entire right, title and interest in and to the application, any inventions or discoveries described therein and the Letters Patent(s), both foreign and domestic, that may or shall issue, including all rights under the International Convention, and
2. all proceeds of the application, any inventions or discoveries described therein and the Letters Patent(s) (including but not limited to, damages for pre-patent grant infringement, all license royalties and proceeds of infringement suits); and in and to any and all causes of action (excepting claims upon the United States of America) for past, present, and future infringement of any of the Letters Patent(s), or relating to any inventions or discoveries described therein, including the right to collect royalties and seek injunctive relief, for all such infringements and the right to sue on all such causes of action for their own use and benefit and the use and benefit of their successors, assigns and legal representatives,

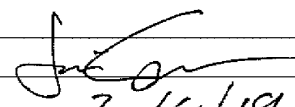
We do hereby authorize and request the Commissioner of Patents to issue the Letters Patent(s) to the Assignee in accordance herewith.

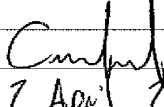
We further authorize the Assignee, its successors and assigns, or anyone it may properly designate, to apply for Letters Patent, in its own name, if desired, in any and all

foreign countries, and additionally to claim the filing date of the United States application and/or otherwise take advantage of the provisions of the International Convention.

We do hereby covenant and agree with the Assignee, its successors and assigns, that we will not execute any writing or do any act whatsoever conflicting with these presents, and that we or our executors or administrators will, at any time upon request, without further or additional consideration, but at the expense of the Assignee, its successors and assigns, execute such additional writings and do such additional acts as the Assignee, its successors and assigns, may deem necessary or desirable to perfect the Assignee's enjoyment of this grant, and render all necessary assistance in making application for and obtaining original, continuation, divisional, reissued, reexamined, substitute or extended Letters Patent(s) of the United States, or of any and all foreign countries on the invention, and in enforcing any rights, occurring as a result of such applications or patents, by giving testimony in any proceedings or transactions involving such applications or patents.

In Witness Whereof, We have hereunto set our hands and affixed our seals on the date written below.

Signature:		Signature:	
Date:	2 APRIL 2019.	Date:	2/4/19
Full Name:	Matthew J. Little	Full Name:	Jamie R. Graves
Mailing Address:	40 Torphichen Street	Mailing Address:	40 Torphichen Street
	Edinburgh EH3 8JB		Edinburgh EH3 8JB
	SCOTLAND		SCOTLAND

Signature:	
Date:	2 April 2019
Full Name:	Carson Leonard
Mailing Address:	40 Torphichen Street
	Edinburgh EH3 8JB
	SCOTLAND



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/362,167	03/22/2019	Matthew J. Little	FORT-031800

64128
MICHAEL A DESANCTIS
JAFFERY WATSON MENDONSA & HAMILTON LLP
7501 Village Square Drive, Ste. 206
Castle Pines, CO 80108

CONFIRMATION NO. 6553
37 CFR 1.48 ACKNOWLEDGEMENT
LETTER



Date Mailed: 04/24/2019

NOTICE OF ACCEPTANCE OF REQUEST UNDER 37 CFR 1.48(a)

This is in response to the applicant's request under 37 CFR 1.48(a) submitted on 04/15/2019.

The request under 37 CFR 1.48(a) to correct the inventorship, to correct or update the name of an inventor, or to correct the order of names of joint inventors is accepted.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/zabaha/



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
16/362,167	03/22/2019	2139	1880	FORT-031800	20	2

CONFIRMATION NO. 6553

UPDATED FILING RECEIPT



64128
MICHAEL A DESANCTIS
JAFFERY WATSON MENDONSA & HAMILTON LLP
7501 Village Square Drive, Ste. 206
Castle Pines, CO 80108

Date Mailed: 04/24/2019

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Matthew J. Little, Loanhead, UNITED KINGDOM;
Jamie R. Graves, Edinburgh, UNITED KINGDOM;
Carson Leonard, Edinburgh, UNITED KINGDOM;

Applicant(s)

Fortinet, Inc., Sunnyvale, CA;

Assignment For Published Patent Application

Fortinet, Inc., Sunnyvale, CA

Power of Attorney: The patent practitioners associated with Customer Number 64128

Domestic Applications for which benefit is claimed - None.

A proper domestic benefit claim must be provided in an Application Data Sheet in order to constitute a claim for domestic benefit. See 37 CFR 1.76 and 1.78.

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

Projected Publication Date: 09/24/2020

Non-Publication Request: No

Early Publication Request: No
Title

FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS

Preliminary Class

711

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 16/362,167			
APPLICATION AS FILED - PART I									
(Column 1)		(Column 2)		SMALL ENTITY		OTHER THAN SMALL ENTITY			
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)		
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	300		
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	660		
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	760		
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*			OR	x 100 =	0.00		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*				x 460 =	0.00		
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00		
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00		
			TOTAL			TOTAL	1720		
* If the difference in column 1 is less than zero, enter "0" in column 2.									
APPLICATION AS AMENDED - PART II									
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OTHER THAN SMALL ENTITY	
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	*	Minus **	=	x =		x =		
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x =		x =		
	Application Size Fee (37 CFR 1.16(s))								
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
			TOTAL ADD'L FEE			OR	TOTAL ADD'L FEE		
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OTHER THAN SMALL ENTITY	
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	*	Minus **	=	x =		x =		
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x =		x =		
	Application Size Fee (37 CFR 1.16(s))								
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
			TOTAL ADD'L FEE			OR	TOTAL ADD'L FEE		
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.									



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
16/362,167	03/22/2019	2139	1880	FORT-031800	20	2

CONFIRMATION NO. 6553

UPDATED FILING RECEIPT



64128
MICHAEL A DESANCTIS
JAFFERY WATSON MENDONSA & HAMILTON LLP
7501 Village Square Drive, Ste. 206
Castle Pines, CO 80108

Date Mailed: 04/24/2019

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Matthew J. Little, Loanhead, UNITED KINGDOM;
Jamie R. Graves, Edinburgh, UNITED KINGDOM;
Carson Leonard, Edinburgh, UNITED KINGDOM;

Applicant(s)

Fortinet, Inc., Sunnyvale, CA;

Assignment For Published Patent Application

Fortinet, Inc., Sunnyvale, CA

Power of Attorney: The patent practitioners associated with Customer Number 64128

Domestic Applications for which benefit is claimed - None.

A proper domestic benefit claim must be provided in an Application Data Sheet in order to constitute a claim for domestic benefit. See 37 CFR 1.76 and 1.78.

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

Projected Publication Date: 09/24/2020

Non-Publication Request: No

Early Publication Request: No
Title

FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS

Preliminary Class

711

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/362,167	03/22/2019	Matthew J. Little	FORT-031800

CONFIRMATION NO. 6553

POA ACCEPTANCE LETTER



OC000000107462786

64128
MICHAEL A DESANCTIS
JAFFERY WATSON MENDONSA & HAMILTON LLP
7501 Village Square Drive, Ste. 206
Castle Pines, CO 80108

Date Mailed: 04/24/2019

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 04/15/2019.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/zabaha/



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/362,167	03/22/2019	Matthew J. Little	FORT-031800

CONFIRMATION NO. 6553

64128

MICHAEL A DESANCTIS
JAFFERY WATSON MENDONSA & HAMILTON LLP
7501 Village Square Drive, Ste. 206
Castle Pines, CO 80108

PUBLICATION NOTICE



OC000000120151294

Title:FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS

Publication No.US-2020-0302074-A1

Publication Date:09/24/2020

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publicly available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <https://portal.uspto.gov/pair/PublicPair>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:

☒ Practitioners associated with Customer Number: 176502

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:

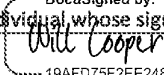
☒ The address associated with Customer Number: 176502

OR

Firm or individual name		
Address		
City	State	Zip
Country		
Telephone	Email	

Assignee name and address: Fortinet, Inc.
899 Kifer Rd., Sunnyvale, CA 94086

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of the practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

DocuSigned by: The individual whose signature and title is supplied below is authorized to act on behalf of the assignee.	
Signature  19AED75F2EE2484	Date 12/28/2020
Name Will Cooper	Telephone
Title VP Legal	

This collection of information is required by 37 CFR 1.31, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public, which is to update (and by the USPTO to process) the file of a patent or reexamination proceeding. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 18 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Fortinet, Inc.

Application No./Patent No.: 16/362,167

Filed/Issue Date: March 22, 2019

Titled: FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS

Fortinet, Inc., a corporation

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose one of options 1, 2, 3 or 4 below):

1. ☒ The assignee of the entire right, title, and interest.
2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):
- ☐ The extent (by percentage) of its ownership interest is ____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.
- ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose one of options A or B below):

- A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 048889, Frame 10660, or for which a copy thereof is attached.
- B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

[Page 1 of 2]

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☒ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Douglas M. Hamilton/

December 31, 2020

Signature

Date

Douglas M. Hamilton

47629

Printed or Typed Name

Title or Registration Number

[Page 2 of 2]

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt	
EFS ID:	41532494
Application Number:	16362167
International Application Number:	
Confirmation Number:	6553
Title of Invention:	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS
First Named Inventor/Applicant Name:	Matthew J. Little
Customer Number:	64128
Filer:	Douglas M. Hamilton
Filer Authorized By:	
Attorney Docket Number:	FORT-031800
Receipt Date:	31-DEC-2020
Filing Date:	22-MAR-2019
Time Stamp:	13:31:12
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment		no			
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		ExecutedPOA_373FORT031800 x.pdf	316338	yes	5
			18a17266d83b506d632bb0ee1dbbaefa2ac7aa0e		

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Power of Attorney	1	2
	Assignee showing of ownership per 37 CFR 3.73	3	5
Warnings:			
Information:			
Total Files Size (in bytes):		316338	
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>			



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/362,167	03/22/2019	Matthew J. Little	FORT-031800

CONFIRMATION NO. 6553

POWER OF ATTORNEY NOTICE



OC000000122410500

64128
MICHAEL A DESANCTIS
JAFFERY WATSON MENDONSA & HAMILTON LLP
7501 Village Square Drive, Ste. 206
Castle Pines, CO 80108

Date Mailed: 01/04/2021

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 12/31/2020.

- The Power of Attorney to you in this application has been revoked by the applicant. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/yteferra/



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/362,167	03/22/2019	Matthew J. Little	FORT-031800

176502
HDC Fortinet
224 South Main Street, #114
Mapleton, UT 84664

CONFIRMATION NO. 6553
POA ACCEPTANCE LETTER



Date Mailed: 01/04/2021

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 12/31/2020.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/ytferra/



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/362,167	03/22/2019	Matthew J. Little	FORT-031800(18167)	6553
176502	7590	10/05/2021	EXAMINER	
Douglas M. Hamilton			YANG, HAN	
HDC Fortinet				
224 S. Main Street, 114			ART UNIT	
Springville, UT 84663			PAPER NUMBER	
			2493	
			NOTIFICATION DATE	
			DELIVERY MODE	
			10/05/2021	
			ELECTRONIC	

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

dhamilton@hdciplaw.com
miquelchamilton@hamiltonshome.com

DETAILED ACTION

Notice of AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

The present office action is responsive to communications received on 3/22/2019. Claims 1-20 are pending.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 4/15/2019 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Examiner's Notes

Analysis under 35 U.S.C. 101, Double Patenting, and 35 U.S.C. 112 have been conducted, but no issues are found.

Non-transitory computer-readable storage medium claims 14-18 depend on dependent claim 13, while corresponding method claims 3-5, 8-9 depend on independent claim 1. Please ensure this inconsistency is intended.

Claim Objections

Claims 2 and 13 are objected to because of the following informalities:

- Claims 2 and 13 recite “wherein said determining ... **a risk score** for the first user comprises”, wherein “a risk score” should be “the risk score”.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-3, 5-7, 9-14, 16 and 18-20 are rejected under 35 U.S.C. 103 as being unpatentable over Levy (US 20190319945 A1) in view of Stamos (US 20040221172 A1).

Regarding claim 1, Levy teaches a method comprising:

obtaining and storing, by one or more servers associated with an enterprise network, information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users; ([0060] The threat management facility 100 may control access to the enterprise facility 102 networks. A network access facility 124 may restrict access to certain applications, networks, files, printers, servers, databases, and so on. In addition, the network access facility 124 may restrict user access under

certain conditions, such as the user's location, usage history, need to know, job position, connection type, time of day, method of authentication, client-system configuration.) Here Levy discloses in ¶150 that “the threat management facility 100 may include a policy management facility 112 that manages rules or policies for the enterprise facility 102. Exemplary rules include access permissions associated with networks, applications, compute instances, users, content, data, and the like. The policy management facility 112 may use a database, a text file, other data store, or a combination to store policies.”

receiving, by the one or more servers, a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the enterprise network in encrypted form; ([0207] FIG. 17 As shown in step 1702, the method 1700 may include receiving a request for a remote resource from a compute instance in an enterprise network, such as a request for authenticated access to the remote resource. This may include any resource that might usefully be accessed by a compute instance from within the enterprise network.) Here Levy discloses in ¶178 that “privacy may be addressed in some cases by user notifications and permissions, anonymization, tokenization, and encryption.”

responsive to receipt of the file access request, determining, by the one or more servers, a risk score for the first user based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request; and ([0208] As shown in step 1704, the method 1700 may include calculating risk scores, for example by calculating a first risk score for a user of the compute instance. In one aspect, the entity models described herein provide useful computer-implemented tools for measuring expected behavior and deviations therefrom, and may be usefully employed in this context to calculate risk scores for the particular entities of interest: the user of the compute instance.) Here Levy discloses in ¶156 “to draw policy or security

conclusions based on a history of users and file usage.”

based on the risk score, permitting or denying, by the one or more servers, access to the file. ([0210, 0211, 0217] As shown in step 1706, the method 1700 may include selecting an authentication model for access to the remote resource by the user and the device. More generally, the authentication models may provide various sets of authentication requirements using various combinations of the foregoing authentication factors or any other authentication factors, with the particular authentication factors varying based on the user and device risk scores. As shown in step 1708, the method 1700 may include authenticating the user to the remote resource according to the authentication model selected in step 1706.)

Levy teaches based on the risk score, permitting or denying, access to the file, but does not **explicitly** teach this is done by returning a decryption key for the file or withholding the decryption key. This aspect of the claim is identified as a difference.

However, Stamos in an analogous art **explicitly** teaches

based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key. ([0008, 0009] Encryption techniques such as those employing a Public Key Infrastructure (PKI) enable an enterprise to provide authentication, access control and confidentiality for its applications and data. Before accessing any information, the recipient must first authenticate with the policy server. The policy sever then issues copies of required keys to permit the recipient to decrypt the information.)

It would have been prima facie obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to combine the “dynamic authentication” concept of Levy, and the “adaptive encryption” approach of Stamos. One of ordinary skill in the art would have been motivated

to perform such a modification to address security problems that originate when authorized users abuse their authority, by selectively applying encryption policies at the point of use of a file, rather than simply at the point of file server and/or access storage (**Stamos [0018]**).

Regarding claim 2, Levy in view of Stamos teaches all the features with respect to claim 1, as outlined above. The combination further teaches **wherein said determining, by the one or more servers, a risk score for the first user comprises evaluating the file access request with reference to a model of user behavior developed by machine-learning.** ([Levy 0209] while event models for a user/device combination can provide a useful measure of riskiness, other measures may also or instead be used, either alone or in combination with such techniques. For example, other risk scores based on, e.g., signatures, context, behavior, machine learning or the like may be used in addition to, or instead of the risk scores described above to dynamically control authentication requirements based on assessed risk.)

Regarding claim 3, Levy in view of Stamos teaches all the features with respect to claim 1, as outlined above. The combination further teaches wherein the information regarding historical user behavior includes for each user of the plurality of users:

historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time; ([Levy 0111] The valuation model may, for example, estimate value based on file location, based on an access control content, based on content, or based on any other context, usage, feature or combination of the foregoing. For example, the valuation model may estimate value based on one or more of encryption status, file type, file usage

history, file creation date, file modification date, file content, and file author.)

historical data regarding observed locations of the user; and historical data regarding observed times at which the user accesses files. ([Levy 0060] A network access facility 124 may restrict access to certain applications, networks, files, printers, servers, databases, and so on. In addition, the network access facility 124 may restrict user access under certain conditions, such as the user's location, usage history, need to know, job position, connection type, time of day, method of authentication, client-system configuration, or the like.)

Regarding claim 5, Levy in view of Stamos teaches all the features with respect to claim 1, as outlined above. The combination further teaches **wherein the observed data includes a status indicative of whether the connection through which the first user initiated the file access request is trusted or untrusted.** ([Levy 0060] A network access facility 124 may restrict access to certain applications, networks, files, printers, servers, databases, and so on. In addition, the network access facility 124 may restrict user access under certain conditions, such as the user's location, usage history, need to know, job position, connection type, time of day, method of authentication, client-system configuration, or the like.) Here Levy depicts in [0033] that connection including "one or more gateways, bridges, wired networks, wireless networks, virtual private networks, other compute instances." It would have been prima facie obvious to one of ordinary skill in the art to conclude that connection through wired networks is more secure/trustworthy than through wireless networks (<https://aberdeencybersecurity.co.uk/wired-vs-wireless-networking>); as well as to conclude that connection with virtual private networks is more secure/trustworthy than without virtual private networks (<https://www.tomsguide.com/us/-vpn-for-beginners,news-17514.html>).

Regarding claim 6, Levy in view of Stamos teaches all the features with respect to claim 5, as outlined above. The combination further teaches **wherein the connection is trusted when the first user is on the enterprise network or accessing the enterprise network remotely via a secure connection.**

([Levy 0216] Other secondary techniques may also or instead be used to support authentication models or provide additional authentication factors. For example, a secondary authentication may be based on information such as whether a user recently logged in to the device, whether a user recently provided a token passcode, whether the device recently connected to the enterprise network, the current IP address for a device, the geolocation of a device, or whether the user/device combination recently logged in to the remote resource.) Here Levy discloses that connection is more trustworthy if user is on the enterprise network by citing “the compute instances 10-26 may be protected from threats even when a compute instance 10-26 is not connected to the enterprise facility 102 network” [0038].

Regarding claim 7, Levy in view of Stamos teaches all the features with respect to claim 5, as outlined above. The combination further teaches **wherein the connection is untrusted when the first user is not on the enterprise network or accessing the enterprise network remotely via an insecure connection.** ([Levy 0216] Other secondary techniques may also or instead be used to support authentication models or provide additional authentication factors. For example, a secondary authentication may be based on information such as whether a user recently logged in to the device, whether a user recently provided a token passcode, whether the device recently connected to the enterprise network, the current IP address for a device, the geolocation of a device, or whether the user/device combination recently logged in to the remote resource.) Here Levy discloses that connection is less trustworthy if user is not on the enterprise network by citing “the compute instances 10-26 may be protected from threats even when a compute instance 10-26 is not connected to the enterprise facility 102 network” [0038].

Regarding claim 9, Levy in view of Stamos teaches all the features with respect to claim 1, as outlined above. The combination further teaches **wherein said permitting or denying further comprises when the risk score is less than a first threshold, returning the decryption key and providing full access to the file.** ([Levy 0213] if the risk score for the device or the user (or some combination of these) is below a threshold such that it indicates that the user and device are safe, then the authentication model may forego an additional authentication factor.)

Regarding claim 10, Levy in view of Stamos teaches all the features with respect to claim 9, as outlined above. The combination further teaches **wherein said permitting or denying further comprises when the risk score is between the first threshold and a second threshold, returning the decryption key and providing limited access to the file.** ([Levy 0211] The risk scores may also generally be used as an authentication factor, e.g., by using the risk score as a property of the user and requiring a minimum or maximum value, or indirectly by using the risk score as a threshold for whether to select an authentication model requiring one or more additional authentication factors. [Levy 0213] if the risk score for the device or the user (or some combination of these) is below a threshold such that it indicates that the user and device are safe, then the authentication model may use an additional authentication factor (analogous to claim limitation “less than second threshold”). If the risk score for the device or the user is above the threshold such that it indicates that the user or the device is compromised or unsafe, then the authentication model may require the additional authentication factor as a condition for access by the device to the remote resource (analogous to claim limitation “greater than first threshold”).)

Regarding claim 11, Levy in view of Stamos teaches all the features with respect to claim 10, as outlined above. The combination further teaches **wherein said permitting or denying further comprises when the risk score is greater than the second threshold, withholding the decryption key.** ([Levy 0213] if the risk score for the device or the user is above the threshold such that it indicates that the user or the device is compromised or unsafe, then the authentication model may withhold the additional authentication factor to prevent access by the device to the remote resource.)

Regarding claims 12-14, 16 and 18-20, the scope of the claims are similar to that of claims 1-3, 5 and 9-11, respectively. Accordingly, the claims are rejected using a similar rationale.

Claims 4 and 15 are rejected under 35 U.S.C. 103 as being unpatentable over Levy (US 20190319945 A1) in view of Stamos (US 20040221172 A1) and Lof (US 20140310779 A1).

Regarding claim 4, Levy in view of Stamos teaches all the features with respect to claim 1, as outlined above. But the combination does not teach wherein the observed data includes a current location of the first user as determined based on a source Internet Protocol (IP) address contained in the file access request. This aspect of the claim is identified as a difference.

However, Lof in an analogous art **explicitly** teaches **wherein the observed data includes a current location of the first user as determined based on a source Internet Protocol (IP) address contained in the file access request.** ([0130] the media content provider can use geo-location techniques to determine a geographic location of the client device (e.g., the country in which the client device resides). Such techniques include using the IP address of the client device (which can be determined from an HTTP request, for example) to lookup the user's probable location in an IP address

database.)

It would have been prima facie obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to combine the “dynamic authentication” concept of Levy, and the “geo-location techniques using IP address” approach of Lof. One of ordinary skill in the art would have been motivated to perform such a modification to provide efficient and secure access to content by obtaining information about the client device that is not explicitly provided or reported by the client device, but available through the communication between the client device and the content provider (Lof [0130, 0010]).

Regarding claim 15, the scope of the claim is similar to that of claim 4, respectively. Accordingly, the claim is rejected using a similar rationale.

Claims 8 and 17 are rejected under 35 U.S.C. 103 as being unpatentable over Levy (US 20190319945 A1) in view of Stamos (US 20040221172 A1) and Pigin (US 20050229258 A1).

Regarding claim 8, Levy in view of Stamos teaches all the features with respect to claim 1, as outlined above. But the combination does not teach wherein the encrypted form involves the file being encapsulated in a cryptographic wrapper. This aspect of the claim is identified as a difference.

However, Pigin in an analogous art **explicitly teaches wherein the encrypted form involves the file being encapsulated in a cryptographic wrapper.** ([0230] These operations manipulate cryptographic objects at the file level. File-level wrappers are based on the crypto container concept. All cryptographic objects, associated with a single original file, are encapsulated into a single file of compound structure (cryptocontainer).)

It would have been prima facie obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to combine the “dynamic authentication” concept of Levy, and the “file level wrappers” approach of Pigin. One of ordinary skill in the art would have been motivated to perform such a modification to provide secure and efficient document rights management and file encryption (**Pigin [0001, 0004]**).

Regarding claim 17, the scope of the claim is similar to that of claim 8, respectively. Accordingly, the claim is rejected using a similar rationale.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- US 20110126293 A1, "System and method for contextual and behavioral based data access control", by Berengoltz, teaches controlling access to information. An encrypted version of the information is stored. An attempt to access encrypted information may be intercepted and an access authorization rank may be computed. If computed access authorization rank is above a predefined level then a decrypted version of the information may be provided.
- US 8688980 B2, "Trust verification schema based transaction authorization", by Davis, teaches for determining one or more behavioral fingerprints associated with one or more network accessible users; relationally mapping the one or more behavioral fingerprints to generate a trust verification schema associated with the one or more network accessible users; and determining whether to authenticate one or more transactions via the trust verification schema.

- US 20110016534 A1, "Implicit authentication", by Jakobsson, teaches method and system for implicitly authenticating a user to access controlled resources. The system receives a request to access the controlled resources. The system then determines a user behavior score based on a user behavior model, and recent contextual data about the user. The user behavior score facilitates identifying a level of consistency between one or more recent user events and a past user behavior pattern. The recent contextual data, which comprise a plurality of data streams, are collected from one or more user devices without prompting the user to perform an action explicitly associated with authentication. The plurality of data streams provide basis for determining the user behavior score, but a data stream alone provides insufficient basis for the determination of the user behavior score. The system also provides the user behavior score to an access controller of the controlled resource.
- US 20210176264 A1, "Leveraging user-behavior analytics for improved security event classification", by Yavo, teaches improving security event classification by leveraging user-behavior analytics are provided. According to an embodiment, a UEBA-based security event classification service of a cloud-based security platform maintains information regarding historical user behavior of various users of an enterprise network. An endpoint protection platform running on an endpoint device that is part of the enterprise network performs an initial classification of the event, based on which the endpoint protection platform blocks activity by the process. The endpoint production platform requests input from the cloud-based security platform which causes the cloud-based security platform performs a reclassification of the event based on contextual information, multiple data feeds and the UEBA-based security event classification service. Based on the reclassification of the event, the cloud-based security platform

causes the endpoint protection platform to allow the process to proceed by providing the resulting security event classification to the endpoint protection platform.

- US 20200195672 A1, "Analyzing user behavior patterns to detect compromised nodes in an enterprise network", by Mugambi, teaches analyzing user behavior patterns to detect compromised computing devices in an enterprise network are provided. According to one embodiment, an enforcement engine running on a network security device, identifies top users of a network exhibiting a suspicious behavior relating to login failures by determining a first set of users having a number of login failure events during a given time duration exceeding a threshold. The enforcement engine identifies from the first set of computers associated with the top users, a second set of computers exhibiting a suspicious behavior relating to new connections exceeding a threshold. The enforcement engine classifies a third set of computers, representing a subset of the second set exhibiting a suspicious behavior relating to consecutive new connections, as compromised source computers when their respective new connections are in a sequence that results in a Shannon entropy measure exceeding a threshold.
- US 20160261606 A1, "Location-based network security", by Salvador, teaches providing a location-aware firewall and/or a network security/gateway device that can authorize and/or deny access of a secured resource to a requester/user based on one or more rules related to physical location and/or IP address tagged geo-location of the user's device.
- CN 112491876 A, "Geographic position access control method and device", by Zhang, teaches acquiring an IP address of an access request; determining a geographic location of the access request based on the IP address, the geographic location including a country or province or city; comparing the geographic location to a plurality of masks in

a restricted zone mask table; and when the comparison result has a matching result, limiting the access of the IP address of the access request.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HAN YANG whose telephone number is (408)918-7638. The examiner can normally be reached on Monday to Friday, 9:00-5:00.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Carl Colin can be reached on 571-272-3862. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/H.Y./
Examiner, Art Unit 2493

/CARL G COLIN/
Supervisory Patent Examiner, Art Unit 2493

Notice of References Cited	Application/Control No. 16/362,167		Applicant(s)/Patent Under Reexamination Little et al.	
	Examiner HAN YANG		Art Unit 2493	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20190319945-A1	10-2019	Levy; Joseph H.	G06F21/6218	1/1
*	B	US-20040221172-A1	11-2004	Stamos, Nicholas	H04L63/10	726/27
*	C	US-20050229258-A1	10-2005	Pigin, Vlad	H04L63/0428	726/27
*	D	US-20110126293-A1	05-2011	Berengoltz; Pavel	G06F21/62	726/26
*	E	US-8688980-B2	04-2014	Davis; Marc E.	G06F21/88	713/166
*	F	US-20110016534-A1	01-2011	Jakobsson; Bjorn Markus	H04L67/22	726/28
*	G	US-20210176264-A1	06-2021	Yavo; Udi	H04L63/1416	1/1
*	H	US-20200195672-A1	06-2020	Mugambi; Ernest	H04L41/142	1/1
*	I	US-20140310779-A1	10-2014	Lof; Henrik Tobias	G06F21/10	726/4
*	J	US-20160261606-A1	09-2016	SALVADOR; MART N HUMBERTO HOZ	H04L63/02	1/1
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N	CN-112491876-A	03-2021	CN	Zhang	
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Dale Sutherland, "Wired vs Wireless Networking", https://aberdeencybersecurity.co.uk/wired-vs-wireless-networking , 02/12/2018, Aberdeen Cyber Security, 2 pages (Year: 2018)
	V	Sue Marquette Poremba, "How a VPN Can Boost Your Security and Privacy", https://www.tomsguide.com/us/-vpn-for-beginners,news-17514.html , October 29, 2018, Tom's Guide, 5 pages (Year: 2018)
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes 	Application/Control No. 16/362,167	Applicant(s)/Patent Under Reexamination Little et al.
	Examiner HAN YANG	Art Unit 2493

CPC - Searched*		
Symbol	Date	Examiner
G06F 21/6218 21/602 21/316	09/25/2021	HY
G06F 16/182	09/25/2021	HY
G06N 20/00	09/25/2021	HY
H04L 9/0819	09/25/2021	HY

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

/H.Y./ Examiner, Art Unit 2493	
-----------------------------------	--

<i>Search Notes</i> 	Application/Control No. 16/362,167	Applicant(s)/Patent Under Reexamination Little et al.
	Examiner HAN YANG	Art Unit 2493

Search Notes		
Search Notes	Date	Examiner
G06F 21/6218 21/602 21/316	09/25/2021	HY
G06F 16/182	09/25/2021	HY
G06N 20/00	09/25/2021	HY
H04L 9/0819	09/25/2021	HY
Classification with text search.	09/25/2021	HY
EAST text search (see search history printout).	09/25/2021	HY
Inventor and applicant search EAST.	09/22/2021	HY
IDS references considered.	09/22/2021	HY
google patent and NPL search.	09/24/2021	HY
Include feedback from SPE.	09/27/2021	HY

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/H.Y./ Examiner, Art Unit 2493	
-----------------------------------	--

<i>Index of Claims</i> 	Application/Control No. 16/362,167	Applicant(s)/Patent Under Reexamination Little et al.
	Examiner HAN YANG	Art Unit 2493

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS										
☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47										
CLAIM		DATE								
Final	Original	09/25/2021								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)

Approved for use through 11/30/2020. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	16362167
	Filing Date	2019-03-22
	First Named Inventor	Matthew J. Little
	Art Unit	2139
	Examiner Name	
	Attorney Docket Number	FORT-031800

U.S.PATENTS							Remove	
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear		
	1	8595497		2013-11-26	Dogu et al.			
	2	8887274		2014-11-11	Buchanan et al.			
If you wish to add additional U.S. Patent citation information please click the Add button.							Add	
U.S.PATENT APPLICATION PUBLICATIONS							Remove	
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear		
	1	20180069881		2018-03-18	Graves et al.			
	2	20180351979		2018-12-06	Mandrychenko et al.			
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add	
FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²ⁱ	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16362167
Filing Date	2019-03-22
First Named Inventor	Matthew J. Little
Art Unit	2139
Examiner Name	
Attorney Docket Number	FORT-031800

If you wish to add additional Foreign Patent Document citation information please click the Add button		Add
NON-PATENT LITERATURE DOCUMENTS		Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.
	1	Kerr, O.S., et al. "Encryption Workarounds." The Georgetown Law Journal. Vol. 106:989 2018. pgs 989-1019.
	2	FinalCode. How FinalCode Works. http://www.finalcode.com/jp/english/about/mechanism/ . 2 pgs.
If you wish to add additional non-patent literature document citation information please click the Add button		Add
EXAMINER SIGNATURE		
Examiner Signature	/HAN YANG/	Date Considered 09/22/2021
<p>*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.</p>		
<p>¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.</p>		

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16362167
Filing Date	2019-03-22
First Named Inventor	Matthew J. Little
Art Unit	2139
Examiner Name	
Attorney Docket Number	FORT-031800

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Michael A. DeSanctis/	Date (YYYY-MM-DD)	2019-04-12
Name/Print	Michael A. DeSanctis	Registration Number	39957

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Bibliographic Data

Application No: 16/362,167

Foreign Priority claimed: ☐ Yes ☒ No

35 USC 119 (a-d) conditions met: ☐ Yes ☒ No ☐ Met After Allowance

Verified and Acknowledged:

/HAN YANG/

Examiner's Signature

Initials

Title:

FILE ACCESS CONTROL BASED ON ANALYSIS OF USER
BEHAVIOR PATTERNS

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
03/22/2019	713	2493	FORT-031800(18167)
RULE			

APPLICANTS

Fortinet, Inc., Sunnyvale, CA, UNITED STATES

INVENTORS

Matthew J. Little, Loanhead, UNITED KINGDOM

Jamie R. Graves, Edinburgh, UNITED KINGDOM

Carson Leonard, Edinburgh, UNITED KINGDOM

CONTINUING DATA

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

STATE OR COUNTRY

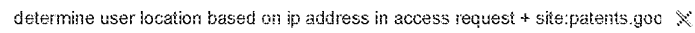
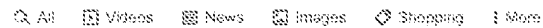
UNITED KINGDOM

ADDRESS

Douglas M. Hamilton
HDC Fortinet
224 S. Main Street, 114
Springville, UT 84663
UNITED STATES

FILING FEE RECEIVED

\$1,720



About 104,000 results (0.55 seconds)

<https://patents.google.com/patent> 3

A database correlating the geographic locations of users of a network to the network address through which the users access the network is maintained and ...

<https://patents.google.com/patent>

Based on the detected network or networks, the device determines a current location. The device then accesses a usage data store to determine whether the access ...

<https://patents.google.com> > patent &

A method of determining a geographical location from IP address information comprising: interrogating a database of IP address information mapped to domain ...

<https://patents.google.com> : patent

A method of determining a geographic location of an Internet user involves determining if the host is on-line, determining ownership of the host name, ...

<https://patents.google.com/patent>

The method may include relating an IP address to an intermediate identifier, ... correlating a specific physical address to a user's internet access point, ...

<https://patents.google.com/patent>

A geographical location of the user device is determined by the network ... with IP address and/or location specific details of requesting user devices 202.

<https://patents.google.com> : patent §

The identity server processes the authentication request, by validating the combination of the user identity and the network access point identity, ...

<https://patents.google.com/patent>

Hash-based puzzles are based on puzzles that require a client to reverse a ... as determined by the server before being allowed access to the server.

<https://patents.google.com/patent> 3

System for verifying access based on a determined geographic location of a ... of on-line users and creating a database with IP addresses and corresponding ...

<https://patents.google.com> : patent §

The method further includes determining a geographical location of the computing ... with a specific computing device via an Internet protocol (IP) address, ...

<https://patents.google.com/patent> 3

Geographically based access management for internet of ...

For example, a user may provide location data, such as an address or ... processing a request for IoT device data with geographically-based access controls.

<https://patents.google.com/patent/>

Location based authentication of mobile device transactions

To determine the location of client computing device 101, bank system 104 may determine the IP address of client computing device 101 and cross reference ...

<https://patents.google.com/patent/>

Geo-location and geo-compliance utilizing a client agent

IP geolocation may refer to a set of techniques that determine the location of a web visitor based on their associated IP address

<https://patents.google.com/patent/>

EP2399367A1 - Location-based ims server selection - Google ...

A user location is estimated based on an IP address assigned to the user's device/equipment during registration for multimedia application services that are ...

<https://patents.google.com/patent/>

Determining and utilizing one or more attributes of IP addresses

Attributes are determined based on request data provided with requests from ... only by an IP address (e.g., cookies have been disabled and the user is not ...

<https://patents.google.com/patent/>

US8990356B2 - Adaptive name resolution - Google Patents

Other servers may use the source IP address to approximate the location ... the user, allowing access to member only or user specific resources.

<https://patents.google.com/patent/>

Determining the precise geolocation of a wireless internet target

Sep 17, 2015 --- Other geolocation efforts may then be used to scope the internet user's ... (b) the ability to roughly geolocate a target's IP address; and,

<https://patents.google.com/patent/>

US7092943B2 - Location based data - Google Patents

Data is provided with location-based access control information, ... and link information, MAC address, IP address, a timestamp, and activity staleness.

<https://patents.google.com/patent/>

US5684951A - Method and system for user authorization over ...

If the user identification is valid but the current IP address is not authorized, the application determines a validation key ("key") based on the user ...

<https://patents.google.com/patent/>

Systems and methods for managing location data and ...

The user interface can be configured to allow a user to view, manage, ... and third party access to location data in the context of internet-protocol (IP) ...

Related searches

geolocation

how to track an ip address

ip info

how to find an ip address

Google

file access control based on user behavior pattern + site:patents.google.com

[All](#)
[Videos](#)
[Images](#)
[News](#)
[Shopping](#)
[More](#)
[Tools](#)

About 77,800 results (0.61 seconds)

<https://patents.google.com/patent/>

US20120222132A1 - Permissions Based on Behavioral Patterns ...

Users may choose to have their behavior analyzed in order to infer default sharing permission settings for documents and other information maintained in one .

<https://patents.google.com/patent/>

CN102999572B - User's behavior pattern mining system and ...

Described Webpage log processing module, is characterized in that, Webpage log information is stored by XML file, stores the access log record that passing user ...

<https://patents.google.com/patent/>

Detecting behavioral patterns and anomalies using activity data

Further, the operating system checks permissions for file accesses based only on user and it does not restrict file accesses based on application programs.

<https://patents.google.com/patent/>

CN105516127A - Internal threat detection-oriented user cross ...

The invention belongs to information security technology, user behavior analysis ... 6. based on the effect of visualization of the user behavior pattern ...

<https://patents.google.com/patent/>

Characterizing user behavior via intelligent identity analytics

The concept of Adaptive Authentication and Access Control is being actively researched, but is unaware of any research that is applying data/information ...

<https://patents.google.com/patent/>

Ranking documents based on user behavior and/or feature data

A system generates a model based on feature data relating to different features of a link from a linking document to a linked document and user behavior ...

<https://patents.google.com/patent/>

System level user behavior biometrics using feature extraction ...

G66F21/316 User authentication by observing the pattern of computer usage, ... and enforce security policies, are fundamentally built upon a system of ...

<https://patents.google.com/patent/>

Behavior-based traffic profiling based on access control ...

for selecting and monitoring traffic flows, and detecting deviations or anomalies based on traffic behavior patterns associated with user information, role ...

<https://patents.google.com/patent/>

Detecting unauthorized use of computing devices based on ...

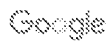
Acceptable behaviorist pattern data can be generated for a computing system ... critical or basic system calls, such as, those required for opening files and ...

<https://patents.google.com/patent/>

US10171488B2 - User behavior profile - Google Patents

Likewise, cyber security approaches have included network access controls, ... use a user device 230 to download a data file from a particular system 254.

<https://patents.google.com/patent/>



file access control based on user behavior pattern + site:patents.google.com
 Network threat detection and management system based on ...

The behavior may relate to one or more requests, from a client device being used by the first user, to access a network resource. The device may determine, ...

<https://patents.google.com/patent/>

Generating notifications based on user behavior - Google ...

For example, the system 100 may determine behavior patterns of a mobile device over time based on historical behavior data and compare current behavior data ...

<https://patents.google.com/patent/>

Automatic management of storage access control - Google ...

A typical proposal for role-based access controls in a multi-user SQL ... includes deriving patterns of usage of the file system by the users from the ...

<https://patents.google.com/patent/>

Dynamic user behavior rhythm profiling for privacy preserving ...

An anonymous user may be identified and categorized based on rhythms of predictive behavior pattern sequences by extracting signatures the rhythms to ...

<https://patents.google.com/patent/>

Method and system for providing authentication through ...

May 6, 2010 ... identification of a user based on behavioral patterns and time patterns, ... Therefore, biometric access control systems are used to ...

<https://patents.google.com/patent/>

Method and apparatus for implementing digital video ...

Thereafter, the process forms a set of unexpected behavioral patterns from ... By observing this unexpected behavior, security personnel may perform a more ...

<https://patents.google.com/patent/>

US20070272744A1 - Detection and visualization of patterns ...

Unusual access patterns are detected from the data in the log file based on the ... For example, access control cards can be based on proximity sensing ...

<https://patents.google.com/patent/>

Behavioral profiling method and system to authenticate a user

Variations between the behavioral characteristics of the user ... and a behavioral profile previously developed based on prior usage patterns of the user ...

<https://patents.google.com/patent/>

US20110016534A1 - Implicit authentication - Google Patents

The system receives a request to access the controlled resources. The system then determines a user behavior score based on a user behavior model, ...

<https://patents.google.com/patent/>

US20120216277A1 - User profile and usage pattern based ...

Embodiments of the present invention provide method, system and computer program product for user profile and usage pattern based user ID prediction.

1 2 3 4 5 6 7 8 9 10 Next

Fairfax County, Virginia - Based on your past activity - Update location

[Help](#) [Send feedback](#) [Privacy](#) [Terms](#)

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	692	((("Fortinet") near3 ("Inc"))).AS,AANM.	USPAT	OR	ON	2021/09/22 16:35
S2	1,399	((("Fortinet") near3 ("Inc"))).AS,AANM.	US-PGPUB; USPAT; USOCR	OR	ON	2021/09/22 16:39
S3	34	((("LITTLE") near3 ("Matthew")) OR ((("GRAVES") near3 ("Jamie")) OR ((("LEONARD") near3 ("Carson")))).INV.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	ON	2021/09/22 16:39
S4	19	S2 and (behavior near pattern\$)	US-PGPUB; USPAT; USOCR	OR	ON	2021/09/22 16:46
S5	10	S2 and (behavior near user)	US-PGPUB; USPAT; USOCR	OR	ON	2021/09/22 19:27
S6	4	("20180069881" "20180351979" "8595497" "8887274").PN.	US-PGPUB; USPAT	OR	ON	2021/09/22 21:16
S7	9	(pattern\$ histor\$4) near2 user near2 (behavior behaviour) with (file near2 access)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/09/22 21:45
S8	41	(pattern\$ histor\$4) near2 (behavior behaviour) with (file near2 access)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/09/22 22:33
S9	115	user near2 (behavior behaviour) with (file near2 access)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/09/23 14:55
S10	1	(cryptograph\$2 crypto) with wrapper with encapsulat\$3 with file with encrypt\$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/09/25 13:11
S11	2	(cryptograph\$2 crypto) with wrapper with encapsulat\$3 with file	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/09/25 13:12

S12	30	(cryptograph\$2 crypto) with wrapper with file	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/09/25 13:12
S13	50	(pattern\$ histor\$4) with user with (behavior behaviour) with (file near2 access)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/09/25 17:10
S14	195,165	(G06F21/6218 or G06F16/182 or G06N20/00 or H04L9/0819 or G06F21/602 or G06F21/316).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/09/25 17:11
S15	9	S13 and S14	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/09/25 17:11
S16	102	(pattern\$ histor\$4) with user with (behavior behaviour) same (file near2 access)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/09/25 17:11
S17	39	S16 and S14	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/09/25 17:12
S18	3	user same (access near2 request) same (file near2 access) same (risk near2 score)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/09/25 17:35
S19	261	determin\$6 with user near4 locat\$3 with based with ip near address with request	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/09/27 14:10
S20	22	determin\$6 with user near4 locat\$3 with based with ip near address with (access near2 request)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/09/27 14:12
S21	54	determin\$6 with locat\$3 with based with ip near address with (access near2 request)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2021/09/27 15:27

			DERWENT; IBM_TDB			
S22	0	correlat\$3 with locat\$3 with based with ip near address with (access near2 request)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/09/27 16:57

EAST Search History (Interference)

<This search history is empty>

9/28/2021 10:50:00 AM

C:\Users\hyang1\Documents\EAST\Workspaces\16362167.wsp

Geographic position access control method and device

Abstract

The disclosure relates to a method and a device for controlling access to a geographic location, an electronic device and a computer readable medium. The method comprises the following steps: acquiring an IP address of an access request; determining a geographic location of the access request based on the IP address, the geographic location including a country or province or city; comparing the geographic location to a plurality of masks in a restricted zone mask table; and when the comparison result has a matching result, limiting the access of the IP address of the access request. The geographic position access control method, the geographic position access control device, the electronic equipment and the computer readable medium can obtain the geographic position access control result more quickly, and especially for some high-performance scenes, compared with a traditional mode, the mode disclosed by the disclosure has higher performance.

Classifications

⌘ H04L63/187 Network architectures or network communication protocols for network security for controlling access to network resources wherein the security policies are location-dependent, e.g. entities privileges depend on current location or allowing specific operations only from locally connected terminals

[View 2 more classifications](#)

CN112491876A

China

[Download PDF](#)

[Find Prior Art](#)

[Similar](#)

Other languages: Chinese

Inventor: 张长顺, 吴庆, 王树太, 田登奥

Current Assignee : Hangzhou DPTech Technologies Co Ltd

Worldwide applications

2020 [CN](#)

Application CN202011348079.9A events ⓘ

2020-11-26 Application filed by Hangzhou DPTech Technologies Co Ltd

2020-11-26 Priority to CN202011348079.9A

2021-03-12 Publication of CN112491876A

Status Pending

Info: Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (10)

[Hide Dependent](#) ^

1. A method for controlling access to a geographic location, comprising:

acquiring an IP address of an access request;

determining a geographic location of the access request based on the IP address, the geographic location including a country or province or city;

comparing the geographic location to a plurality of masks in a restricted zone mask table;

and when the comparison result has a matching result, limiting the access of the IP address of the access request.

2. The method of claim 1, further comprising:

and generating the limited region mask table based on names, region identifications and masks corresponding to a plurality of geographic positions.

3. The method of claim 2, wherein generating the restricted zone mask table based on names, zone identifications, and masks corresponding to a plurality of geographic locations comprises:

deleting the range overlapping area in the matching table of the limited area;

generating an identification of a region in the restricted region matching table;

generating a mask of regions in the restricted region matching table;

and generating the limited region mask table based on the identification of the region and the corresponding mask thereof.

4. The method of claim 3, wherein generating an identification of a locale in the restricted locale matching table comprises:

uniformly coding the names of countries, provinces and cities in the geographic position;

and respectively allocating identifications for the names of the country, the province and the city based on the codes.

5. The method of claim 3, wherein generating a mask that restricts the regions in the region matching table comprises:

determining a mask generation mode according to the type of the region;

and respectively distributing masks for the names of the country, the province and the city based on the generation mode.

6. The method of claim 1, wherein comparing the geographic location to a plurality of masks in a restricted zone mask table comprises:

determining an identifier in the restricted area mask table according to the geographic position;

bitwise operations are performed on each of a plurality of masks in the geographic location and restricted zone mask table for comparison.

7. The method of claim 1, wherein when there is a match in the comparison results, comprising:

judging whether the comparison result is the same as the area identification or not;

a match is determined when the two are the same.

8. The method of claim 1, further comprising:

and processing the access request when the comparison result does not have a matching result.

9. An access control device for a geographic location, comprising:

the request module is used for acquiring the IP address of the access request;

an address module to determine a geographic location of the access request based on the IP address, the geographic location including a country or province or city;

a comparison module for comparing the geographic location with a plurality of masks in a restricted area mask table;

and the limiting module is used for limiting the access of the IP address of the access request when the comparison result has a matching result.

10. The apparatus of claim 9, further comprising:

and the mask table module is used for generating the restricted area mask table based on the names, the area identifications and the masks corresponding to the plurality of geographic positions.

Description

Geographic position access control method and device

Technical Field

The present disclosure relates to the field of computer information processing, and in particular, to a method and an apparatus for controlling access to a geographic location, an electronic device, and a computer-readable medium.

Background

With the development of network technology, attacks on various networks are more and more frequent, and in order to count the sources of the attacks and limit the geographical location to which the IP address generating the attacks belongs, the IP address generating the attacks needs to be converted into the geographical location, and a policy is made to perform access control on the geographical location generating the attacks. The general method is to generate a restricted area table according to the access control requirement, then convert the IP address into a geographical location, and determine whether the geographical location is in the restricted area table, if so, the access control is performed on the IP address.

The geographical location and the restricted area may be a country, a province (generally, the next administrative unit of the country, such as province, municipality, prefecture, and special administrative district, which is uniformly expressed by province), or a city (generally, the next administrative unit of the province, such as prefecture, municipality, and municipality, which is uniformly expressed by city).

In the prior art, three comparison operations are required for access control of an IP address, and in some high-performance scenes, the mode matching speed in the prior art is slow, and the performance is poor.

Therefore, a new method, apparatus, electronic device and computer readable medium for controlling access to a geographic location is needed.

The above information disclosed in this background section is only for enhancement of understanding of the background of the disclosure and therefore it may contain information that does not constitute prior art that is already known to a person of ordinary skill in the art.

Disclosure of invention

In view of the above, the present disclosure provides a method and an apparatus for controlling access to a geographic location, an electronic device, and a computer readable medium, which can obtain a result of controlling access to the geographic location faster, especially for some high performance scenarios, compared to the conventional approach, the performance of the approach in the present disclosure is higher.

Additional features and advantages of the disclosure will be set forth in the detailed description which follows, or in part will be obvious from the description, or may be learned by practice of the disclosure.

According to an aspect of the present disclosure, a method for controlling access to a geographic location is provided, the method including: acquiring an IP address of an access request; determining a geographic location of the access request based on the IP address, the geographic location including a country or province or city; comparing the geographic location to a plurality of masks in a restricted zone mask table; and when the comparison result has a matching result, limiting the access of the IP address of the access request.

In an exemplary embodiment of the present disclosure, further comprising: and generating the limited region mask table based on names, region identifications and masks corresponding to a plurality of geographic positions.

In an exemplary embodiment of the present disclosure, generating the restricted geographic mask table based on names, geographic identifications and masks corresponding to a plurality of geographic locations includes: deleting the range overlapping area in the matching table of the limited area; generating an identification of a region in the restricted region matching table; generating a mask of regions in the restricted region matching table; and generating the limited region mask table based on the identification of the region and the corresponding mask thereof.

In an exemplary embodiment of the disclosure, generating an identification of a locale in the restricted locale matching table includes: uniformly coding the names of countries, provinces and cities in the geographic position; and respectively allocating identifications for the names of the country, the province and the city based on the

codes.

In an exemplary embodiment of the disclosure, generating a mask that restricts the regions in the region matching table includes: determining a mask generation mode according to the type of the region; and respectively distributing masks for the names of the country, the province and the city based on the generation mode.

In an exemplary embodiment of the disclosure, comparing the geographic location to a plurality of masks in a restricted zone mask table includes: determining an identifier in the restricted area mask table according to the geographic position; bitwise operations are performed on each of a plurality of masks in the geographic location and restricted zone mask table for comparison.

In an exemplary embodiment of the present disclosure, when there is a matching result in the comparison results, the method includes: judging whether the comparison result is the same as the area identification or not; a match is determined when the two are the same.

In an exemplary embodiment of the present disclosure, further comprising: and processing the access request when the comparison result does not have a matching result.

According to an aspect of the present disclosure, an access control apparatus for a geographic location is provided, the apparatus comprising: the request module is used for acquiring the IP address of the access request; an address module to determine a geographic location of the access request based on the IP address, the geographic location including a country or province or city; a comparison module for comparing the geographic location with a plurality of masks in a restricted area mask table; and the limiting module is used for limiting the access of the IP address of the access request when the comparison result has a matching result.

In an exemplary embodiment of the present disclosure, further comprising: and the mask table module is used for generating the restricted area mask table based on the names, the area identifications and the masks corresponding to the plurality of geographic positions.

According to an aspect of the present disclosure, an electronic device is provided, the electronic device including: one or more processors; storage means for storing one or more programs; when executed by one or more processors, cause the one or more processors to implement a method as above.

According to an aspect of the disclosure, a computer-readable medium is proposed, on which a computer program is stored, which program, when being executed by a processor, carries out the method as above.

According to the access control method, the access control device, the electronic equipment and the computer readable medium of the geographic position, an IP address of an access request is obtained; determining a geographic location of the access request based on the IP address, the geographic location including a country or province or city; comparing the geographic location to a plurality of masks in a restricted zone mask table; when the comparison result has a matching result, the method for limiting the access of the IP address of the access request can obtain the geographic position access control result more quickly, and particularly for some high-performance scenes, the method disclosed by the disclosure has higher performance compared with the traditional method.

It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory only and are not restrictive of the disclosure.

Drawings

The above and other objects, features and advantages of the present disclosure will become more apparent by describing in detail exemplary embodiments thereof with reference to the attached drawings. The drawings described below are merely some embodiments of the present disclosure, and other drawings may be derived from those drawings by those of ordinary skill in the art without inventive effort.

FIG. 1 is a flow chart illustrating a method for access control of a geographic location according to an exemplary embodiment.

Fig. 2 is a flow chart illustrating a method of access control for a geographic location according to another exemplary embodiment.

Fig. 3 is a flow chart illustrating a method of access control for a geographic location according to another exemplary embodiment.

Fig. 4 is a diagram illustrating a method of access control for a geographic location according to another exemplary embodiment.

Fig. 5 is a diagram illustrating a method of access control for a geographic location according to another exemplary embodiment.

Fig. 6 is a diagram illustrating a method of access control for a geographic location according to another exemplary embodiment.

Fig. 7 is a diagram illustrating a method of access control for a geographic location according to another exemplary embodiment.

Fig. 8 is a diagram illustrating a method of access control for a geographic location according to another exemplary embodiment.

Fig. 9 is a diagram illustrating a method of access control for a geographic location according to another exemplary embodiment.

Fig. 10 is a diagram illustrating a method of access control for a geographic location according to another exemplary embodiment.

FIG. 11 is a block diagram illustrating a geo-location access control device in accordance with an exemplary embodiment.

FIG. 12 is a block diagram illustrating an electronic device in accordance with an example embodiment.

FIG. 13 is a block diagram illustrating a computer-readable medium in accordance with an example embodiment.

Detailed Description

Example embodiments will now be described more fully with reference to the accompanying drawings. Example embodiments may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the concept of example embodiments to those skilled in the art. The same reference numerals denote the same or similar parts in the drawings, and thus, a repetitive description thereof will be omitted.

Furthermore, the described features, structures, or characteristics may be combined in any suitable manner in one or more embodiments. In the following description, numerous specific details are provided to give a thorough understanding of embodiments of the disclosure. One skilled in the relevant art will recognize, however, that the subject matter of the present disclosure can be practiced without one or more of the specific details, or with other methods, components, devices, steps, and so forth. In other instances, well-known methods, devices, implementations, or operations have not been shown or described in detail to avoid obscuring aspects of the disclosure.

The block diagrams shown in the figures are functional entities only and do not necessarily correspond to physically separate entities, i.e. these functional entities may be implemented in the form of software, or in one or more hardware modules or integrated circuits, or in different networks and/or processor means and/or microcontroller means.

The flow charts shown in the drawings are merely illustrative and do not necessarily include all of the contents and operations/steps, nor do they necessarily have to be performed in the order described. For example, some operations/steps may be decomposed, and some operations/steps may be combined or partially combined, so that the actual execution sequence may be changed according to the actual situation.

It will be understood that, although the terms first, second, third, etc. may be used herein to describe various components, these components should not be limited by these terms. These terms are used to distinguish one element from another. Thus, a first component discussed below may be termed a second component without departing from the teachings of the disclosed concept. As used herein, the term "and/or" includes any and all combinations of one or more of the associated listed items.

It is to be understood by those skilled in the art that the drawings are merely schematic representations of exemplary embodiments, and that the blocks or processes shown in the drawings are not necessarily required to practice the present disclosure and are, therefore, not intended to limit the scope of the present disclosure.

The technical abbreviations of the present disclosure are explained as follows:

IP address: the IP Address is an abbreviation of Internet Protocol Address, which is a unified Address format provided by the IP Protocol, and allocates a logical Address to each network and each host on the Internet, so as to shield the difference of physical addresses. The IP address is divided into a Public address and a private address, wherein the Public address is responsible for being distributed to organizations applying for the Public address by an InterNIC (Internet Network Information Center), and the organizations can directly access the Internet through the Public address; the Private address (Private address) belongs to a non-registered address and is used exclusively for the inside of the organization.

Shaping: a basic, technical term in computers refers to data without a fractional part. The integer may be designated with a decimal, hexadecimal or octal symbol, preceded by an optional symbol (-or +). The method comprises an integer constant and an integer variable, wherein the integer variable comprises a short integer, a basic integer and a long integer, the short integer, the basic integer and the long integer are divided into two versions, namely a signed version and an unsigned version, and the method is an intelligent calculation mode.

Hexadecimal system: hexadecimal (abbreviated hex or subscript 16) is a carry system in mathematics for a stride of 1 into 16. Generally represented by the numbers 0 to 9 and the letters A to F (or a to f), wherein A to F represent 10 to 15, these being referred to as hexadecimal numbers.

According to the bit sum: the bitwise and operator "&" is a binocular operator. Its function is to take part in the binary AND of the two numbers respectively corresponding to the operation. The result bit is 1 only if both corresponding bins are 1. Both numbers participating in the operation appear complementary. The integer is represented by binary bits in a computer, and the C language provides that some operators can directly operate on the bits in the integer, which are called bit operations, and operands of the operators are required to be integer.

The existing scheme is as follows:

firstly, establishing three restricted area tables according to the three levels of states, provinces and cities according to access control requirements;

second, the IP address is translated to a geographic location, which may be a country, province, or city.

Finally, whether the country to which the geographic position belongs exists in the country list or not is judged, and if yes, the countries are matched; judging whether the province to which the geographical position belongs exists in the province list or not, and if so, indicating province matching; and then judging whether the city to which the geographic position belongs exists in the city list, if so, indicating that the geographic position exists in the configured restricted area table, and needing to execute an access control strategy on the IP address.

The scheme in the prior art judges whether a certain geographic position needs to be compared for three times in a restricted area table, and for some high-performance scenes, the matching speed is low and the performance is poor. In the scheme of the present disclosure, three levels of country, province and city are organized into a region ID (generally, 32-bit unsigned integer in computer language), and the region ID is from high to low, country, province and city, respectively, as shown in table 1. The method and the device use the form of the mask to carry out quick judgment, and only need to carry out judgment once to obtain a result.

TABLE 1 area ID storage content

State of the country	Economic	City (R)
----------------------	----------	----------

FIG. 1 is a flow chart illustrating a method for access control of a geographic location according to an exemplary embodiment. The method 10 for access control of a geographical location comprises at least steps S102 to S108.

As shown in fig. 1, in S102, the IP address of the access request is acquired.

In S104, a geographic location of the access request is determined based on the IP address, the geographic location including a country or province or city. The IP address is translated to a geographic location, which may be a country, province, or city.

In S106, the geographic location is compared to a plurality of masks in a restricted area mask table. The method comprises the following steps: determining an identifier in the restricted area mask table according to the geographic position; bitwise operations are performed on each of a plurality of masks in the geographic location and restricted zone mask table for comparison.

In S108, when there is a matching result in the comparison result, the access of the IP address of the access request is restricted. More specifically, whether the comparison result is the same as the area identifier is judged; a match is determined when the two are the same.

In S110, when there is no matching result in the comparison result, the access request is processed. More specifically, whether the comparison result is the same as the area identifier is judged; a mismatch is determined when not identical.

According to the access control method of the geographic position, an IP address of an access request is obtained; determining a geographic location of the access request based on the IP address, the geographic location including a country or province or city; comparing the geographic location to a plurality of masks in a restricted zone mask table; when the comparison result has a matching result, the method for limiting the access of the IP address of the access request can obtain the geographic position access control result more quickly, and particularly for some high-performance scenes, the method disclosed by the disclosure has higher performance compared with the traditional method.

It should be clearly understood that this disclosure describes how to make and use particular examples, but the principles of this disclosure are not limited to any details of these examples. Rather, these principles can be applied to many other embodiments based on the teachings of the present disclosure.

Fig. 2 is a flow chart illustrating a method of access control for a geographic location according to another exemplary embodiment. The process 20 shown in fig. 2 is a detailed description of the process 10 of fig. 1.

As shown in fig. 2, in S202, the IP address is converted into a geographical location.

In S204, one entry in the restricted area mask table is acquired.

In S206, the mask and the geographic location in this entry are bitwise and operated.

In S208, it is determined whether the previous step result is the same as the area ID.

In S210, whether or not all the areas in the area table have been processed is restricted.

In S212, there is no match.

In S214, matching is performed.

Firstly, constructing a disordered limited region table with range overlapping into an ordered limited region ID table without range overlapping, wherein the table consists of a plurality of region IDs; and calculating the mask of each region according to the type of the restricted region to obtain a restricted region mask table, wherein the mask table consists of the region ID and the region mask. The matching process first converts the IP address into a geographic location, which may be a country, province, or city; and circularly processing each item in the restricted area mask table, calculating whether the result of bitwise AND of the physical position and the mask of each item is the same as the area ID of the item, and if the result is the same, indicating that the physical position exists in the restricted area mask table and the access control of the IP address is required.

Fig. 3 is a flow chart illustrating a method of access control for a geographic location according to another exemplary embodiment. The flow 30 shown in fig. 3 is a detailed description of "generating the restricted geographic mask table based on names, geographic identifications, and masks corresponding to a plurality of geographic locations". More specifically, the method can comprise the following steps: deleting the range overlapping area in the matching table of the limited area; generating an identification of a region in the restricted region matching table; generating a mask of regions in the restricted region matching table; and generating the limited region mask table based on the identification of the region and the corresponding mask thereof.

As shown in fig. 3, in S302, the area where the range is overlapped is deleted. The region in which the range overlaps in the restricted region table is deleted. If a certain area is a country, deleting all provinces and cities under the jurisdiction of the country; if a certain area is province, deleting all cities under the jurisdiction of the area.

In S304, one area in the restricted area table is acquired.

In S306, the area name is converted into an area identifier according to the serial number of country, province, city. Uniformly coding all countries, provinces and cities, and converting the restricted area table into a restricted area ID table. If a certain area is a country, only the serial number of the country is filled in the country position; if a certain area is province, a country serial number needs to be filled in a country position, and a province serial number needs to be filled in a province position; if a certain region is a city, the country serial number, province serial number and city serial number are filled in the country position, province position and city position. After the conversion is finished, sorting the restricted area ID table according to the size of the area ID.

In S308, a mask of the region is determined according to the country, province, city type. Different masks are calculated according to different region types, and the calculation method comprises the following steps: if the region is a country, the national bit is 1, and the provincial and municipal bit is 0; if the area is province, the national bit and the province bit are both 1, and the city bit is 0; if the region is city, the bits of the country, province and city are all 1. The region ID and the calculated mask are combined into a restricted region mask table.

In S310, whether or not all the areas in the area table have been processed is restricted.

In S312, the process ends.

The detailed technical scheme of the disclosure is illustrated by specific examples below:

the restricted area table and the area code table are shown in fig. 4, the restricted area may have three types of countries, provinces, and cities, and the area code table lists only a part of areas for reasons of space, in which the number of areas of the same type cannot be repeated, but the number of areas of different types may be repeated.

The construction process is as follows:

the method comprises the following steps: deleting regions having range overlap in restricted region configuration table

Since the Shijiazhuang city is a prefecture-level city in Hebei province and conflicts with the scope of Hebei province, the Shijiazhuang is deleted. Luoyang was deleted because Luoyang was the prefecture city in Henan province and conflicts with the range of Henan province.

Step two: converting a restricted area table to a restricted area ID table

The region ID is represented by a 32-bit unsigned integer in this example, with the country field accounting for the top 8 bits, the province field accounting for the second highest 8 bits, and the city field accounting for the next lowest 16 bits. First, the "Hebei" is processed, the country is China, the serial number is 1, province is Hebei, the serial number is 1, the city is 0, so the area ID is 0x 01010000. Next, the country of "Jinan" is China, with serial number 1, Shandong province, 2, Jinan city, and 2, so the region ID is 0x 01020002. The "Korea" is processed again, the country is Korea, the serial number is 2, province and city are both 0, so the area ID is 0x 02000000. By analogy, a restricted region ID table can be obtained, and after the region IDs are sorted in order from small to large, an ordered restricted region ID table can be obtained, as shown in fig. 5.

Step three: calculating a mask and obtaining a restricted area mask table

First, processing the river north, the type is province, the national and provincial bit is 1, the city bit is 0, the country and province occupy 16 bits, so the mask is 0xffff 0000. The second process is "Jinan", which is the type of City, and the bits of the country, province and city are all 1, so the mask is 0 xffffff. The following regions are analogized in the same way, and the Korean is finally processed, the type of the Korean is the country, the country bit is 1, the province and city bit is 0, and the mask is 0xf000000 because the country occupies 8 higher bits. The final restricted area mask table is shown in fig. 6.

Matching process:

In one embodiment, assuming that an IP address is 175.45.176.3, its geographic location is Korean after conversion, and the locale code table is looked up to obtain a locale ID of 0x02000000. The mask of each region in the restricted area mask table is bitwise and-calculated with the geographical position, and the obtained result is as shown in fig. 7, and since the Korean area ID is the same as the calculation result, it is known that the geographical position of the IP address exists in the restricted area table, and it is necessary to perform access control for the IP address.

In one embodiment, assuming that the IP address is 1.192.83.25, the geographic location is Zheng Henan, China, and the region ID is 0x01040006 by looking up the region code table. The result of bitwise and operation of the mask of each region in the restricted region mask table with the geographical position is shown in fig. 8. Since the area ID of the south of the river is the same as the calculation result, it is known that the geographical location of the IP address exists in the restricted area table, and it is necessary to perform access control on the IP address.

In one embodiment, assuming that an IP address is 59.48.112.112, its geographical location is Shanxi Jieyi in China after transformation, and the area code table is checked to obtain the area ID of 0x01030005. The mask of each region in the restricted region mask table is bitwise and-ed with the geographical position, and the obtained result is shown in fig. 9. Since the ID of no area is the same as the calculation result, it is known that the geographical location of the IP address does not exist in the restricted area table, and it is not necessary to perform access control on the IP address.

In one embodiment, assuming that a certain IP address is 60.215.135.140, the geographical location is Shandong, and the area code table is checked to obtain the area ID of 0x01020000. The mask of each region in the restricted region mask table is bitwise and-ed with the geographical location, and the obtained result is as shown in fig. 10. Since the ID of no area is the same as the calculation result, it is known that the geographical location of the IP address does not exist in the restricted area table, and it is not necessary to perform access control on the IP address.

According to the technical scheme, three levels of regions of the country, the province and the city are organized into an integer, the result can be obtained only by one-time comparison in the form of the mask, the country, the province and the city do not need to be compared respectively, the calculation steps are reduced, the result can be obtained more quickly, and particularly for some high-performance scenes, compared with the traditional mode, the performance is higher.

Those skilled in the art will appreciate that all or part of the steps implementing the above embodiments are implemented as computer programs executed by a CPU. When executed by the CPU, performs the functions defined by the above-described methods provided by the present disclosure. The program may be stored in a computer readable storage medium, which may be a read-only memory, a magnetic or optical disk, or the like.

Furthermore, it should be noted that the above-mentioned figures are only schematic illustrations of the processes involved in the methods according to exemplary embodiments of the present disclosure, and are not intended to be limiting. It will be readily understood that the processes shown in the above figures are not intended to indicate or limit the chronological order of the processes. In addition, it is also readily understood that these processes may be performed synchronously or asynchronously, e.g., in multiple modules.

The following are embodiments of the disclosed apparatus that may be used to perform embodiments of the disclosed methods. For details not disclosed in the embodiments of the apparatus of the present disclosure, refer to the embodiments of the method of the present disclosure.

FIG. 11 is a block diagram illustrating a geo-location access control device in accordance with an exemplary embodiment. As shown in fig. 11, the access control device 110 for a geographical location includes: a request module 1102, an address module 1104, a comparison module 1106, a limit module 1108, and a mask table module 1110.

The request module 1102 is configured to obtain an IP address of the access request;

an address module 1104 for determining a geographic location of the access request based on the IP address, the geographic location including a country or province or city;

a comparison module 1106 is configured to compare the geographic location with a plurality of masks in a restricted zone mask table;

the restricting module 1108 is configured to restrict access to the IP address of the access request when there is a matching result in the comparison result.

The mask table module 1110 is configured to generate the restricted geographic mask table based on the names, the geographic identifications, and the masks corresponding to the plurality of geographic locations.

According to the access control device of the geographical position, the IP address of the access request is obtained; determining a geographic location of the access request based on the IP address, the geographic location including a country or province or city; comparing the geographic location to a plurality of masks in a restricted zone mask table; when the comparison result has a matching result, the method for limiting the access of the IP address of the access request can obtain the geographic position access control result more quickly, and particularly for some high-performance scenes, the method disclosed by the disclosure has higher performance compared with the traditional method.

FIG. 12 is a block diagram illustrating an electronic device in accordance with an example embodiment.

An electronic device 1200 according to this embodiment of the disclosure is described below with reference to fig. 12. The electronic device 1200 shown in fig. 12 is only an example and should not bring any limitation to the functions and the scope of use of the embodiments of the present disclosure.

As shown in fig. 12, the electronic device 1200 is embodied in the form of a general purpose computing device. The components of the electronic device 1200 may include, but are not limited to: at least one processing unit 1210, at least one memory unit 1220, a bus 1230 connecting the various system components including the memory unit 1220 and the processing unit 1210, a display unit 1240, and the like.

Wherein the storage unit stores program code that can be executed by the processing unit 1210 such that the processing unit 1210 performs the steps described in this specification in accordance with various exemplary embodiments of the present disclosure. For example, the processing unit 1210 may perform the steps as shown in fig. 1, 2, 3.

The storage unit 1220 may include a readable medium in the form of a volatile memory unit, such as a random access memory unit (RAM) 12201 and/or a cache memory unit 12202, and may further include a read only memory unit (ROM) 12203.

The memory unit 1220 may also include a program/utility 12204 having a set (at least one) of program modules 12205, such program modules 12205 including, but not limited to: an operating system, one or more application programs, other program modules, and program data, each of which, or some combination thereof, may comprise an implementation of a network environment.

Bus 1230 may be one or more of several types of bus structures, including a memory unit bus or memory unit controller, a peripheral bus, an accelerated graphics port, a processing unit, or a local bus using any of a variety of bus architectures.

The electronic device 1200 can also communicate with one or more external devices 1200' (e.g., keyboard, pointing device, bluetooth device, etc.) such that a user can communicate with devices with which the electronic device 1200 interacts, and/or any devices (e.g., router, modem, etc.) with which the electronic device 1200 can communicate with one or more other computing devices. Such communication may occur via input/output (I/O) interfaces 1250. Also, the electronic device 1200 may communicate with one or more networks (e.g., a Local Area Network (LAN), a Wide Area Network (WAN), and/or a public network such as the internet) via the network adapter 1260. The network adapter 1260 may communicate with other modules of the electronic device 1200 via the bus 1230. It should be appreciated that although not shown, other hardware and/or software modules may be used in conjunction with the electronic device 1200, including but not limited to: microcode, device drivers, redundant processing units, external disk drive arrays, RAID systems, tape drives, and data backup storage systems, among others.

Through the above description of the embodiments, those skilled in the art will readily understand that the exemplary embodiments described herein may be implemented by software, or by software in combination with necessary hardware. Therefore, as shown in fig. 13, the technical solution according to the embodiment of the present disclosure may be embodied in the form of a software product, which may be stored in a non-volatile storage medium (which may be a CD-ROM, a usb disk, a removable hard disk, etc.) or on a network, and includes several instructions to enable a computing device (which may be a personal computer, a server, or a network device, etc.) to execute the above method according to the embodiment of the present disclosure.

The software product may employ any combination of one or more readable media. The readable medium may be a readable signal medium or a readable storage medium. A readable storage medium may be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any combination of the foregoing. More specific examples (a non-exhaustive list) of the readable storage medium include: an electrical connection having one or more wires, a portable disk, a hard disk, a Random Access Memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable combination of the foregoing.

The computer readable storage medium may include a propagated data signal with readable program code embodied therein, for example, in baseband or as part of a carrier wave. Such a propagated data signal may take many forms, including, but not limited to, electro-magnetic, optical, or any suitable combination thereof. A readable storage medium may also be any readable medium that is not a readable storage medium and that can communicate, propagate, or transport a program for use by or in connection with an instruction execution system, apparatus, or device. Program code embodied on a readable storage medium may be transmitted using any appropriate medium, including but not limited to wireless, wireline, optical fiber cable, RF, etc., or any suitable combination of the foregoing.

Program code for carrying out operations for the present disclosure may be written in any combination of one or more programming languages, including an object oriented programming language such as Java, C++ or the like and conventional procedural programming languages, such as the "C" programming language or similar programming languages. The program code may execute entirely on the user's computing device, partly on the user's device, as a stand-alone software package, partly on the user's computing device and partly on a remote computing device, or entirely on the remote computing device or server. In the case of a remote computing device, the remote computing device may be connected to the user computing device through any kind of network, including a Local Area Network (LAN) or a Wide Area Network (WAN), or may be connected to an external computing device (e.g., through the internet using an internet service provider).

The computer readable medium carries one or more programs which, when executed by a device, cause the computer readable medium to perform the functions of: acquiring an IP address of an access request; determining a geographic location of the access request based on the IP address, the geographic location including a country or province or city; comparing the geographic location to a plurality of masks in a restricted zone mask table; and when the comparison result has a matching result, limiting the access of the IP address of the access request.

Those skilled in the art will appreciate that the modules described above may be distributed in the apparatus according to the description of the embodiments, or may be modified accordingly in one or more apparatuses unique from the embodiments. The modules of the above embodiments may be combined into one module, or further split into multiple sub-modules.

Through the above description of the embodiments, those skilled in the art will readily understand that the exemplary embodiments described herein may be implemented by software, or by software in combination with necessary hardware. Therefore, the technical solution according to the embodiments of the present disclosure may be embodied in the form of a software product, which may be stored in a non-volatile storage medium (which may be a CD-ROM, a usb disk, a removable hard disk, etc.) or on a network, and includes several instructions to enable a computing device (which may be a personal computer, a server, a mobile terminal, or a network device, etc.) to execute the method according to the embodiments of the present disclosure.

Exemplary embodiments of the present disclosure are specifically illustrated and described above. It is to be understood that the present disclosure is not limited to the precise arrangements, instrumentalities, or instrumentalities described herein; on the contrary, the disclosure is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the appended claims.

Similar Documents

Publication	Publication Date	Title
US20110154297A1	2011-06-23	Dynamic instrumentation
CN105391811A	2016-03-09	DNS (domain name resolution) method, access method for application server, and terminal
JPH1097421A	1998-04-14	Method and device for addressing memory in microprocessor that is structured to execute compression instruction
CN104539750A	2015-04-22	IP locating method and device
CN104021124A	2014-09-03	Method, device and system used for processing webpage data
JP2011123712A	2011-06-23	Outsourced analysis system of personal information
CN112491876A	2021-03-12	Geographic position access control method and device
JP2006155081A	2006-06-15	Program and device for electronic data exchange, and information processing program
CN109194736B	2021-04-27	Message duplicate removal method and device, electronic equipment, medium and unmanned vehicle

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA VA 22313-1451

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE PAID
POSTEDIGITAL
NNNNN

Douglas M. Hamilton
HDC Fortinet
224 S. Main Street, 114
Springville, UT 84663



**Courtesy Reminder for
Application Serial No: 16/362,167**

Attorney Docket No: FORT-031800(18167)
Customer Number: 176502
Date of Electronic Notification: 10/05/2021

This is a courtesy reminder that new correspondence is available for this application. If you have not done so already, please review the correspondence. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:

miquelchamilton@hamiltonshome.com
dhamilton@hdciplaw.com

To view your correspondence online or update your email addresses, please visit us anytime at **<https://ppair-my.uspto.gov/pair/PrivatePair>**.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov or call 1-866-217-9197.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Fortinet, Inc. First Inventor: Little App. No.: 16/362,167 Filed: March 19, 2020 For: DETECTING ACCESSSS POINTS LOCATED WITHIN PROXIMITY OF A COMPUTING DEVICE FOR TROUBLESHOOTING OF A NETWORK	Examiner: YANG Group Art Unit: 2493 Conf. No.: 6553 Docket No.: FORT-031800(18167)
--	---

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE TO OFFICE ACTION

Sir/Madam:

In response to the Office action having a notification date of October 5, 2021 (the “Office Action”), the Applicant respectfully requests the Examiner to enter the following amendment and to consider the following remarks:

Amendments to the Claims begin at page 2 of this paper.

Remarks begin at page 8 of this paper.

Amendments to the Claims

1. (Currently Amended) A method comprising:

obtaining and storing, by one or more servers associated with an enterprise network, information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users;

receiving, by the one or more servers, a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the enterprise network in encrypted form;

responsive to receipt of the file access request, determining, by the one or more servers, a risk score for the first user based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request; and

based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key, wherein said permitting or denying comprises:

when the risk score is less than a first threshold, returning the decryption key and providing full access to the file; and

when the risk score is greater than a second threshold, withholding the decryption key.

2. (Currently Amended) The method of claim 1, wherein said determining, by the one or more servers, the a risk score for the first user comprises evaluating the file access request with reference to a model of user behavior developed by machine-learning.

3. (Original) The method of claim 1, wherein the information regarding historical user behavior includes for each user of the plurality of users:

historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time;

historical data regarding observed locations of the user; and

historical data regarding observed times at which the user accesses files.

4. (Original) The method of claim 1, wherein the observed data includes a current location of the first user as determined based on a source Internet Protocol (IP) address contained in the file access request.

5. (Original) The method of claim 1, wherein the observed data includes a status indicative of whether the connection through which the first user initiated the file access request is trusted or untrusted.

6. (Original) The method of claim 5, wherein the connection is trusted when the first user is on the enterprise network or accessing the enterprise network remotely via a secure connection.

7. (Original) The method of claim 5, wherein the connection is untrusted when the first user is not on the enterprise network or accessing the enterprise network remotely via an insecure connection.

8. (Original) The method of claim 1, wherein the encrypted form involves the file being encapsulated in a cryptographic wrapper.

9. (Canceled)

10. (Currently Amended) The method of claim 1 9, wherein said permitting or denying further comprises when the risk score is between the first threshold and a second threshold, returning the decryption key and providing limited access to the file.

11. (Canceled)

12. (Original) A non-transitory computer-readable storage medium embodying a set of instructions, which when executed by one or more processors of one or more servers associated with an enterprise network, causes the one or more processors to perform a method comprising:

obtaining and storing information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users, wherein the information regarding historical user behavior includes for each user of the plurality of users:

historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time;

historical data regarding observed locations of the user; and

historical data regarding observed times at which the user accesses files;

receiving a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the enterprise network in encrypted form;

responsive to receipt of the file access request, determining a risk score for the first user based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request; and

based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key.

13. (Currently Amended) The non-transitory computer-readable storage medium of claim 12, wherein said determining the a risk score for the first user comprises evaluating the file access request with reference to a model of user behavior developed by machine-learning.

14. (Canceled)

15. (Original) The non-transitory computer-readable storage medium claim 13, wherein the observed data includes a current location of the first user as determined based on a source Internet Protocol (IP) address contained in the file access request.

16. (Original) The non-transitory computer-readable storage medium claim 13, wherein the observed data includes a status indicative of whether the connection through which the first user initiated the file access request is trusted or untrusted.

17. (Original) The non-transitory computer-readable storage medium claim 13, wherein the encrypted form involves the file being encapsulated in a cryptographic wrapper.

18. (Original) The non-transitory computer-readable storage medium claim 13, wherein said permitting or denying further comprises when the risk score is less than a first threshold, returning the decryption key and providing full access to the file.

19. (Original) The non-transitory computer-readable storage medium claim 18, wherein said permitting or denying further comprises when the risk score is between the first threshold and a second threshold, returning the decryption key and providing limited access to the file.

20. (Original) The non-transitory computer-readable storage medium claim 19, wherein said permitting or denying further comprises when the risk score is greater than the second threshold, withholding the decryption key.

21. (New) The method of claim 1, wherein the first threshold and the second threshold are the same.

22. (New) A system, the system comprising:

one or more processors; and

a non-transitory computer-readable storage medium coupled to the one or more processors and embodying a set of instructions, which when executed by the one or more processors of one or more servers associated with an enterprise network, causes the one or more processors to perform a method comprising:

obtaining and storing information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users;

receiving a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the enterprise network in encrypted form;

responsive to receipt of the file access request, determining a risk score for the first user based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request; and

based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key, wherein said permitting or denying comprises:

when the risk score is less than a first threshold, returning the decryption key and providing full access to the file; and

when the risk score is greater than a second threshold, withholding the decryption key.

23. (New) The system of claim 22, wherein said permitting or denying further comprises when the risk score is between the first threshold and a second threshold, returning the decryption key and providing limited access to the file.

24. (New) The system of claim 22, wherein the first threshold and the second threshold are the same.

25. (New) The system of claim 22, wherein the information regarding historical user behavior includes for each user of the plurality of users:

historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time;

historical data regarding observed locations of the user; and

historical data regarding observed times at which the user accesses files.

Remarks

The undersigned respectfully requests reconsideration of the above-captioned patent application in view of the following remarks. Claims 1-20 as originally filed were pending in the application. Claims 1, 2, 10, 12, and 13 have been amended, claims 21-25 have been added, and claims 9, 11, and 14 have been canceled. Hence, claims 1-8, 10, 12-13, and 15-25 remain pending.

Claims 2 and 13 are objected to for technicalities that are corrected herein by amendment. Applicant also thanks the examiner for their careful in identifying that claim 14 depended from claim 13, and has corrected it by amendment herein to depend from independent claim 12.

Claims 1-3, 5-7, 9-14, 16, and 18-20 stand rejected under 35 USC 103 as allegedly obvious over a combination US Pat. Pub. No. 2019/0319945 (hereinafter “Levy”) and US Pat. Pub. No. 2004/0221172 (hereinafter “Stamos”). Claims 4 and 15 stand rejected under 35 USC 103 as allegedly obvious over a combination Levy, Stamos, and US Pat. Pub. No. 2014/03100779 (hereinafter “Lof”). Claims 8 and 17 stand rejected under 35 USC 103 as allegedly obvious over a combination Levy, Stamos, and US Pat. Pub. No. 2005/0229258 (hereinafter “Pigin”). Applicant respectfully amends in part and traverses in part to overcome the rejections.

Claim 1 has been amended to include the limitations of original claims 9 and 11. Thus, as amended claim 1 sets forth a method that includes, *inter alia*, determining a risk score for a first user based on a plurality of factors, and based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key. The permitting or denying includes: when the risk score is less than a first threshold, returning the decryption key and providing full access to the file; and when the risk score is greater than a second threshold, withholding the decryption key.

None of the cited references, either separately or in combination disclose, teach, or suggest such a limitation. In particular, the Office Action relies on paragraph 0213 of Levy to provide disclosure to reject original claims 9 and 11. Office Action at pp. 9-10. Paragraph 0213 says:

Further, selecting the authentication model may include selecting an authentication model that conditionally uses an additional authentication factor. For example, if the risk score for the device or the user (or some combination of these) is below a threshold such that it indicates that the user and device are safe, then the authentication model may use an additional authentication factor. Conversely, if the risk score for the device or the user is above the threshold such that it indicates that the user or the device is compromised or unsafe, then the authentication model may withhold the additional authentication factor to prevent access by the device to the remote resource. Other conditional configurations may also or instead be employed. For example, in one embodiment, if the risk score for the device or the user (or some combination of these) is below a threshold such that it indicates that the user and device are safe, then the authentication model may forego an additional authentication factor. Conversely, if the risk score for the device or the user is above the threshold such that it indicates that the user or the device is compromised or unsafe, then the authentication model may require the additional authentication factor as a condition for access by the device to the remote resource.

The additional authentication factor is “a token or biometric identifier” that is conditionally provided by the user to the computer performing an authentication conditionally based upon the “risk for the device”. Levy at ¶0211. It is nonsense to argue that, for example, a biometric identifier is provided to the user as a biometric identifier is by definition part of the individual. Rather, it only makes sense that the additional authentication factor is provided from the user to the computer performing the authentication. This is the opposite of claim 1 where the computer performing an authentication provides or withholds the decryption key based upon a risk score.

In the context of paragraph 0211 of Levy, the cited paragraph 0213 of Levy can be understood. Paragraph 0213 says that where the risk score indicates that the user and device are safe, the model “forgoes the additional authentication factor.” Said another way, where the risk score indicates a defined threshold of safety, there is no reason for requesting the additional authentication factor as access is going to be granted without it. Conversely, where the risk factor indicates a lack of safety, the additional authentication factor is required (i.e., a request is made for the user to provide the additional authentication factor) as without it access will not be granted. As another example, where the risk score indicates a defined threshold of safety, there is reason for requesting

the additional authentication factor as it is only when the low risk factor is coupled with the additional authentication factor that access will be granted. Conversely, where the risk score does not indicate a defined threshold of safety, there is no reason for requesting the additional authentication factor as, again, it is only when the low risk factor is coupled with the additional authentication factor that access will be granted and requesting the additional authentication factor would not change the result of the denial. Simply stated, one of ordinary skill in the art would not understand the additional authentication factor of Levy to be the decryption key of claim 1, and also would not understand Levy as disclosing, teaching, or suggesting the process of claim 1.

As none of the other cited references are even alleged to provide the aforementioned disclosure missing from Levy, and in fact none provide such missing disclosure, the combination fails to render claim 1 obvious. For at least this reason, Applicant respectfully requests withdrawal of the rejection and allowance of claim 1.

Additionally, each of claims 12 and 22 includes a limitation similar to that discussed above in relation to claim 1, and are each in condition for allowance for at least this reason. Such allowance is respectfully requested herein. Further, claims 2-8, 10, 13, 15-21, and 23-25 each depend from an allowable base claim, and are thus in condition for allowance for at least this reason. Such allowance is respectfully requested herein.

Conclusion

The undersigned respectfully submits that the amendments and remarks presented herein have overcome the rejections, and that the pending claims are in condition for allowance. Accordingly, the undersigned respectfully requests that the rejections be withdrawn and that a Notice of Allowance be promptly issued for the pending claims.

By responding in the foregoing remarks only to particular positions taken by the Examiner, the Applicant does not acquiesce with any other positions that have not been explicitly addressed. Applicant's arguments for the patentability of a claim should not be understood as implying that no other reasons for the patentability of that claim exist. The absence of a reply to a specific rejection, issue or comment set forth in the Office Action does not signify agreement with or concession of that rejection, issue or comment. In addition, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, and the amendment of any claim does not necessarily signify any concession of unpatentability of the claim prior to its amendment.

Request for a Telephone Interview

If the Examiner believes a telephone conference would expedite prosecution of the above-captioned patent application, please telephone the undersigned at (720) 266-4728.

Respectfully submitted,

HDC Intellectual Property Law, LLP

Date January 2022

By /Douglas M. Hamilton/
Douglas M. Hamilton
Reg. No. 47,629

Electronic Patent Application Fee Transmittal				
Application Number:		16362167		
Filing Date:		22-Mar-2019		
Title of Invention:		FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		
First Named Inventor/Applicant Name:		Matthew J. Little		
Filer:		Douglas M. Hamilton		
Attorney Docket Number:		FORT-031800(18167)		
Filed as Large Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	1202	2	100	200
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				200

Electronic Acknowledgement Receipt	
EFS ID:	44677447
Application Number:	16362167
International Application Number:	
Confirmation Number:	6553
Title of Invention:	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS
First Named Inventor/Applicant Name:	Matthew J. Little
Customer Number:	176502
Filer:	Douglas M. Hamilton
Filer Authorized By:	
Attorney Docket Number:	FORT-031800(18167)
Receipt Date:	05-JAN-2022
Filing Date:	22-MAR-2019
Time Stamp:	17:33:08
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$ 200
RAM confirmation Number	E202215H34032798
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		FORT-031800ResponsetoOAMailed10052021.pdf	56183	yes	11
			6ef102a49d1d27273a0cca2df7a30af0c7537547		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Amendment/Req. Reconsideration-After Non-Final Reject		1	1	
	Claims		2	7	
	Applicant Arguments/Remarks Made in an Amendment		8	11	
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	38083	no	2
			59b08cca7c8424dfc6f626886e3e944fdc278bd5		
Warnings:					
Information:					
Total Files Size (in bytes):			94266		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/362,167	03/22/2019	Matthew J. Little	FORT-031800(18167)	6553
176502	7590	03/10/2022	EXAMINER	
Douglas M. Hamilton			YANG, HAN	
HDC Fortinet				
224 S. Main Street, 114			ART UNIT	
Springville, UT 84663			PAPER NUMBER	
			2493	
			NOTIFICATION DATE	
			DELIVERY MODE	
			03/10/2022	
			ELECTRONIC	

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

dhamilton@hdciplaw.com
miquelchamilton@hamiltonshome.com

DETAILED ACTION

Notice of AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

The present office action is responsive to communications received on 1/5/2022. Applicant added claims 21-25 and cancelled claims 9, 11, and 14. Claims 1-8, 10, 12-13, and 15-25 are pending.

Response to Arguments

The arguments/remarks filed by the applicant on 1/5/2022 have been fully considered and are responded in the following.

Applicant's amendments to the claims have overcome the objections previously set forth in the Non-Final Office Action mailed 10/5/2021. All objections have been withdrawn.

Applicant's arguments regarding the 35 USC § 103 rejection of **amended** independent claim 1 have been fully considered but they are not persuasive. Applicant states that **'None of the cited references, either separately or in combination disclose, teach, or suggest such a limitation "when the risk score is less than a first threshold, returning the decryption key and providing full access to the file; and when the risk score is greater than a second threshold, withholding the decryption key." The additional authentication factor is "a token or biometric identifier" that is conditionally provided by the user to the computer performing an authentication conditionally based upon the "risk for the device". (p. 8, ¶4-5 and p. 9, ¶12)**' In response to applicant's arguments, the examiner respectfully

disagrees. Levy in ¶213 discloses “if the risk score for the device or the user is below a threshold such that it indicates that the user and device are safe, then the authentication model may forego an additional authentication factor. if the risk score for the device or the user is above the threshold such that it indicates that the user or the device is compromised or unsafe, then the authentication model may withhold the additional authentication factor to prevent access by the device to the remote resource.” Authentication factor being a biometric identifier or a security token is for example only (¶210), and “are set forth by way of example and not of limitation” (¶233). In summary, Reference Levy discloses granting/preventing access based on risk score. Reference Stamos discloses this can be achieved through the issue/holdback of decryption key by reciting “The policy sever then issues copies of required keys to permit the recipient to decrypt the information” (¶19). Therefore the combination discloses the entire limitation. Similar rationale applies to claims 12 and 22 (Argument p. 10, ¶13).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-3, 5-7, 10, 12-13, 16, 18-20, 22-23 and 25 are rejected under 35 U.S.C. 103 as being unpatentable over Levy (US 20190319945 A1) in view of Stamos (US 20040221172 A1).

Regarding claim 1, Levy teaches a method comprising:

obtaining and storing, by one or more servers associated with an enterprise network, information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users; ([0060] The threat management facility 100 may control access to the enterprise facility 102 networks. A network access facility 124 may restrict access to certain applications, networks, files, printers, servers, databases, and so on. In addition, the network access facility 124 may restrict user access under certain conditions, such as the user's location, usage history, need to know, job position, connection type, time of day, method of authentication, client-system configuration.) Here Levy discloses in ¶50 that “the threat management facility 100 may include a policy management facility 112 that manages rules or policies for the enterprise facility 102. Exemplary rules include access permissions associated with networks, applications, compute instances, users, content, data, and the like. The policy management facility 112 may use a database, a text file, other data store, or a combination to store policies.”

receiving, by the one or more servers, a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the enterprise network in encrypted form; ([0207] FIG. 17 As shown in step 1702, the method 1700 may include receiving a request for a remote resource from a compute instance in an enterprise network, such as a request for authenticated access to the remote resource. This may include any resource that might usefully be accessed by a compute instance from within the enterprise network.) Here Levy discloses in ¶78 that “privacy may be addressed in some cases by user notifications and permissions, anonymization, tokenization, and encryption.”

responsive to receipt of the file access request, determining, by the one or more servers, a risk score for the first user based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request; and ([0208] As shown in step 1704, the method 1700 may include calculating risk scores, for example by calculating a first risk score for a user of the compute instance. In one aspect, the entity models described herein provide useful computer-implemented tools for measuring expected behavior and deviations therefrom, and may be usefully employed in this context to calculate risk scores for the particular entities of interest: the user of the compute instance.) Here Levy discloses in ¶ 156 “to draw policy or security conclusions based on a history of users and file usage.”

based on the risk score, permitting or denying, by the one or more servers, access to the file. ([0210, 0211, 0217] As shown in step 1706, the method 1700 may include selecting an authentication model for access to the remote resource by the user and the device. More generally, the authentication models may provide various sets of authentication requirements using various combinations of the foregoing authentication factors or any other authentication factors, with the particular authentication factors varying based on the user and device risk scores. As shown in step 1708, the method 1700 may include authenticating the user to the remote resource according to the authentication model selected in step 1706.)

Levy teaches based on the risk score, permitting or denying, access to the file, but does not **explicitly** teach this is done by returning a decryption key for the file or withholding the decryption key, wherein said permitting or denying comprises: when the risk score is less than a first threshold, returning the decryption key and providing full access to the file; and when the risk score is greater than a second threshold, withholding the decryption key. This aspect of the claim is identified as a difference.

However, Stamos in an analogous art **explicitly** teaches

based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key, ([0008, 0009] Encryption techniques such as those employing a Public Key Infrastructure (PKI) enable an enterprise to provide authentication, access control and confidentiality for its applications and data. Before accessing any information, the recipient must first authenticate with the policy server. The policy sever then issues copies of required keys to permit the recipient to decrypt the information.)

wherein said permitting or denying comprises:

when the risk score is less than a first threshold, returning the decryption key and providing full access to the file; and ([Levy 0213] if the risk score for the device or the user (or some combination of these) is below a threshold such that it indicates that the user and device are safe, then the authentication model may forego an additional authentication factor.) **when the risk score is greater than a second threshold, withholding the decryption key.** ([Levy 0213] if the risk score for the device or the user is above the threshold such that it indicates that the user or the device is compromised or unsafe, then the authentication model may withhold the additional authentication factor to prevent access by the device to the remote resource.) In summary, Reference Levy discloses granting/preventing access based on risk score. Reference Stamos discloses this can be achieved through the issue/holdback of decryption key by reciting “The policy sever then issues copies of required keys to permit the recipient to decrypt the information” (¶19). Therefore the combination discloses the entire limitation.

It would have been prima facie obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to combine the “dynamic authentication” concept of Levy, and the “adaptive encryption” approach of Stamos. One of ordinary skill in the art would have been motivated to perform such a modification to address security problems that originate when authorized users abuse

their authority, by selectively applying encryption policies at the point of use of a file, rather than simply at the point of file server and/or access storage (**Stamos [0018]**).

Regarding claim 2, Levy in view of Stamos teaches all the features with respect to claim 1, as outlined above. The combination further teaches **wherein said determining, by the one or more servers, the risk score for the first user comprises evaluating the file access request with reference to a model of user behavior developed by machine-learning.** ([Levy 0209] while event models for a user/device combination can provide a useful measure of riskiness, other measures may also or instead be used, either alone or in combination with such techniques. For example, other risk scores based on, e.g., signatures, context, behavior, machine learning or the like may be used in addition to, or instead of the risk scores described above to dynamically control authentication requirements based on assessed risk.)

Regarding claim 3, Levy in view of Stamos teaches all the features with respect to claim 1, as outlined above. The combination further teaches wherein the information regarding historical user behavior includes for each user of the plurality of users:

historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time; ([Levy 0111] The valuation model may, for example, estimate value based on file location, based on an access control content, based on content, or based on any other context, usage, feature or combination of the foregoing. For example, the valuation model may estimate value based on one or more of encryption status, file type, file usage history, file creation date, file modification date, file content, and file author.)

historical data regarding observed locations of the user; and historical data regarding observed times at which the user accesses files. ([Levy 0060] A network access facility 124 may restrict access to certain applications, networks, files, printers, servers, databases, and so on. In addition, the network access facility 124 may restrict user access under certain conditions, such as the user's location, usage history, need to know, job position, connection type, time of day, method of authentication, client-system configuration, or the like.)

Regarding claim 5, Levy in view of Stamos teaches all the features with respect to claim 1, as outlined above. The combination further teaches **wherein the observed data includes a status indicative of whether the connection through which the first user initiated the file access request is trusted or untrusted.** ([Levy 0060] A network access facility 124 may restrict access to certain applications, networks, files, printers, servers, databases, and so on. In addition, the network access facility 124 may restrict user access under certain conditions, such as the user's location, usage history, need to know, job position, connection type, time of day, method of authentication, client-system configuration, or the like.) Here Levy depicts in [0033] that connection including "one or more gateways, bridges, wired networks, wireless networks, virtual private networks, other compute instances." It would have been prima facie obvious to one of ordinary skill in the art to conclude that connection through wired networks is more secure/trustworthy than through wireless networks (<https://aberdeencybersecurity.co.uk/wired-vs-wireless-networking>); as well as to conclude that connection with virtual private networks is more secure/trustworthy than without virtual private networks (<https://www.tomsguide.com/us/-vpn-for-beginners,news-17514.html>).

Regarding claim 6, Levy in view of Stamos teaches all the features with respect to claim 5, as

outlined above. The combination further teaches **wherein the connection is trusted when the first user is on the enterprise network or accessing the enterprise network remotely via a secure connection.**

([Levy 0216] Other secondary techniques may also or instead be used to support authentication models or provide additional authentication factors. For example, a secondary authentication may be based on information such as whether a user recently logged in to the device, whether a user recently provided a token passcode, whether the device recently connected to the enterprise network, the current IP address for a device, the geolocation of a device, or whether the user/device combination recently logged in to the remote resource.) Here Levy discloses that connection is more trustworthy if user is on the enterprise network by citing “the compute instances 10-26 may be protected from threats even when a compute instance 10-26 is not connected to the enterprise facility 102 network” [0038].

Regarding claim 7, Levy in view of Stamos teaches all the features with respect to claim 5, as outlined above. The combination further teaches **wherein the connection is untrusted when the first user is not on the enterprise network or accessing the enterprise network remotely via an insecure connection.** ([Levy 0216] Other secondary techniques may also or instead be used to support authentication models or provide additional authentication factors. For example, a secondary authentication may be based on information such as whether a user recently logged in to the device, whether a user recently provided a token passcode, whether the device recently connected to the enterprise network, the current IP address for a device, the geolocation of a device, or whether the user/device combination recently logged in to the remote resource.) Here Levy discloses that connection is less trustworthy if user is not on the enterprise network by citing “the compute instances 10-26 may be protected from threats even when a compute instance 10-26 is not connected to the enterprise facility 102 network” [0038].

Regarding claim 10, Levy in view of Stamos teaches all the features with respect to claim 1, as outlined above. The combination further teaches **wherein said permitting or denying further comprises when the risk score is between the first threshold and a second threshold, returning the decryption key and providing limited access to the file.** ([Levy 0211] The risk scores may also generally be used as an authentication factor, e.g., by using the risk score as a property of the user and requiring a minimum or maximum value, or indirectly by using the risk score as a threshold for whether to select an authentication model requiring one or more additional authentication factors. [Levy 0213] if the risk score for the device or the user (or some combination of these) is below a threshold such that it indicates that the user and device are safe, then the authentication model may use an additional authentication factor (analogous to claim limitation “less than second threshold”). If the risk score for the device or the user is above the threshold such that it indicates that the user or the device is compromised or unsafe, then the authentication model may require the additional authentication factor as a condition for access by the device to the remote resource (analogous to claim limitation “greater than first threshold”).)

Regarding claims 12-13, 16, 18-20, 22-23 and 25, the scope of the claims are similar to that of claims 1-3, 5 and 10, respectively. Accordingly, the claims are rejected using a similar rationale.

Claims 4 and 15 are rejected under 35 U.S.C. 103 as being unpatentable over Levy (US 20190319945 A1) in view of Stamos (US 20040221172 A1) and Lof (US 20140310779 A1).

Regarding claim 4, Levy in view of Stamos teaches all the features with respect to claim 1, as outlined above. But the combination does not teach wherein the observed data includes a current

location of the first user as determined based on a source Internet Protocol (IP) address contained in the file access request. This aspect of the claim is identified as a difference.

However, Lof in an analogous art **explicitly** teaches **wherein the observed data includes a current location of the first user as determined based on a source Internet Protocol (IP) address contained in the file access request.** ([0130] the media content provider can use geo-location techniques to determine a geographic location of the client device (e.g., the country in which the client device resides). Such techniques include using the IP address of the client device (which can be determined from an HTTP request, for example) to lookup the user's probable location in an IP address database.)

It would have been prima facie obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to combine the “dynamic authentication” concept of Levy, and the “geo-location techniques using IP address” approach of Lof. One of ordinary skill in the art would have been motivated to perform such a modification to provide efficient and secure access to content by obtaining information about the client device that is not explicitly provided or reported by the client device, but available through the communication between the client device and the content provider **(Lof [0130, 0010])**.

Regarding claim 15, the scope of the claim is similar to that of claim 4, respectively. Accordingly, the claim is rejected using a similar rationale.

Claims 8 and 17 are rejected under 35 U.S.C. 103 as being unpatentable over Levy (US 20190319945 A1) in view of Stamos (US 20040221172 A1) and Pigin (US 20050229258 A1).

Regarding claim 8, Levy in view of Stamos teaches all the features with respect to claim 1, as outlined above. But the combination does not teach wherein the encrypted form involves the file being encapsulated in a cryptographic wrapper. This aspect of the claim is identified as a difference.

However, Pigin in an analogous art **explicitly** teaches **wherein the encrypted form involves the file being encapsulated in a cryptographic wrapper**. ([0230] These operations manipulate cryptographic objects at the file level. File-level wrappers are based on the crypto container concept. All cryptographic objects, associated with a single original file, are encapsulated into a single file of compound structure (cryptocontainer).)

It would have been prima facie obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to combine the “dynamic authentication” concept of Levy, and the “file level wrappers” approach of Pigin. One of ordinary skill in the art would have been motivated to perform such a modification to provide secure and efficient document rights management and file encryption (**Pigin [0001, 0004]**).

Regarding claim 17, the scope of the claim is similar to that of claim 8, respectively. Accordingly, the claim is rejected using a similar rationale.

Claims 21 and 24 are rejected under 35 U.S.C. 103 as being unpatentable over Levy (US 20190319945 A1) in view of Stamos (US 20040221172 A1) and Kobres (US 20160063227 A1).

Regarding claim 21, Levy in view of Stamos teaches all the features with respect to claim 1, as outlined above. But the combination does not teach wherein the first threshold and the second threshold are the same. This aspect of the claim is identified as a difference.

However, Kobres in an analogous art **explicitly** teaches **wherein the first threshold and the second threshold are the same**. ([0155] At 430, the authenticator determines whether to grant access to one of: a device and a resource of the device based on the comparison performed at 420. This can be a binary determination such that access is either granted or denied.) Here Kobres discloses an example of binary determination (granted or denied, meaning first threshold and second threshold are the same). Kobres also discloses that the decision does not have to be a binary decisions (granted, denied or limited, meaning first threshold and second threshold are not the same) if desired, by reciting that “the decision does not have to be a binary decisions meaning that different levels of authenticated access can be granted based on the confidence value when that confidence value is compared to predefined values, thresholds, or ranges of values that the authentication service uses to make decisions about authentication” (¶65) and a detail example in ¶125

It would have been prima facie obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to combine the “dynamic authentication” concept of Levy, and the “threshold comparison” approach of Kobres. One of ordinary skill in the art would have been motivated to perform such a modification to provide flexibility in security restrictions, which can be a straightforward binary determination such that access is either granted or denied. Alternatively, this can be access based on some resolved access-level, which is less than complete and unfettered access (Kobres [0155]).

Regarding claim 24, the scope of the claim is similar to that of claim 21, respectively. Accordingly, the claim is rejected using a similar rationale.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- US 20070297610 A1, "Data protection for a mobile device", by Chen, teaches managing a decryption key at a key server that is remote from the mobile device, the decryption key enabling decryption of encrypted information stored at the mobile device; performing an authentication procedure for a user of the mobile device; transmitting the decryption key to the mobile device if the authentication procedure authenticates the user; withholding transmission of the decryption key to the mobile device if the authentication procedure does not authenticate the user.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HAN YANG whose telephone number is (408)918-7638. The examiner can normally be reached on Monday to Friday, 9:00-5:00.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Carl Colin can be reached on 571-272-3862. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/H.Y./
Examiner, Art Unit 2493

/CHAU LE/
Primary Examiner, Art Unit 2493

<i>Notice of References Cited</i>	Application/Control No. 16/362,167		Applicant(s)/Patent Under Reexamination Little et al.	
	Examiner HAN YANG		Art Unit 2493	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20160063227-A1	03-2016	Kobres; Erick	H04L63/08	726/3
*	B	US-20070297610-A1	12-2007	Chen; Yuqun	H04L9/083	380/270
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

<i>Index of Claims</i> 	Application/Control No. 16/362,167	Applicant(s)/Patent Under Reexamination Little et al.
	Examiner HAN YANG	Art Unit 2493

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS										
☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47										
CLAIM		DATE								
Final	Original	09/25/2021	03/05/2022							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	-							
	10	✓	✓							
	11	✓	-							
	12	✓	✓							
	13	✓	✓							
	14	✓	-							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							
	21		✓							
	22		✓							
	23		✓							
	24		✓							
	25		✓							

Search Notes 	Application/Control No. 16/362,167	Applicant(s)/Patent Under Reexamination Little et al.
	Examiner HAN YANG	Art Unit 2493

CPC - Searched*		
Symbol	Date	Examiner
G06F 21/6218 21/602 21/316	09/25/2021	HY
G06F 16/182	09/25/2021	HY
G06N 20/00	09/25/2021	HY
H04L 9/0819	09/25/2021	HY

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

/H.Y./ Examiner, Art Unit 2493	
-----------------------------------	--

<i>Search Notes</i> 	Application/Control No. 16/362,167	Applicant(s)/Patent Under Reexamination Little et al.
	Examiner HAN YANG	Art Unit 2493

Search Notes		
Search Notes	Date	Examiner
G06F 21/6218 21/602 21/316	09/25/2021	HY
G06F 16/182	09/25/2021	HY
G06N 20/00	09/25/2021	HY
H04L 9/0819	09/25/2021	HY
Classification with text search.	09/25/2021	HY
EAST text search (see search history printout).	09/25/2021	HY
Inventor and applicant search EAST.	09/22/2021	HY
IDS references considered.	09/22/2021	HY
google patent and NPL search.	09/24/2021	HY
Include feedback from SPE.	09/27/2021	HY
Updated complete search.	03/05/2022	HY
ip.com patent and NPL search.	03/05/2022	HY
google patent and NPL search.	03/05/2022	HY

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/H.Y./ Examiner, Art Unit 2493	
-----------------------------------	--

1 - 50

☐ Mechanisms for anomaly detection and access management

The present disclosure relates generally to threat detection, and more particularly, to techniques for managing user access to resources in an enterprise environment. Some aspects are directed to the concept of managing access to a target resource based on a threat perception of a user that is...

ORACLE INTL CORP

US20200267162 : US Applications : 2020-08-20 : 4

☐ System and method to identify abnormalities to continuously measure transaction risk

Aspects of the disclosure provide techniques for using behavior based information for providing and restricting access to a secure website, or computer network and its assets to a user. Components of the system may include the following. Client remote computing device, network and browser unique...

SECUREAUTH CORP

US11065809 : US Patents : 2021-05-11 : 4

☐ System, method, and apparatus for data cognition incorporating autonomous security protection

A method, apparatus and computer readable medium for data cognition incorporating autonomous security protection including, a data file stored on a storage medium, and having stored instructions for an embedded autonomous executable program which is executed each time there is an attempt to access,...

AZOS AI LLC

US20120151553 : US Applications : 2012-05-14 : 4

☐ Data-defined architecture for network data management

Techniques are disclosed relating to data management. A computer system may evaluate network traffic to extract and group data objects based on their content satisfying similarity criteria, and to identify baseline behavior with respect to those data objects. The computer system may generate...

HELIOS DATA INC

US20180280797 : US Applications : 2018-09-22 : 4

☐ Permissions policy manager to configure permissions on computing devices

For increased device security, a security policy manager is used to configure permissions for applications installed on mobile computing devices. In one approach, an evaluation server receives data associated with a context for a computing device. Based on the received data, a policy that is...

LOOKOUT INC

EP3020584A1 : EPO Applications : 2021-12-08 : 4

☐ Cybersecurity Detection and Mitigation System Using Machine Learning and Advanced Data Correlation

Computer system security is often implemented using rules-based systems (e.g., allow traffic to this network port, deny it for those network ports; user A is allowed access to these files, but not those files). In enterprises, multiple such systems may be deployed, but fail to be able to...

PAYPAL INC

US20200280573 : US Applications : 2020-09-08 : 4

☐ Distributed security analysis for shared content

Methods and systems for providing a cost effective and robust security solution for shared files stored by file sharing software solutions are described herein. The methods and systems for generating a ledger associated with shared files, which may include scanning data received from applications...

CITRIX SYS INC

WO2020036724A1 : WIPO Applications : 2020-02-26 : 4

☐ Contextual and risk-based multi-factor authentication

A system for contextual and risk-based multi-factor authentication having a multi-dimensional time series data server configured to monitor and record a network's traffic data and to serve the traffic data to other modules and a directed computation graph module configured to receive network traffic...

COMPLX INC

US20180159852 : US Applications : 2018-06-07 : 4

Relevance

Publication Date

1999

First Our Assignees by Relevanc

ORACLE INTL CORP (22)
SECUREAUTH CORP (2)
AZOS AI LLC (1)
HELIOS DATA INC (3)
LOOKOUT INC (11)
PAYPAL INC (4)
CITRIX SYS INC (71)
COMPLX INC (1)

Charts based on top 1500 results

The present invention provides a policy specification framework to enable an enterprise to specify a given insider attack using a holistic view of a given data access, as well as the means to specify and implement one or more intrusion mitigation methods in response to the detection of such an

IBM TECH CORP

US20060971642 : US Applications : 2006-03-31 : 4

☐ Network security

A security platform that iteratively adapts to a changing security environment by creating and updating entity models based on observed activities and detecting patterns of events that deviate from these entity models.

SOPHOS LTD

WO201920097A1 : WIPO Applications : 2019-10-17 : 4

☐ Data management platform

Techniques are disclosed relating to the management of data. A data provider computer system may store particular data of a user. The data provider computer system may commence sharing of a portion of the particular data with a data consumer computer system. The data provider computer system may...

HELLOS DATA INC

US20200239143 : US Applications : 2020-07-23 : 4

☐ Data segmentation

Techniques are disclosed relating to data management. A computer system may evaluate network traffic to extract and group data objects based on their content satisfying similarity criteria, and to identify baseline behavior with respect to those data objects. The computer system may generate...

HELLOS DATA INC

US20200239124 : US Applications : 2020-07-23 : 4

☐ Key throttling to mitigate unauthorized file access

A file system extension for an endpoint controls access to files by selectively decrypting files under certain conditions. Where a pattern of access to the files suggests malicious and/or automated file access activity, the file system extension may limit the rate of file access by regulating the...

SOPHOS LTD

US20200038747 : US Applications : 2020-01-30 : 4

☐ Access control system for enterprise cloud storage

Systems and corresponding computer-implemented methods for context-based rule evaluation in an electronic data storage system are described. A request to perform an operation with respect to a resource is received from a client device, with the request including various attributes associated with...

BOX INC

US20170033867 : US Applications : 2017-03-30 : 4

☐ Key throttling to mitigate unauthorized file access

A file system extension for an endpoint controls access to files by selectively decrypting files under certain conditions. Where a pattern of access to the files suggests malicious and/or automated file access activity, the file system extension may limit the rate of file access by regulating the...

SOPHOS LTD

US10486522 : US Patents : 2019-11-05 : 4

☐ Emotion-based database security

A computer-implemented method is provided. The method may include determining a behavioral pattern of a user based on historical data access events and historical data access conditions corresponding to the historical data access events, wherein the data access events are associated with a computer

INTEL BUSINESS MACHINES CORP

US11062604 : US Patents : 2021-07-13 : 4

☐ Cloud based security monitoring using unsupervised pattern recognition and deep learning

Provided are systems and methods for a cloud security system that learns patterns of user behavior and uses the patterns to detect anomalous behavior in a network. Techniques discussed herein include obtaining activity data from a service provider system. The activity data describes actions...

ORACLE INTL CORP

US11166850 : US Patents : 2021-11-02 : 4

Data is collected from a set of devices according to a data collection policy. The data is associated with at least one of: device configuration, device state, or device behavior. A norm is established using the collected data. A different data collection policy is established based on the norm...

LOOKOUT INC

US20200368702 : US Applications : 2020-11-19 : 4

☐ Data security in a disconnected environment

Systems and methods are provided for the detection and prevention of intrusions in data at rest systems such as file systems and web servers. The systems and methods regulate access to sensitive data with minimal dependency on a communications network. Data access is quantitatively limited to...

PROTECTOR USA INC

US20140337623 : US Applications : 2014-11-13 : 4

☐ Ransomware file modification prevention technique

A computerized system and method to detect ransomware cyber-attacks is described. The approach entails analyzing the features associated with a file access event by a process operating on a computing device, to ascertain whether the process is associated with a ransomware cyber-attack.

MANDIANT INC

US10893068 : US Patents : 2021-01-12 : 4

☐ Technology for the safety for finding and managing application

Disclose the technology for application to be found and managed in the computing environment of tissue. The use that safety management system discovery is applied in a computing environment is to manage the access to application, the security threat and risk in computing environment to minimize...

ORACLE INTL CORP

ON108702367A : China Applications : 2018-10-23 : 4

☐ Systems and methods of secure self-service access to content

In one embodiment, a method is performed by a computer system. The method includes receiving a request from a user to access particular content. The method further includes determining a trust measure of the user, wherein the trust measure is based, at least in part, on an analysis of logged...

QUEST SOFTWARE INC

US9842230 : US Patents : 2017-12-12 : 4

☐ Labeling computing objects for improved threat detection

Processes executing on an endpoint are labelled as either "in", wherein the processes conform to a compliance policy administered for the endpoint from a remote threat management facility, or the processes are "out", wherein the processes do not conform to the compliance policy, thereby providing a...

SOPHOS LTD

G82585734A : Great Britain Applications : 2019-02-20 : 4

☐ User Authentication by Endpoint Device Using Local Policy Engine and Endpoint Data

Techniques are provided for authenticating a user using an endpoint device of the user with a local policy and endpoint data. One method comprises obtaining, at an endpoint device of a given user, behavioral anomalies from a remote engine that generates the behavioral anomalies based on behavior of...

DELL EMC

US20200242222 : US Applications : 2020-07-30 : 4

☐ Gracefully handling endpoint feedback when starting to monitor

A method, system and computer-useable medium for adaptively assessing risk associated with an endpoint, comprising: determining a risk level corresponding to an entity associated with an endpoint; selecting a frequency and a duration of an endpoint monitoring interval; collecting user behavior to...

FORCEPOINT FEDERAL HLDG LLC

US10842987 : US Patents : 2020-05-05 : 4

☐ Systems and methods for event-based authentication

More V



Main Concept Document

=====

US20200302074

Title: File access control based on analysis of user behavior patterns

(No Concept Modifiers)

=====

Filters (1)

=====

Earliest Priority Date: To 2019-03-22

Options

=====

De-dup: Extended Family Numbers

Cut-off: None

Sort: Relevance

Content: Patent Publications (164)

=====

US Patents

US Designs

US Applications

EPO Patents

EPO Applications

China Patents

China Applications

Japan Patents

Japan Applications

Korea Patents

Korea Applications

WIPO Applications

Argentina Patents

Argentina Applications

Brazil Patents

Brazil Applications

Canada Patents

Canada Applications

Chile Patents

Chile Applications

Colombia Applications

Costa Rica Applications
Cuba Patents
Cuba Applications
Dominican Republic Applications
Ecuador Patents
Ecuador Applications
El Salvador Applications
Guatemala Applications
Honduras Applications
Mexico Patents
Mexico Applications
Nicaragua Patents
Panama Applications
Peru Applications
Trinidad & Tobago Patents
Uruguay Applications
Austria Patents
Austria Applications
Belarus Patents
Belgium Patents
Belgium Applications
Bosnia & Herzegovina Patents
Bosnia & Herzegovina Applications
Bulgaria Patents
Bulgaria Applications
Croatia Patents
Croatia Applications
Czech Republic Patents
Czech Republic Applications
Czechoslovakia Patents
Czechoslovakia Applications
Denmark Patents
Denmark Applications
Estonia Patents
Estonia Applications
EUIPO Patents
Finland Patents
Finland Applications
France Patents
France Applications
Germany Patents
Germany Applications
Great Britain Patents
Great Britain Applications
Greece Patents
Greece Applications

Hungary Patents
Hungary Applications
Iceland Patents
Iceland Applications
Ireland Patents
Ireland Applications
Italy Patents
Italy Applications
Latvia Patents
Latvia Applications
Lithuania Patents
Lithuania Applications
Luxembourg Patents
Malta Patents
Monaco Patents
Montenegro Patents
Montenegro Applications
Netherlands Patents
Netherlands Applications
Norway Patents
Norway Applications
Poland Patents
Poland Applications
Portugal Patents
Portugal Applications
Republic of Moldova Patents
Republic of Moldova Applications
Romania Patents
Romania Applications
San Marino Patents
San Marino Applications
Serbia Patents
Serbia Applications
Slovakia Patents
Slovakia Applications
Slovenia Patents
Spain Patents
Spain Applications
Sweden Patents
Sweden Applications
Switzerland Patents
Switzerland Applications
Ukraine Patents
Yugoslavia/Serbia and Montenegro Patents
Yugoslavia/Serbia and Montenegro Applications
Armenia Patents

Australia Patents
Australia Applications
Cyprus Patents
Gulf Cooperation Council Patents
Hong Kong Patents
India Patents
India Applications
Indonesia Patents
Indonesia Applications
Israel Applications
Jordan Patents
Kyrgyzstan Patents
Macao Applications
Malaysia Patents
Mongolia Patents
New Zealand Patents
Philippines Patents
Philippines Applications
Saudi Arabia Patents
Singapore Patents
Singapore Applications
Taiwan Patents
Taiwan Applications
Tajikistan Patents
Tajikistan Applications
Thailand Applications
Uzbekistan Patents
Vietnam Patents
Algeria Patents
ARIPO Patents
ARIPO Applications
Egypt Patents
Kenya Patents
Malawi Patents
Morocco Patents
Morocco Applications
OAPI Patents
South Africa Patents
Tunisia Applications
Zambia Patents
Zimbabwe Patents
EAPO Patents
EAPO Applications
Georgia Patents
Georgia Applications
Kazakhstan Patents

Kazakhstan Applications

Russia Patents

Russia Applications

Turkey Patents

Turkey Applications

About 4,239 results

Sort by: Relevance Group by: None Deduplicate by: Family Results / page: 25

Secure execution of enterprise applications on mobile devices



US • US11134104B2 • Waheed Qureshi • Citrix Systems, Inc.
Priority 2011-10-11 • Filed 2019-05-02 • Granted 2021-09-28 • Published 2021-09-28
Similar A system is disclosed that includes components and features for enabling enterprise users to securely access enterprise resources (documents, data, application servers, etc.) using their mobile devices. An enterprise can use some or all components of the system to, for example, securely but ...

Systems and methods for providing mobile security based on dynamic attestation



WO US JP KR IL • US2020058832 • Srinivas Kumar • Tassera, Inc.
Priority 2012-05-01 • Filed 2012-07-27 • Granted 2014-09-30 • Published 2014-09-30
Similar Instrumented networks, machines and platforms having target subjects (devices, transactions, services, users, organizations) are disclosed. A security orchestration service generates runtime operational integrity profiles representing and identifying a level of threat or contextual trustworthiness ...

System and method for identifying unauthorized endpoints



US • US9479267B2 • Daryl E. Donley • Sophos Limited
Priority 2009-06-30 • Filed 2009-06-30 • Granted 2013-07-02 • Published 2013-07-02
Similar BACKGROUND 1. Field The present invention is related to identifying unauthorized endpoints. 2. Description of the Related Art Identifying unauthorized devices may include accessing each and every device on a network. Deploying network monitors in the form of hardware may be costly and complex.

Technology for detecting security vulnerabilities

WO EP US CN JP • JP6658812B2 • リヴェラ・シリコン・シマンテック コーポレーション Symantec Corporation
Priority 2013-06-28 • Filed 2014-06-26 • Granted 2017-01-11 • Published 2017-01-11
Similar A method executed on a server capable of communicating with a client, Assigning a reputation to the application; The method comprising the steps of: delivering the reputation to the client; Receiving monitored system behavior of the client executing the application from the client; Determining ...

System and method for dynamic security provisioning of computing resources



US • US9112536B2 • Mark Markow • American Express Travel Related Services Company, Inc.
Priority 2004-05-06 • Filed 2010-09-24 • Granted 2012-02-07 • Published 2012-02-07
Similar The present invention facilitates the dynamic provisioning of computing and data assets in a commodity computing environment. The invention provides a system and method for dynamically provisioning and de-provisioning computing resources based on multi-dimensional decision criteria. By employing ...

Systems and methods for privately performing application security analysis



WO EP US • EP3212243B1 • David Alexander Jevens • Proofpoint, Inc.
Priority 2014-10-31 • Filed 2015-10-30 • Granted 2020-09-09 • Published 2020-09-09
Similar A method, comprising the following steps performed by an application risk control system (504): receiving (505) a request from a mobile device (115, 510), the request comprising a cryptographic representation of application information for an application residing on the mobile device (115, 510) ...

Methods for behavioral detection and prevention of cyberattacks, and related ...



WO US • US11008775B2 • Jeffrey Albin Kraemer • Carbon Black, Inc.
Priority 2017-09-11 • Filed 2018-09-11 • Granted 2021-05-11 • Published 2021-05-11
Similar A security engine may use event-stream processing and behavioral techniques to detect ransomware. The engine may detect process behavior associated with encrypting a file, encrypting a storage device, or disabling a backup file, and may assign a ransomware category to the process based thereon.

Secure behavior analysis over trusted execution environment



WO US • US9756066B2 • Rajarshi Gupta • Qualcomm Incorporated
Priority 2012-08-15 • Filed 2015-12-03 • Granted 2017-09-05 • Published 2017-09-05
Similar Systems and methods for recognizing and reacting to malicious or performance-degrading behaviors in a mobile computing device include observing mobile device behaviors in an observer module within a privileged-normal portion of a secure operating environment to identify a suspicious mobile device ...

Methods and apparatus providing computer and network security utilizing ...



WO EP US • US9288935B2 • Jeffrey A. Kraemer • Cisco Technology, Inc.
Priority 2005-12-16 • Filed 2010-05-27 • Granted 2012-08-28 • Published 2012-08-28
Similar A system defines at least one key event to be monitored by at least one agent, and creates a graphical model for the at least one key event. The system observes the at least one key event. The system infers a degree of attack on the computer system based on an observation of the at least one key ...

1. *Pharmaceutical Innovation and the Role of the State*
 2. *The Impact of Patent Law on Drug Development*
 3. *The Role of Government in Regulating Pharmaceuticals*
 4. *The Impact of Globalization on the Pharmaceutical Industry*
 5. *The Role of the Pharmaceutical Industry in Public Health*

Similar. A computer implemented method to generate a classification scheme for configuration parameters of virtual machines (VMs) in a virtualized computing environment including: training a machine learning algorithm as a classifier based on a plurality of training data items, each training data item ...

Similar. A method for computer workstation based information protection is presented, the method comprises: a) monitoring user's actions on the computer workstation, b) analysis of the actions in respect to a pre-defined policy to determine whether the actions prejudice information to which the policy ...

Similar CROSS REFERENCE TO RELATED APPLICATIONS This application is continuation of U.S. application Ser. No. 15/402,883, filed Jan. 10, 2017, which is a continuation of U.S. application Ser. No. 14/034,147 (now U.S. Pat. No. 9,542,560), filed Sep. 23, 2013, which is a divisional of U.S. application Ser.

Similar. A computer-implemented method for enforcing data loss prevention policies on mobile devices may include (1) identifying a mobile device that connected to a network and that may include sensitive data and that is in a predetermined state that is designated for transferring data for data loss . . .

Similar: The present invention relates to a method and system for tracking the movement of data elements as they are shared and moved between authorized and unauthorized devices and among authorized and unauthorized users.

12

Similar: In a virtualized environment where multiple guest virtual machines receive security services from multiple security virtual machines, a guest virtual machine automatically transitions to a new virtual security machine under various conditions. For example, the guest virtual machine may select a ...

Similar. A security system and method secures and responds to security threats in a computer having a CPU, a Kernel/OS, and software applications. A low-level data collector intercepts a selection of first tier calls between the CPU and Kernel/OS, and stores associated first tier call IDs. A Kernel module ...

Similar: A system or method for network access protection executes steps for receiving, at a server, an access request for access to at least one network resource from a client machine, the access request including account authentication information comprising an account identifier and password, obtaining ...

Similar Systems, methods, and apparatus, including computer programs encoded on computer storage media, for detecting insider fraud. One method includes identifying one or more insider threat detection rules for an enterprise and obtaining behavioral data for an enterprise insider from multiple behavioral ...

Similar: A process control system software security architecture that more effectively protects against zero-day or other types of malware attacks, enabling the use of "minimal privileges" when executing applications and services are running within a computer device. The least privilege based architecture...

System and method for implementing content and network security inside a chip



US • [US20190245829A1](#) • Shlomo Touboul • Cpp Computing As
Priority 2008-03-26 • Filed 2019-04-19 • Published 2019-08-08

Similar Systems and methods for implementing content, streaming, and network security inside a chip or inside a computing device are disclosed. In exemplary embodiments, a system comprises a communication chip and a second processor. The communication chip comprises a router and security instructions. The ...

Calculating quantitative asset risk



WO EP US CN • [US2019044882](#) • Prasanna Ganapathi Basavepatra • McAfee, Inc.
Priority 2012-01-19 • Filed 2012-01-19 • Granted 2013-11-26 • Published 2013-11-26

Similar A standardized vulnerability score is identified for a particular vulnerability in a plurality of known vulnerabilities, the standardized vulnerability score indicating a relative level of risk associated with the particular vulnerability relative other vulnerabilities. A vulnerability detection ...

System and methods for malware detection using log based crowdsourcing analysis



US • [US20150361637A1](#) • Avly Raff • Seculert Ltd.
Priority 2010-07-21 • Filed 2015-06-15 • Published 2015-12-31

Similar A crowdsourcing log analysis system and methods for protecting computers and networks from malware attacks by analyzing data log information obtained from a plurality of client network. The client networks are associated with a set of network entities representing a plurality of business units or ...

Cross-user correlation for detecting server-side multi-target intrusion



WO US KR • [US2015265382](#) • Ezekiel Kruglick • Empire Technology Development Llc
Priority 2012-06-05 • Filed 2012-06-05 • Granted 2015-11-24 • Published 2015-11-24

Similar Technologies are generally described for time-correlating administrative events within virtual machines of a datacenter across many users and/or deployments. In some examples, the correlation of administrative events enables the detection of confluences of repeated unusual events that may indicate ...

System and method for facilitating malware scanning using reputation indicators



WO EP US CN JP KR AU CA ES HK IL RU SG • [JP2017234882](#) • ミルチェスク, ダニエル・アレクサンドル・ピットディフエンダー・アイビー・アール・マネジメントリミテッド
Priority 2013-09-27 • Filed 2014-09-25 • Granted 2018-04-25 • Published 2018-04-25

Similar Memory. A client system including at least one hardware processor connected to the memory and configured to run an anti-malware engine, the anti-malware engine configured to monitor malicious activity of a target process. The target process is executed on the client system, and the target process ...

Chain of custody for enterprise documents

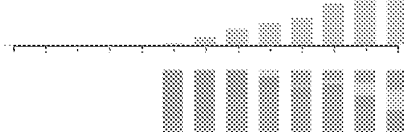


WO US GB • [US20192318128A1](#) • Karl Ackerman • Sophos Limited
Priority 2018-04-13 • Filed 2018-10-19 • Published 2019-10-17

Similar A ledger stores chain of custody information for files throughout an enterprise network. By identifying files with a homologous identifier such as a fuzzy hash that permits piecewise evaluation of similarity, the ledger can be used to track a chain of custody over a sequence of changes in content, ...

Next > >> About 4,239 results

Top 1000 results by filing date



Relative count of top 5 values

Assignees	Inventors	CPCs
Symantec Corporation		9.2%
International Business Machines Corporation		3.8%
Sophos Limited		2.2%
Amazon Technologies, Inc.		1.7%
Bank Of America Corporation		1.5%
Expand		

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L23	46	(Artificial Intelligence) More Like: US-20200302074-A1 Text: (WO-2019200317-A1 OR US-10558797-B2 OR CN-109597822-A OR JP-2020509511-A OR US-9485271-B1 OR US-20200007539-A1 OR US-20180007069-A1 OR US- 20180046796-A1 OR CN-110968888-A OR US-20200259836-A1 OR US-11165788-B2 OR US-20210084049-A1 OR JP-2019057133-A OR CN-110765488-A OR CN-110928880-A OR US-11176276-B1 OR DE-202018106629-U1 OR CN-110851847-A OR CN-110674140-A OR US-9219728-B1).did.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/03/03 11:51 AM
L24	13	L23 AND key	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/03/03 03:35 PM
L25	121	(holdback OR (hold\$ OR held OR keep\$ OR kept) ADJ back OR withheld OR withhold\$) near2 decrypt\$ NEAR key	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL,	OR	ON	ON	2022/03/03 03:48 PM

			PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L26	88	(holdback OR (hold\$ OR held OR keep\$ OR kept) ADJ back OR withheld OR withhold\$) near2 decrypt\$ NEAR key	(US-PGPUB; USPAT)	OR	ON	ON	2022/03/03 03:49 PM
L27	6169	(return\$ provid\$) near2 decrypt\$ NEAR key	(US-PGPUB; USPAT)	OR	ON	ON	2022/03/03 04:52 PM
L28	1	(return\$ provid\$) near2 decrypt\$ NEAR key WITH (scor\$ rank\$) WITH threshold	(US-PGPUB; USPAT)	OR	ON	ON	2022/03/03 04:54 PM
L29	1	(return\$ provid\$) near2 decrypt\$ NEAR key WITH (scor\$ rank\$) WITH threshold	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/03/03 04:54 PM
L30	7	(return\$ provid\$) near2 decrypt\$ NEAR key WITH (scor\$ rank\$)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/03/03 04:54 PM
L32	30	(return\$ provid\$) near2 decrypt\$ NEAR key WITH threshold	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA,	OR	ON	ON	2022/03/03 05:05 PM

			EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L33	1438	((("Fortinet") near3 ("Inc"))).AS,AANM.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/03/05 11:53 AM
L34	35	((("LITTLE") near3 ("Matthew")) OR (("GRAVES") near3 ("Jamie")) OR (("LEONARD") near3 ("Carson"))).INV.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2022/03/05 11:53 AM
L35	19	L33 AND (behavior NEAR pattern\$)	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/03/05 11:55 AM
L36	10	L33 AND (behavior NEAR user)	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/03/05 11:56 AM
L37	4	("20180069881" "20180351979" "8595497" "8887274").PN.	(US-PGPUB; USPAT)	OR	ON	ON	2022/03/05 11:56 AM
L38	9	(pattern\$ histor\$4) near2 user near2 (behavior behaviour) with (file near2 access)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/03/05 11:56 AM
L39	46	(pattern\$ histor\$4) near2 (behavior behaviour) with (file near2 access)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/03/05 11:56 AM
L40	121	user near2 (behavior behaviour) with (file near2 access)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/03/05 11:56 AM
L41	1	(cryptograph\$2 crypto) with wrapper with encapsulat\$3 with file with encrypt\$3	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/03/05 11:56 AM
L42	2	(cryptograph\$2 crypto) with wrapper with encapsulat\$3 with file	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/03/05 11:56 AM
L43	30	(cryptograph\$2 crypto) with wrapper with file	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/03/05 11:57 AM
L44	52	(pattern\$ histor\$4) with user with (behavior behaviour) with (file	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	ON	2022/03/05 11:57 AM

		near2 access)	IBM_TDB)				
L45	225151	(G06F21/6218 or G06F16/182 or G06N20/00 or H04L9/0819 or G06F21/602 or G06F21/316).cpc.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/03/05 11:58 AM
L46	11	L44 AND L45	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/03/05 11:59 AM
L47	106	(pattern\$ histor\$4) with user with (behavior behaviour) same (file near2 access)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/03/05 11:59 AM
L48	41	L47 AND L45	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/03/05 12:00 PM
L49	5	user same (access near2 request) same (file near2 access) same (risk near2 score)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/03/05 12:00 PM
L50	262	determin\$6 with user near4 locat\$3 with based with ip near address with request	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/03/05 12:00 PM
L51	21	determin\$6 with user near4 locat\$3 with based with ip near address with (access near2 request)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/03/05 12:00 PM
L52	58	determin\$6 with locat\$3 with based with ip near address with (access near2 request)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/03/05 12:00 PM
L53	0	correlat\$3 with locat\$3 with based with ip near address with (access near2 request)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/03/05 12:01 PM

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.

Downloaded v Side-by-si



WO EP US CN JP • [JP2014003381](#) • Ganesh Kirti • Oracle International Corporation
Priority 2017-06-22 • Filed 2018-06-19 • Granted 2021-11-10 • Published 2021-11-10
... statistics (including attempts and successes), file operations, access metrics, network download/upload metrics, application metrics (e.g., use, ...), using the activity data, one or more risk scores for the one or more users; determining that a risk score of said one or more risk scores for a user ...

Key throttling to mitigate unauthorized file access



US • [US10273448B2](#) • Russell Humphries • Sophos Limited
Priority 2016-06-10 • Filed 2019-10-01 • Granted 2021-04-13 • Published 2021-04-13
102 computing resources, including authentication, levels of access, risk assessment, and usage history tracking; rules for when an action is not ... may include transcribing the first one of the plurality of files for access using the first key. If the file is in use by the process and thus in a ...

Device and method for providing intent-based access control



US • [US2020025282](#) • Abdulaziz Mohammed Almahmadi • University Of Ontario Institute Of Technology
Priority 2014-07-07 • Filed 2015-07-07 • Granted 2017-07-11 • Published 2017-07-11
) . An integrated system could be deployed, for example, to secure physical access to a facility, a user's car, access to computer files. For example, ... , and the risk score, determining a level of access to be provided to the user; and providing access at the determined level of access to the user.

Detecting endpoint compromise based on network usage history



US • [US11155797B2](#) • Karl Ackerman • Sophos Limited
Priority 2016-04-22 • Filed 2017-04-05 • Granted 2021-11-02 • Published 2021-11-02
may generally control access to files 708 based on an exposure state, a security state, or other context such as the user of a calling process or the ... requesting access to a denied network location. In an embodiment, the information received from the facility may be a command or a command file.

Detecting triggering events for distributed denial of service attacks



US • [US20210344707A1](#) • Karl Ackerman • Sophos Limited
Priority 2016-04-22 • Filed 2021-07-08 • Published 2021-11-04
may generally control access to files 708 based on an exposure state, a security state, or other context such as the user of a calling process or the ... requesting access to a denied network location. In an embodiment, the information received from the facility may be a command or a command file.

Middleware security layer for cloud computing services



WO EP US JP • [JP2013084481](#) • クリシュナナラヤナスワミ, ネットスコープ, インク, Netskope
e, Inc.
Priority 2016-03-11 • Filed 2017-03-10 • Granted 2019-05-22 • Published 2019-05-22
... to the separate object store (API) request, a second data packet including a request to access the data object to receive at the proxy from the user ... -File name / owner / size / type-Application and instance name-File path-Tracking record including activity, user, access data-File version history- ...

Method and system for generating an entities view with risk-level scoring for ...



US • [US10586106B2](#) • Sudhakar Muddu • Splunk Inc.
Priority 2015-08-31 • Filed 2019-01-31 • Granted 2021-04-20 • Published 2021-04-20
By visually presenting analytical results scored with risk ratings and supporting evidence, the security platform enables network security ... The contextual settings can involve scenarios such as specific networking scenarios, user login scenarios, file access scenarios, application ...

Graph-based network anomaly detection across time and entities



US • [US10600039B2](#) • Georgios Apostolopoulos • Splunk Inc.
Priority 2017-01-30 • Filed 2018-12-13 • Granted 2020-03-31 • Published 2020-03-31
The contextual settings can involve scenarios such as specific networking scenarios, user login scenarios, file access scenarios, application ... adjust the scores. For example, a known attack pattern is a file transfer taking place after malware installation, which may increase the risk score.

System and method for secure three-party communications



US • [US8804181B1](#) • David P. Felscher • David P. Felscher
Priority 2001-03-23 • Filed 2012-11-20 • Granted 2014-12-02 • Published 2014-12-02
... into all aspects of business and daily life—entertainment, financial, medical, education, government, and communications—the concern over secure file ... 802 the Intermediary Private Session Key * User Public Session Key * Persistent Record (encryption or decryption) Key. An encrypted file is received

Combining internet routing information with access logs to assess risk of user ...



US • [US10721270B2](#) • Anoop Reddy • Citrix Systems, Inc.
Priority 2015-05-08 • Filed 2019-05-02 • Granted 2020-07-21 • Published 2020-07-21
405 via the hypervisor 401 in order to request access to a disk or a network. In still another embodiment, the guest operating system 410 and the With these techniques, a remote user may obtain a computing environment and access to server stored applications and data files from any network ...

Intermediate encryption for exposed content



US • [US10666827B2](#) • Harald Schutz • Sophos Limited
Priority 2016-04-14 • Filed 2016-04-14 • Granted 2020-06-16 • Published 2020-06-16
102 computing resources, including authentication, levels of access, risk assessment, and usage history tracking; rules for when an action is not ... may include combining the encrypted file, the object containing the decryption key, and application logic providing a user interface for accessing ...

Electronic device based security management background



WO EP US CN • [EP3455733B1](#) • Sudheer Koganti • Qualcomm Incorporated
Priority 2016-05-13 • Filed 2017-03-08 • Granted 2020-09-09 • Published 2020-09-09
Access to file system content for high value security applications -Allow access to all file system content for authenticated primary user -Deny ... Network access security policy -Allow access of application to file system content -Selectively restrict access of application to file system content ...

Network appliance for dynamic protection from risky network activities



US • [US9984225B2](#) • Tommy Stansen • Norse Networks, Inc.
Priority 2014-08-06 • Filed 2015-02-26 • Granted 2018-04-10 • Published 2018-04-10
... a user of the first computer being engaged in a risk activity; obtaining the first computer network address from the communication; assigning a risk ... records the IP Address of a user (101) connecting to a P2P service or engaged in P2P transactions, including file transfers and natural language ...

Event-driven malware detection for mobile devices



US GB • [US20190268302A1](#) • Sean Patrick McDonald • Sophos Limited
Priority 2016-06-10 • Filed 2019-05-15 • Published 2019-08-29
... requesting access to a denied network location, in an embodiment, the information received from the facility may be a command or a command file. ... may generally control access to files 708 based on an exposure state, a security state, or other context such as the user of a calling process or the ...

Behavioral-based control of access to encrypted content by a process



US • [US10665777B2](#) • Kenneth D. Ray • Sophos Limited
Priority 2016-02-12 • Filed 2017-11-20 • Granted 2020-08-19 • Published 2020-05-19
102 computing resources, including authentication, levels of access, risk assessment, and usage history tracking; rules for when an action is not ... access function may include an access request as generally contemplated by step 804 , which may initially include a request to open or create a file, ...

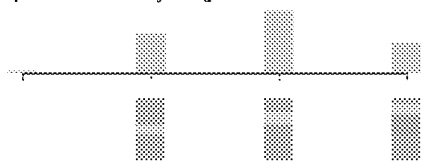
Just-in-time encryption



US • [US10628587B2](#) • Andreas Berger • Sophos Limited
Priority 2016-04-14 • Filed 2016-04-14 • Granted 2020-04-21 • Published 2020-04-21
102 computing resources, including authentication, levels of access, risk assessment, and usage history tracking; rules for when an action is not ... adding a file system extension to the endpoint, the file system extension providing use of a key to access files whenever a security state of the ...

Next > >> About 138,307 results

Top 1000 results by filing date



Relative count of top 5 values

Assignees	Inventors	CPCs
Commvault Systems, Inc.		11.3%
OneTrust, LLC		4.4%
Sophos Limited		4.4%
Splunk Inc.		3.2%
Oracle International Corporation		1.6%
Expand		

1 - 50

☐ Rule based trust evaluation using fuzzy logic in cloud computing

Presently, the cloud computing is a regarded research both in scholars and enterprise, because of its unique features such as low expenditure, easy maintenance, flexibility, fast deployment and reliable service. However to administer cloud computing, improvement in academic, legal and institutional...

IEEE Xplore : IEEE Conferences : 2017-09-01 : 4 : 2017 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) (Page(s): 510-514)

☐ CloudSky: A Controllable Data Self-Destruction System for Untrusted Cloud Storage Networks

In cloud services, users may frequently be required to reveal their personal private information which could be stored in the cloud to be used by different parts for different purposes. However, in a cloud-wide storage network, the servers are easily under strong attacks and also commonly experience...

IEEE Xplore : IEEE Conferences : 2015-06-01 : 4 : 2015 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (Page(s): 552-561)

☐ Agile Composition of Compliant Data Analytics Platforms

Sensitive data such as health records and financial transactions are increasingly being stored and processed in the cloud. Correspondingly, laws and regulations have been established to protect such data. For a cloud-based analytics service provider, it is of paramount importance to protect these sensitive...

IEEE Xplore : IEEE Conferences : 2017-04-01 : 4 : 2017 IEEE International Conference on Cloud Engineering (IC2E) (Page(s): 51-56)

☐ Insider attack and real-time data mining of user behavior

Early detection of employees' improper access to sensitive or valuable data is critical to limiting negative financial impacts to an organization, including regulatory penalties for misuse of customer data that results from these insider attacks. Implementing a system for detecting insider attacks...

IEEE Xplore : IBM Periodicals : 2007-05-01 : 4 : IBM Journal of Research and Development

☐ Turning Data into Insight with IBM Machine Learning for z/OS

The exponential growth in data over the last decade coupled with a drastic drop in cost of storage has enabled organizations to amass a large amount of data. This vast data becomes the new natural resource that these organizations must tap in to innovate and stay ahead of the competition, and they...

5024842100 : IBM Redbooks : 2018-05-11 : 4

☐ The Study and Design on Secure-Intranet Storage System

For the security issue in intranet storage systems, we design a data security storage system, which integrates information isolation, accessing control, virus detection, metadata safeguard of crucial data and fast-speed retrieval. This system can provide a solid foundation for data protection and...

IEEE Xplore : IEEE Conferences : 2010-10-01 : 4 : 2010 Third International Symposium on Information Processing (Page(s): 537-541)

☐ A Survey on Detection Techniques for Cryptographic Ransomware

Crypto-ransomware is a type of malware that encrypts user files, deletes the original data, and asks for a ransom to recover the hijacked documents. It is a cyber threat that targets both companies and residential users, and has spread in recent years because of its lucrative results. Several...

IEEE Xplore : IEEE Periodicals : 2019-01-01 : 4 : IEEE Access

☐ Security Architecture and Protocol for Trust Verifications Regarding the Integrity of Files Stored in Cloud Services †

Cloud computing is considered an interesting paradigm due to its scalability, availability and virtually unlimited storage capacity. However, it is challenging to organize a cloud storage service (CSS) that is safe from the client point-of-view and to implement this CSS in public clouds since it is...

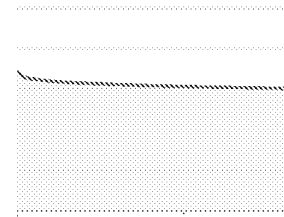
PM25876326 : PubMed Central : 2015-03-02 : 4 : Sensors (Basel, Switzerland), 15(3), 753

☐ Reduce Risk and Improve Security on IBM Mainframes. Volume 1 Architecture and Platform Security

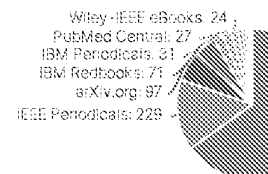
This IBM® Redbooks® publication documents the strength and value of the IBM security strategy with IBM System z® hardware and software. In an age of increasing security consciousness, IBM System z provides the capabilities to address the needs of today's business security challenges. This...

5024780301 : IBM Redbooks : 2014-12-08 : 4

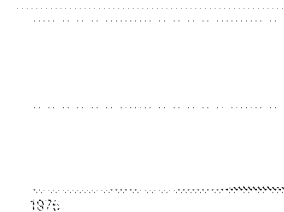
Relevance



Collections



Publication Date



Charts based on top 1500 results

Threats come from a variety of sources. Insider threats, as well as malicious hackers, are not only difficult to detect and prevent, but many times the authors of these threats are using resources without anybody being aware that those threats are there. Threats would not be harmful if there were no...

5024758101 : IBM Redbooks : 2011-02-17 : 4

Countering Network-Centric Insider Threats through Self-Protective Autonomic Rule Generation

Insider threats are a growing problem in today's organizations. Detecting such attacks is especially challenging because most system owners and system administrators use networks to remotely manage the systems they are responsible for. In previous work, we introduced the Autonomic Violation...

IEEE Xplore : IEEE Conferences : 2012-06-01 : 4 : 2012 IEEE Sixth International Conference on Software Security and Reliability (Page(s): 273-282)

Securing Data in Storage: A Review of Current Research

Protecting data from malicious computer users continues to grow in importance. Whether preventing unauthorized access to personal photographs, ensuring compliance with federal regulations, or ensuring the integrity of corporate secrets, all applications require increased security to protect data...

cs3408034 : arXiv.org : 2004-09-17 : 4

Gargoyle: A Network-based Insider Attack Resilient Framework for Organizations

Anytime, Anywhere' data access model has become a widespread IT policy in organizations making insider attacks even more complicated to model, predict and deter. Here, we propose Gargoyle, a network-based insider attack resilient framework against the most complex insider threats within a pervasive...

IEEE Xplore : IEEE Conferences : 2016-10-01 : 4 : 2016 IEEE 43rd Conference on Local Computer Networks (LCN) (Page(s): 553-561)

Passive security intelligence to analyze the security risks of mobile/BYOD activities

As enterprises embrace mobile technologies and enable their employees to bring their own devices, traditional security mechanisms are challenged by the co-location of personal and business activities on employee-owned mobile devices on the enterprise network. This presents a new risk to enterprises...

IEEE Xplore : IBM Periodicals : 2016-07-01 : 4 : IBM Journal of Research and Development

Design and implementation of an improved cloud storage system

The detailed designs, technologies and implementations of cloud storage are presented, including the multi-tenant concurrency, separated framework between buffer and business etc. Master/Workers partition algorithm is adopted to improve the reading and writing efficiency for big data in the cloud...

IEEE Xplore : IEEE Conferences : 2016-06-01 : 4 : 2016 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD) (Page(s): 1616-1623)

Design Issues of Trustworthy Cloud Platform Based on IP Monitoring and File Risk

With the rising popularity of Web applications and cloud computing technology, a secure cloud computing environment is one of the main concerns. Currently, enterprise cloud platforms often rely on their maintenance and operation, and medium and small companies cannot effectively save manpower...

IEEE Xplore : IEEE Conferences : 2016-09-01 : 4 : 2016 IEEE Fifth International Conference on Big Data and Cloud Computing (Page(s): 110-117)

A survey on miscellaneous attacks in Hadoop framework

The world is progressing towards innovative advancement step by step bringing about an exponential rise in data. This enormous volume of data has presented the possibility of Big data, which has caught the consideration of business and IT researchers as a gift and a source of various opportunities...

IEEE Xplore : IEEE Conferences : 2016-01-01 : 4 : 2016 2nd International Conference on Inventive Systems and Control (ICISCI) (Page(s): 1043-1046)

Security intelligence for cloud management infrastructures

In this paper, we address the problem of protecting cloud infrastructures and customer workloads via smart auditing and logging, satisfying regulatory and compliance requirements. We observe that traditional approaches of logging and auditing events in cloud-scale infrastructures will not be...

IEEE Xplore : IBM Periodicals : 2016-07-01 : 4 : IBM Journal of Research and Development

Multitenant Access Control for Cloud-Aware Distributed Filesystems

In a virtualization environment that serves multiple tenants (independent organizations), storage consolidation at the filesystem level is desirable because it enables data sharing, administration efficiency, and performance optimizations. The scalable deployment of filesystems in such environments...

IEEE Xplore : IEEE Periodicals : 2017-06-15 : 4 : IEEE Transactions on Dependable and Secure Computing



computing

Context Integrity Measurement Architecture (CI-MIA) was inspired by risk assessments used by credit card companies. These assessments flag excursions from "normal" or "typical" behavior. If an excursion exceeds some threshold level, the card companies require additional proof of identity before...

IEEE Xplore : IEEE Conferences : 2016-10-01 : 4 : 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCCON) (Page(s): 1-10)

☐ Computer Software Security

This chapter contains sections titled: Specific Operating Systems (OSS) Applications Example Detailed Security Requirements for Specific Operating Systems and Applications Chapter Summary Further Reading and Resources Questions Exercises

IEEE Xplore : Wiley-IEEE eBooks : 2011-01-01 : 4 : Wiley-IEEE Press 2011 (Edition: 1, Pages: 512)

☐ Deployment Guide for InfoSphere Guardium

IBM® InfoSphere® Guardium® provides the simplest, most robust solution for data security and data privacy by assuring the integrity of trusted information in your data center. InfoSphere Guardium helps you reduce support costs by automating the entire compliance auditing process across heterogeneous...

5024812500 : IBM Redbooks : 2014-03-19 : 4

☐ IEEE Standard for information Technology: Hardcopy Device and System Security

This standard defines security requirements (all aspects of security including but not limited to authentication, authorization, privacy, integrity, device management, physical security and information security) for manufacturers, users, and others on the selection, installation, configuration and...

IEEE Xplore : IEEE Standards : 2006-06-30 : 4 : IEEE Std 2600-2006 (Page(s): 1-177)

☐ FileWall: A Firewall for Network File Systems

Access control in network file systems relies on primitive mechanisms like access control lists and permission bits, which are not enough when operating in a hostile network environment. Network middleboxes, e.g., firewalls, completely ignore file system semantics when defining policies. Therefore,...

IEEE Xplore : IEEE Conferences : 2007-09-01 : 4 : Third IEEE International Symposium on Dependable, Autonomic and Secure Computing (DA-SC 2007) (Page(s): 153-162)

☐ Detecting and Preventing Cyber Insider Threats: A Survey

Information communications technology systems are facing an increasing number of cyber security threats, the majority of which are originated by insiders. As insiders reside behind the enterprise-level security defence mechanisms and often have privileged access to the network, detecting and...

IEEE Xplore : IEEE Periodicals : 2018-01-31 : 4 : IEEE Communications Surveys & Tutorials

☐ The study and design on secure-cloud storage system

For the security issue in cloud storage systems, we design a cloud security storage system (for short CSSS). Firstly, The CSSS integrates information isolation, accessing control, virus detection, metadata safeguard of crucial data and fast-speed retrieval; Secondly, with the help of connect control...

IEEE Xplore : IEEE Conferences : 2011-08-01 : 4 : 2011 International Conference on Electrical and Control Engineering (Page(s): 5120-5126)

☐ Software agents and computer network security

Preventing unauthorised access to corporate information systems is essential for many organisations. To address this problem we built a security enhancement software system using software agents, in which a core software agent resides on a server and user end software agents reside at each user...

IEEE Xplore : IEEE Conferences : 2000-01-01 : 4 : Proceedings Seventh IEEE International Conference and Workshop on the Engineering of Computer-Based Systems (ECBS 2000) (Page(s): 211-217)

☐ EndBox: Scalable Middlebox Functions Using Client-Side Trusted Execution

Many organisations enhance the performance, security, and functionality of their managed networks by deploying middleboxes centrally as part of their core network. While this simplifies maintenance, it also increases cost because middlebox hardware must scale with the number of clients. A promising...

IEEE Xplore : IEEE Conferences : 2018-06-01 : 4 : 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (Page(s): 1-10)

[More V](#)

Main Concept Document

=====

US20200302074

Title: File access control based on analysis of user behavior patterns

(No Concept Modifiers)

=====

Filters (1)

=====

Publication Date: To 2019-03-22

Options

=====

De-dup: None

Cut-off: None

Sort: Relevance

Content: Non-Patent Literature (23)

=====

IEEE Xplore Publications: IEEE Periodicals

IEEE Xplore Publications: IEEE Conferences

IEEE Xplore Publications: IEEE Standards

IEEE Xplore Publications: IEEE Early Access

IEEE Xplore Publications: SMPTE Periodicals

IEEE Xplore Publications: SMPTE Conferences

IEEE Xplore Publications: SMPTE Standards

IEEE Xplore Publications: MIT Press eBooks

IEEE Xplore Publications: Wiley-IEEE eBooks

IEEE Xplore Publications: IBM Periodicals

IEEE Xplore Publications: URSI Periodicals

IEEE Xplore Publications: VDE Conferences

IEEE Xplore Publications: Periodicals from China

IP.com Prior Art Database: The IP.com Journal

IP.com Prior Art Database: Internet Society RFC

IP.com Prior Art Database: IBM TDB Archive

IP.com Prior Art Database: Legacy Journals

IP.com Prior Art Database: Software Patent Institute

OnePetro.org: Periodicals at OnePetro.org

OnePetro.org: Conferences at OnePetro.org

Other Literature: IBM Redbooks

IQSearchText-202203051642.txt

Other Literature: PubMed Central

Other Literature: arXiv.org

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA VA 22313-1451

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE PAID
POSTEDIGITAL
NNNNN

Douglas M. Hamilton
HDC Fortinet
224 S. Main Street, 114
Springville, UT 84663



**Courtesy Reminder for
Application Serial No: 16/362,167**

Attorney Docket No: FORT-031800(18167)
Customer Number: 176502
Date of Electronic Notification: 03/10/2022

This is a courtesy reminder that new correspondence is available for this application. If you have not done so already, please review the correspondence. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:

miquelchamilton@hamiltonshome.com
dhamilton@hdciplaw.com

To view your correspondence online or update your email addresses, please visit us anytime at **<https://ppair-my.uspto.gov/pair/PrivatePair>**.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov or call 1-866-217-9197.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875				Application or Docket Number 16/362,167		Filing Date 03/22/2019		☐ To be Mailed			
ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO											
APPLICATION AS FILED - PART I											
		(Column 1)		(Column 2)							
FOR		NUMBER FILED		NUMBER EXTRA		RATE (\$)		FEE (\$)			
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))		N/A		N/A		N/A					
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))		N/A		N/A		N/A					
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		N/A		N/A		N/A					
TOTAL CLAIMS (37 CFR 1.16(j))		minus 20 = *				x \$100 =					
INDEPENDENT CLAIMS (37 CFR 1.16(h))		minus 3 = *				x \$460 =					
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))		If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).									
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))											
* If the difference in column 1 is less than zero, enter "0" in column 2.						TOTAL					
APPLICATION AS AMENDED - PART II											
		(Column 1)		(Column 2)		(Column 3)					
AMENDMENT	04/26/2022	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR		PRESENT EXTRA		RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	* 15	Minus	** 20	= 0			x \$100 =		0	
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0			x \$480 =		0	
	☐ Application Size Fee (37 CFR 1.16(s))										
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))										
								TOTAL ADD'L FEE		0	
		(Column 1)		(Column 2)		(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR		PRESENT EXTRA		RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	*	Minus	**	=			x \$0 =			
	Independent (37 CFR 1.16(h))	*	Minus	***	=			x \$0 =			
	☐ Application Size Fee (37 CFR 1.16(s))										
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))										
								TOTAL ADD'L FEE			
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.								LIE			
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".								/JAMES W TUNSTALL/			
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".											
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.											

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Fortinet, Inc. First Inventor: Little App. No.: 16/362,167 Filed: March 19, 2020 For: DETECTING ACCESSSS POINTS LOCATED WITHIN PROXIMITY OF A COMPUTING DEVICE FOR TROUBLESHOOTING OF A NETWORK	Examiner: YANG Group Art Unit: 2493 Conf. No.: 6553 Docket No.: FORT-031800(18167)
--	---

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE TO OFFICE ACTION

Sir/Madam:

In response to the final Office action having a notification date of March 10, 2022 (the “Office Action”), the Applicant respectfully requests the Examiner to enter the following amendment and to consider the following remarks:

Amendments to the Claims begin at page 2 of this paper.

Remarks begin at page 7 of this paper.

Amendments to the Claims

1. (Currently Amended) A method comprising:

obtaining and storing, by one or more servers associated with an enterprise network, information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users;

receiving, by the one or more servers, a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the enterprise network in encrypted form;

responsive to receipt of the file access request, determining, by the one or more servers, a risk score for the first user based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request; and

based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key, wherein said permitting or denying comprises:

when the risk score is less than a first threshold, returning the decryption key and providing full access to the file; ~~and~~

when the risk score is greater than a second threshold, withholding the decryption key; and

when the risk score is between the first threshold and the second threshold, returning the decryption key and providing limited access to the file.

2. (Previously Presented) The method of claim 1, wherein said determining, by the one or more servers, the risk score for the first user comprises evaluating the file access request with reference to a model of user behavior developed by machine-learning.

3. (Original) The method of claim 1, wherein the information regarding historical user behavior includes for each user of the plurality of users:

historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time;

historical data regarding observed locations of the user; and

historical data regarding observed times at which the user accesses files.

4. (Original) The method of claim 1, wherein the observed data includes a current location of the first user as determined based on a source Internet Protocol (IP) address contained in the file access request.

5. (Original) The method of claim 1, wherein the observed data includes a status indicative of whether the connection through which the first user initiated the file access request is trusted or untrusted.

6. (Original) The method of claim 5, wherein the connection is trusted when the first user is on the enterprise network or accessing the enterprise network remotely via a secure connection.

7. (Original) The method of claim 5, wherein the connection is untrusted when the first user is not on the enterprise network or accessing the enterprise network remotely via an insecure connection.

8. (Original) The method of claim 1, wherein the encrypted form involves the file being encapsulated in a cryptographic wrapper.

9-11. (Canceled)

12. (Currently Amended) A non-transitory computer-readable storage medium embodying a set of instructions, which when executed by one or more processors of one or more servers associated with an enterprise network, causes the one or more processors to perform a method comprising:

obtaining and storing information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users, wherein the information regarding historical user behavior includes for each user of the plurality of users:

historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time;

historical data regarding observed locations of the user; and

historical data regarding observed times at which the user accesses files;

receiving a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the enterprise network in encrypted form;

responsive to receipt of the file access request, determining a risk score for the first user based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request; and

based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key; wherein said permitting or denying comprises:

when the risk score is less than a first threshold, returning the decryption key and providing full access to the file; and

when the risk score is greater than a second threshold, withholding the decryption key; and

when the risk score is between the first threshold and the second threshold, returning the decryption key and providing limited access to the file.

13. (Previously Presented) The non-transitory computer-readable storage medium of claim 12, wherein said determining the risk score for the first user comprises evaluating the file access request with reference to a model of user behavior developed by machine-learning.

14. (Canceled)

15. (Original) The non-transitory computer-readable storage medium claim 13, wherein the observed data includes a current location of the first user as determined based on a source Internet Protocol (IP) address contained in the file access request.

16. (Original) The non-transitory computer-readable storage medium claim 13, wherein the observed data includes a status indicative of whether the connection through which the first user initiated the file access request is trusted or untrusted.

17. (Original) The non-transitory computer-readable storage medium claim 13, wherein the encrypted form involves the file being encapsulated in a cryptographic wrapper.

18-21. (Canceled)

22. (Previously Presented) A system, the system comprising:

one or more processors; and

a non-transitory computer-readable storage medium coupled to the one or more processors and embodying a set of instructions, which when executed by the one or more processors of one or more servers associated with an enterprise network, causes the one or more processors to perform a method comprising:

obtaining and storing information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users;

receiving a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the enterprise network in encrypted form;

responsive to receipt of the file access request, determining a risk score for the first user based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request; and

based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key, wherein said permitting or denying comprises:

when the risk score is less than a first threshold, returning the decryption key and providing full access to the file; ~~and~~

when the risk score is greater than a second threshold, withholding the decryption key; and

when the risk score is between the first threshold and the second threshold, returning the decryption key and providing limited access to the file

23-24. (Canceled)

25. (Previously Presented) The system of claim 22, wherein the information regarding historical user behavior includes for each user of the plurality of users:

historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time;

historical data regarding observed locations of the user; and

historical data regarding observed times at which the user accesses files.

Remarks

The undersigned respectfully requests reconsideration of the above-captioned patent application in view of the following remarks. Claims 1-8, 10, 12, 13, and 15-25 were pending. Claims 1, 12, and 22 have been amended, claims 10, 14, 18-21, and 23-24 have been canceled. Hence, claims 1-8, 12-13, 15-17, 22, and 25 remain pending. Claims 1-3, 5-7, 10, 12-13, 16, 18-20, 22-23, and 25 stand rejected under 35 USC 103 as allegedly obvious over a combination US Pat. Pub. No. 2019/0319945 (hereinafter “Levy”) and US Pat. Pub. No. 2004/0221172 (hereinafter “Stamos”). Claims 4 and 15 stand rejected under 35 USC 103 as allegedly obvious over a combination Levy, Stamos, and US Pat. Pub. No. 2014/03100779 (hereinafter “Lof”). Claims 8 and 17 stand rejected under 35 USC 103 as allegedly obvious over a combination Levy, Stamos, and US Pat. Pub. No. 2005/0229258 (hereinafter “Pigin”). Applicant respectfully amends in part and traverses in part to overcome the rejections.

Claim 1 has been amended to include the limitations of original claim 10. Thus, as amended claim 1 sets forth a method that includes, *inter alia*, determining a risk score for a first user based on a plurality of factors, and based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key. The permitting or denying includes: when the risk score is less than a first threshold, returning the decryption key and providing full access to the file; when the risk score is greater than a second threshold, withholding the decryption key; and when the risk score is between the first threshold and the second threshold, returning the decryption key and providing limited access to the file.

At the outset, it is noted that Levy and Stamos are not properly combinable as the combination would render the system of Stamos inoperative for its intended purpose. In particular, Stamos discloses that a centralized document storage with centralized access control requires “overhead [that] can become cumbersome . . .” Stamos at ¶¶0009-0013. To avoid such cumbersome implementations, Stamos expressly implements a system that avoids the use of prior art authentication, but rather simply provides a decryption key based upon “the sensitivity of the information stored in a document, [and] also based upon a proposed action to be taken with [the document].” Stamos at ¶¶0014-0018. The

proposed combination of Levy and Stamos not only does not render the claims obvious, it would result in the cumbersome system that Stamos was expressly trying to avoid rendering it inoperable for its intended purpose. It is noted that the Office Action specifically relies upon the disclosure of Stamos that is expressly disclosed as not included in Stamos to avoid being cumbersome. See e.g., Office Action at p. 6 citing Stamos at ¶¶0008-0009. One of ordinary skill in the art would not be motivated to combine references in a way that results in a situation decried by the combined reference itself. For at least this reason, the rejection of claim 1 should be withdrawn and the claim allowed. Such allowance is respectfully requested herein.

It is noted that the Office Action specifically relies upon the disclosure of Stamos that is expressly disclosed as not included in Stamos to avoid being cumbersome. See e.g., Office Action at p. 6 citing Stamos at ¶¶0008-0009. Again, one of ordinary skill in the art would not be motivated to combine teachings of Stamos that are “cumbersome” and unnecessary.

Further, even if the cited references are properly combinable, *which they are not*, the combination does not render claim 1 obvious. In particular, Levy is limited to disclosure of use of an “additional authentication factor” where a risk score is “below a threshold such that it indicates that the user and device are safe”. Levy at ¶0213. In contrast, where the risk score is above the threshold, “the additional authentication factor” is withheld. Id. In all disclosed implementations, Levy specifically compares the risk score with a single threshold yielding a binary access result. Levy at ¶¶0211-0213. This is in stark contrast to claim 1 where two thresholds are used to differentiate between a non-binary result set: (a) providing a decryption key and providing full access to the file, (b) not providing the decryption key, and (c) providing the decryption key yet providing only limited access as set forth in claim 1. Stamos does not disclose, teach or suggest a cure for the defect in Levy, and indeed is not even alleged to do so. It thus follows that the combination of Levy and Stamos does not disclose, teach, or suggest each and every limitation of claim 1. For at least this reason the rejection of claim 1 should be withdrawn and the claim allowed. Such allowance is respectfully requested herein.

Additionally, each of claims 12 and 22 includes a limitation similar to that discussed above in relation to claim 1, and are each in condition for allowance for at least this reason. Such allowance is respectfully requested herein. Further, claims 2-8, 13, 15-17, and 25 each depend from an allowable base claim, and are thus in condition for allowance for at least this reason. Such allowance is respectfully requested herein.

Conclusion

The undersigned respectfully submits that the amendments and remarks presented herein have overcome the rejections, and that the pending claims are in condition for allowance. Accordingly, the undersigned respectfully requests that the rejections be withdrawn and that a Notice of Allowance be promptly issued for the pending claims.

By responding in the foregoing remarks only to particular positions taken by the Examiner, the Applicant does not acquiesce with any other positions that have not been explicitly addressed. Applicant's arguments for the patentability of a claim should not be understood as implying that no other reasons for the patentability of that claim exist. The absence of a reply to a specific rejection, issue or comment set forth in the Office Action does not signify agreement with or concession of that rejection, issue or comment. In addition, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, and the amendment of any claim does not necessarily signify any concession of unpatentability of the claim prior to its amendment.

Request for a Telephone Interview

If the Examiner believes a telephone conference would expedite prosecution of the above-captioned patent application, please telephone the undersigned at (720) 266-4728.

Respectfully submitted,

HDC Intellectual Property Law, LLP

Date April 2022

By /Douglas M. Hamilton/
Douglas M. Hamilton
Reg. No. 47,629

Electronic Acknowledgement Receipt	
EFS ID:	45563232
Application Number:	16362167
International Application Number:	
Confirmation Number:	6553
Title of Invention:	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS
First Named Inventor/Applicant Name:	Matthew J. Little
Customer Number:	176502
Filer:	Douglas M. Hamilton
Filer Authorized By:	
Attorney Docket Number:	FORT-031800(18167)
Receipt Date:	26-APR-2022
Filing Date:	22-MAR-2019
Time Stamp:	13:15:10
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment		no			
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		FORT-031800ResponsetoOAMa iled03102022.pdf	53065 3b3d470f131acd509173a4ed44a0075e69f 83774	yes	10

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Response After Final Action	1	1
	Claims	2	6
	Applicant Arguments/Remarks Made in an Amendment	7	10
Warnings:			
Information:			
Total Files Size (in bytes):		53065	
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>			



NOTICE OF ALLOWANCE AND FEE(S) DUE

176502 7590 05/18/2022
Douglas M. Hamilton
HDC Fortinet
224 S. Main Street, 114
Springville, UT 84663

EXAMINER

YANG, HAN

ART UNIT

PAPER NUMBER

2493

DATE MAILED: 05/18/2022

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/362,167	03/22/2019	Matthew J. Little	FORT-031800(18167)	6553

TITLE OF INVENTION: FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1200	\$0.00	\$0.00	\$1200	08/18/2022

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

176502 7590 05/18/2022
Douglas M. Hamilton
HDC Fortinet
224 S. Main Street, 114
Springville, UT 84663

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/362,167	03/22/2019	Matthew J. Little	FORT-031800(18167)	6553

TITLE OF INVENTION: FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1200	\$0.00	\$0.00	\$1200	08/18/2022

EXAMINER	ART UNIT	CLASS-SUBCLASS
YANG, HAN	2493	713-165000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

- (1) The names of up to 3 registered patent attorneys or agents OR, alternatively, 1 _____
- (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 _____
- 3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☐ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

- ☐ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)
- ☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. Change in Entity Status (from status indicated above)

- ☐ Applicant certifying micro entity status. See 37 CFR 1.29
- ☐ Applicant asserting small entity status. See 37 CFR 1.27
- ☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/362,167	03/22/2019	Matthew J. Little	FORT-031800(18167)	6553
176502	7590	05/18/2022	EXAMINER	
Douglas M. Hamilton			YANG, HAN	
HDC Fortinet			ART UNIT	PAPER NUMBER
224 S. Main Street, 114			2493	
Springville, UT 84663			DATE MAILED: 05/18/2022	

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b) (2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 16/362,167	Applicant(s) Little et al.	
	Examiner HAN YANG	Art Unit 2493	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to Amendment on 4/26/2022.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are See Continuation Sheet. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov**.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐ All b) ☐ Some* c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.

2. ☐ Certified copies of the priority documents have been received in Application No. _____.

3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)	5. ☒ Examiner's Amendment/Comment
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.	6. ☒ Examiner's Statement of Reasons for Allowance
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.	7. ☐ Other _____.
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date. <u>5/5/2022</u> .	

/H.Y./ Examiner, Art Unit 2493	/CARL G COLIN/ Supervisory Patent Examiner, Art Unit 2493
-----------------------------------	--

Continuation of 3. The allowed claim(s) is/are: 1-8,12-13,15-17,22 and 25

DETAILED ACTION

Notice of AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

The present office action is responsive to communications received on 4/26/2022. Applicant cancelled claims 10, 18-21, and 23-24. Claims 1-8, 12-13, 15-17, 22, and 25 are pending.

Response to Arguments

Applicant's arguments, filed 4/26/2022, and with this Examiner's Amendment, have been fully considered and are persuasive. All previous rejections have been withdrawn.

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

An examiner's amendment to the record appears below (claim 22 should end with a **period** to comply with MPEP § 608.01(m)), which is based on claims submitted 4/26/2022. Rest of the claims remain the same.

Claim 22 (p. 6)

add period "." at the end of the claim.

Allowable Subject Matter

The claims 1-8, 12-13, 15-17, 22, and 25 are allowed.

This communication warrants no examiner's reason for allowance, as applicant's reply makes evident the reason for allowance, satisfying the record as whole as required by rule 37 CFR 1.104 (e). In this case, the substance of applicant's remarks in the Amendment filed on 4/26/2022 point out the reasons claims are patentable over the prior art of record. Thus, the reason for allowance is in all probability evident from the record and no statement for examiner's reason for allowance is necessary (see MPEP 1302.14).

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HAN YANG whose telephone number is (408)918-7638. The examiner can normally be reached on Monday to Friday, 9:00-5:00.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Carl Colin can be reached on (571) 272-3862. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/H.Y./
Examiner, Art Unit 2493

/CARL G COLIN/
Supervisory Patent Examiner, Art Unit 2493

<i>Examiner-Initiated Interview Summary</i>	Application No. 16/362,167	Applicant(s) Little et al.		
	Examiner HAN YANG	Art Unit 2493	AIA (First Inventor to File) Status Yes	Page 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	Title	Type
HAN YANG	Examiner	Telephonic
Hamilton, Douglas	Attorney of Record	

Date of Interview: 05 May 2022

Issues Discussed:

Proposed Amendment(s)

Examiner contacted attorney to propose the following examiner amendment to fix minor issue and expedite prosecution.

Claim 22: need to add period "." at the end of the claim to comply with MPEP § 608.01(m).

/HAN YANG/ Examiner, Art Unit 2493	/CARL G COLIN/ Supervisory Patent Examiner, Art Unit 2493
<p>Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04</p> <p>Please further see: MPEP 713.04 Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b) 37 CFR § 1.2 Business to be transacted in writing</p>	

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

Issue Classification 	Application/Control No. 16/362,167	Applicant(s)/Patent Under Reexamination Little et al.
	Examiner HAN YANG	Art Unit 2493

CPC						
Symbol					Type	Version
G06F	/	21	/	6218	F	2013-01-01
G06F	/	16	/	182	I	2019-01-01
G06N	/	20	/	00	I	2019-01-01
H04L	/	9	/	0819	I	2013-01-01
G06F	/	21	/	602	I	2013-01-01

CPC Combination Sets				
Symbol	Type	Set	Ranking	Version
/				

/HAN YANG/ Examiner, Art Unit 2493 (Assistant Examiner)	06 May 2022 (Date)	Total Claims Allowed: 15	
/CARL G COLIN/ Supervisory Patent Examiner, Art Unit 2493 (Primary Examiner)	11 May 2022 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 3A

U.S. Patent and Trademark Office

Part of Paper No.: 20220506

Issue Classification 	Application/Control No. 16/362,167	Applicant(s)/Patent Under Reexamination Little et al.
	Examiner HAN YANG	Art Unit 2493

INTERNATIONAL CLASSIFICATION		
CLAIMED		
G06F21/62	/ 21	/ 62

NON-CLAIMED		
/	/	/

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS

CROSS REFERENCES(S)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)					

/HAN YANG/ Examiner, Art Unit 2493 (Assistant Examiner)	06 May 2022 (Date)	Total Claims Allowed: 15	
/CARL G COLIN/ Supervisory Patent Examiner, Art Unit 2493 (Primary Examiner)	11 May 2022 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 3A

U.S. Patent and Trademark Office

Part of Paper No.: 20220506

Issue Classification 	Application/Control No. 16/362,167	Applicant(s)/Patent Under Reexamination Little et al.
	Examiner HAN YANG	Art Unit 2493

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47															
CLAIMS															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1		10		19										
2	2		11		20										
3	3	9	12		21										
4	4	10	13	14	22										
5	5		14		23										
6	6	11	15		24										
7	7	12	16	15	25										
8	8	13	17												
	9		18												

/HAN YANG/ Examiner, Art Unit 2493 (Assistant Examiner)	06 May 2022 (Date)	Total Claims Allowed: 15	
/CARL G COLIN/ Supervisory Patent Examiner, Art Unit 2493 (Primary Examiner)	11 May 2022 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 3A

U.S. Patent and Trademark Office

Part of Paper No.: 20220506

Search Notes 	Application/Control No. 16/362,167	Applicant(s)/Patent Under Reexamination Little et al.
	Examiner HAN YANG	Art Unit 2493

CPC - Searched*		
Symbol	Date	Examiner
G06F 21/6218 21/602 21/316	09/25/2021	HY
G06F 16/182	09/25/2021	HY
G06N 20/00	09/25/2021	HY
H04L 9/0819	09/25/2021	HY

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

/H.Y./ Examiner, Art Unit 2493	
-----------------------------------	--

<i>Search Notes</i> 	Application/Control No. 16/362,167	Applicant(s)/Patent Under Reexamination Little et al.
	Examiner HAN YANG	Art Unit 2493

Search Notes		
Search Notes	Date	Examiner
G06F 21/6218 21/602 21/316	09/25/2021	HY
G06F 16/182	09/25/2021	HY
G06N 20/00	09/25/2021	HY
H04L 9/0819	09/25/2021	HY
Classification with text search.	09/25/2021	HY
EAST text search (see search history printout).	09/25/2021	HY
Inventor and applicant search EAST.	09/22/2021	HY
IDS references considered.	09/22/2021	HY
google patent and NPL search.	09/24/2021	HY
Include feedback from SPE.	09/27/2021	HY
Updated complete search.	03/05/2022	HY
ip.com patent and NPL search.	03/05/2022	HY
google patent and NPL search.	03/05/2022	HY
Updated complete search.	05/06/2022	HY
ip.com patent and NPL search.	05/06/2022	HY
google patent and NPL search.	05/06/2022	HY
Interference search using PGPUB + USPAT with text search.	05/06/2022	HY

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
G06F	21/6218 21/602 21/316	05/06/2022	HY
G06F	16/182	05/06/2022	HY
G06N	20/00	05/06/2022	HY
H04L	9/0819	05/06/2022	HY

/H.Y./ Examiner, Art Unit 2493	
-----------------------------------	--

Bibliographic Data

Application No: 16/362,167

Foreign Priority claimed: ☐ Yes ☒ No

35 USC 119 (a-d) conditions met: ☐ Yes ☒ No ☐ Met After Allowance

Verified and Acknowledged:

/HAN YANG/

Examiner's Signature

Initials

Title:

FILE ACCESS CONTROL BASED ON ANALYSIS OF USER
BEHAVIOR PATTERNS

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
03/22/2019	713	2493	FORT-031800(18167)
RULE			

APPLICANTS

Fortinet, Inc., Sunnyvale, CA, UNITED STATES

INVENTORS

Matthew J. Little, Loanhead, UNITED KINGDOM

Jamie R. Graves, Edinburgh, UNITED KINGDOM

Carson Leonard, Edinburgh, UNITED KINGDOM

CONTINUING DATA

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

STATE OR COUNTRY

UNITED KINGDOM

ADDRESS

Douglas M. Hamilton
HDC Fortinet
224 S. Main Street, 114
Springville, UT 84663
UNITED STATES

FILING FEE RECEIVED

\$1,720

05/06/2022

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Fortinet, Inc.	Examiner: YANG
First Inventor: Little	Group Art Unit: 2493
App. No.: 16/362,167	Conf. No.: 6553
Filed: March 19, 2020	Docket No.: FORT-031800(18167)
For: DETECTING ACCESSS POINTS LOCATED WITHIN PROXIMITY OF A COMPUTING DEVICE FOR TROUBLESHOOTING OF A NETWORK	

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE TO OFFICE ACTION

Sir/Madam:

In response to the final Office action having a notification date of March 10, 2022 (the “Office Action”), the Applicant respectfully requests the Examiner to enter the following amendment and to consider the following remarks:

Amendments to the Claims begin at page 2 of this paper.

Remarks begin at page 7 of this paper.

About 138,908 results

Download Side-by-side

Sort by: Relevance Group by: None Deduplicate by: Family Results / page: 25

System and method for securing an enterprise computing environment

WO EP US CN • CN107409126B • 吉爾遜爾森 • 思科技術公司

Priority 2015-02-24 • Filed 2016-02-24 • Granted 2021-03-09 • Published 2021-03-09

14. The system of claim 1, wherein at least one of the modules is an audit module. 15. The system of claim 1, wherein at least one of the modules is at least one of a user behavior monitoring module and a user behavior analysis module. 16. The system of claim 1, wherein at least one of the modules ...

Cloud based security monitoring using unsupervised pattern recognition and deep ...

US • US20190068627A1 • Sajit Thampy • Oracle International Corporation

Priority 2017-08-28 • Filed 2018-05-25 • Published 2019-02-28

wherein identifying the pattern includes mapping the activity data according a set of usage levels associated with the cloud service, and wherein mapping the activity data produces normalized activity data. 3. The computer-implemented method of claim 1, wherein identifying the pattern includes ...

Mechanisms for anomaly detection and access management

US • US10721239B2 • Vipin Kootayi • Oracle International Corporation

Priority 2017-03-31 • Filed 2018-03-29 • Granted 2020-07-21 • Published 2020-07-21

receive, at the information management system from the user device, data associated with an access request, the access request requesting access to the target resource, by a user; analyze, by the information management system, the data associated with the access request against data collected ...

Method, system, medium for monitoring privileged users and detecting abnormal ...

WO EP US CN • CN110399288B • 吉爾遜爾森 • 甲骨文國際公司

Priority 2017-06-22 • Filed 2018-06-19 • Granted 2021-11-05 • Published 2021-11-05

determining one or more risk scores for the one or more users using the activity data; determining that a risk score for a user in the set of users is greater than a threshold; determining a security control for the service provider system, wherein the security control is used by the service ...

System and method for fraud monitoring, detection, and tiered user ...

WO EP US CN JP AU SA • EP1875553B1 • Thomas Emmanuel Varghese • Oracle International Corporation

Priority 2005-04-29 • Filed 2006-04-28 • Granted 2018-12-12 • Published 2018-12-12

A computer system for authenticating a current request (1320) to access a service provider server application, the current access request originating from a network-connected device (720), the system comprising: a device central repository database (1110) that stores historical information ...

Technology for the safety for finding and managing application

WO EP US CN JP • CN108762367A • 吉爾遜爾森 • 甲骨文國際公司

Priority 2016-02-26 • Filed 2017-02-24 • Published 2018-10-23

1. a method of computer implementation is included in the computer systems division of safety management system: Obtain the data of the network activity about user on the network of tissue; The application being accessed by the user on network is identified using the data about network activity; ...

Monitoring user authenticity in distributed system



US • US10110634B2 • Virginie Armar • Amadeus S.A.S.

Priority 2016-02-04 • Filed 2016-02-04 • Granted 2018-10-23 • Published 2018-10-23

wherein the adaptive risk-score engine is replicated on the at least one application server from the at least one user-model server after being adapted, and the total-specific risk score value is determined by the adaptive risk-score engine on the at least one application server based on the user ...

Automated access control management for computing systems



WO US • US11178182B2 • Abhishek Saxena • Sailpoint Technologies, Inc.

Priority 2018-04-20 • Filed 2019-04-19 • Granted 2021-11-16 • Published 2021-11-16

, wherein the at least one attribute comprises at least one of: an access privilege, or an access pattern, or an activity pattern, the activity pattern comprising one or more of: an activity type, or an activity volume over a time period, or an activity time, or a variance of one or more parameters ...

Cloud-based threat detection



US • US20210009837A1 • Venkatesubramanian Venkatesh • Oracle International Corporation

Priority 2017-09-28 • Filed 2018-09-26 • Published 2019-03-28

determining that the first event is associated with a security rule configured for the tenant, wherein the security rule includes a sequence of events and a threshold, wherein, when the network security system determines that a number of events from the sequence of events have occurred and the ...

Behavioral engine for identifying anomalous data access patterns

US • US9273065B1 • Arantharaman Ganesh • Symantec Corporation

Priority 2010-12-14 • Filed 2011-07-26 • Granted 2016-03-01 • Published 2016-03-01

A computing device receives data access records and determines a user data access behavior pattern for a user based on the data access records. The computing device receives new data access records and identifies any deviation from the user data access behavior pattern based on the new data access ...

High granularity application and data security in cloud environments



US • US11055417B2 • Gaurav Bhatia • Oracle International Corporation

Priority 2016-04-17 • Filed 2018-09-20 • Granted 2021-07-06 • Published 2021-07-06

15. The non-transitory computer-readable medium of claim 13, wherein the operations further comprise maintaining and training a model specific to the application that describes usage patterns for the application by the one or more users of the tenant, 16. The non-transitory computer-readable medium ...

Intelligent security management

WO EP US CN JP • JP6888199B2 • ワトソン、アレキサンダー・アマゾン・テクノロジーズ、インコーポレイテッド

Priority 2017-02-27 • Filed 2018-02-08 • Granted 2021-06-16 • Published 2021-06-16

The user activity is expected based on further comparing the peer activity of the peer in the peer group containing the specified user with the user activity, and further based on a second deviation of the user activity with respect to the peer activity. The computer implementation method of claim ...

Key throttling to mitigate unauthorized file access



US • US1097244B2 • Russell Humphries • Sophos Limited

Priority 2016-06-10 • Filed 2019-10-01 • Granted 2021-04-13 • Published 2021-04-13

, wherein the indication of compromise includes a pattern of access to the files indicating potentially malicious automated file access, 6. The method of claim 4, wherein the indication of compromise includes access to a number of files beyond a predetermined threshold within a predetermined time ...

Graph-based network anomaly detection across time and entities



US • US1060000B2 • Georgios Apostolopoulos • Splunk Inc.

Priority 2017-01-30 • Filed 2018-12-13 • Granted 2020-03-31 • Published 2020-03-31

1406 with comparing the subset of the threat indicator data against pre-configured patterns or pre-set rules associated with each candidate threat. For example, an insider threat may be associated with known patterns identified by security experts and therefore be associated with pre-set rules.

Network security anomaly and threat detection using rarity scoring



US • US20210030262A1 • Sudhakar Muddu • Splunk Inc

Priority 2015-08-31 • Filed 2018-06-22 • Published 2018-10-18

18 . The method of claim 1 further comprising: determining that an event of which the feature is a part as an anomaly based on a rarity score for at least some features in the event and a number of the features whose rarity scores do not satisfy a score threshold for the event, 19 . The method of

Artifact modification and associated abuse detection



US • US20200058111A1 • Bjorn Markus Jakobsson • Rightquestion LLC

Priority 2016-08-08 • Filed 2019-08-02 • Published 2020-02-13

10 . The apparatus of claim 1 wherein making a security determination based at least in part on the determined profile comprises: computing a risk score for the request; and identifying the request as an anomalous request responsive to the risk score exceeding a specified threshold, 11 . The ...

Methods, systems and computer program products for monitoring user behavior for ...



US • US2004022482 • David Lee Morsinger • Covellight Systems, Inc.

Priority 2004-02-24 • Filed 2004-02-24 • Granted 2008-05-13 • Published 2008-05-13

Methods, systems and computer program products are disclosed for monitoring user behavior for a server application in a computer network. The methods, systems, and computer program products can monitor communication data between a server application and a client. The methods, systems, and computer ...

Threat response using event vectors



WO US GB • US20190019980A1 • Joseph H. Levy • Sophos Limited

Priority 2018-04-13 • Filed 2019-04-12 • Published 2019-10-17

A security platform uses a sensor-event-analysis-response methodology to iteratively adapt to a changing security environment by continuously creating and updating entity models based on observed activities and detecting patterns of events that deviate from these entity models.

A cyber security appliance for a cloud infrastructure



EP US JP AU CA SG • EP2523658B1 • Andrew Stewart WOODFORD • Darktrace Limited

Priority 2018-02-20 • Filed 2019-02-19 • Granted 2020-09-23 • Published 2020-09-23

The appliance of claim 1, 2 or 3 where the one or more machine learning models trained on the cloud system examine at least the behaviors of the entities of devices, containers, users, and traffic patterns falling outside of the normal pattern of life and what is the likelihood of the chain of ...

Techniques for fraud monitoring and detection using application fingerprinting

US • US8732278B2 • Thomas Emmanuel Varghese • Oracle International Corporation

Priority 2006-04-28 • Filed 2008-10-29 • Granted 2014-05-27 • Published 2014-05-27



, wherein the processing component is not configured to run the software application. 19. The system of claim 17, wherein the storage component is further configured to store one or more access policies, each access policy comprising rules for calculating the risk score. 20. The system of claim 19,

Using message context to evaluate security of requested data



WO US • US1980531482 • Bjorn Markus Jakobsson • Agari Data, Inc.
Priority 2017-05-19 • Filed 2018-05-15 • Granted 2020-10-13 • Published 2020-10-13
15. The method of claim 1, wherein the security action includes determining that the security risk is below a threshold criterion and in response to the request made using the alternative resource identifier, providing a redirection response specifying the original resource identifier. 16. The ...

Systems and methods for matching and scoring sameness

WO EP US CN AU CA IL SG • AU201927193092 • Christopher Everett Bailey • Mastercard Technologies Canada ULC
Priority 2015-09-05 • Filed 2019-11-25 • Granted 2021-02-18 • Published 2021-02-18
displaying, via a backend user interface, a risk assessment report to an operator of a web site or mobile device app via which the web site or mobile device app interaction is conducted, wherein the risk assessment report is based on a result of analyzing the additional data collected from the web ...

Systems and methods for contextual and cross application threat detection and ...



US • US1003654482 • Ganesh Kirti • Oracle International Corporation
Priority 2013-12-13 • Filed 2015-06-24 • Granted 2018-08-28 • Published 2018-08-28
wherein the activity data includes a number of login failures associated with the user account. 11. The method of claim 1, wherein the activity data includes a count of login failures greater than a predetermined threshold. 12. The method of claim 1, wherein the activity data includes a count of ...

Artificial intelligence for context classifier



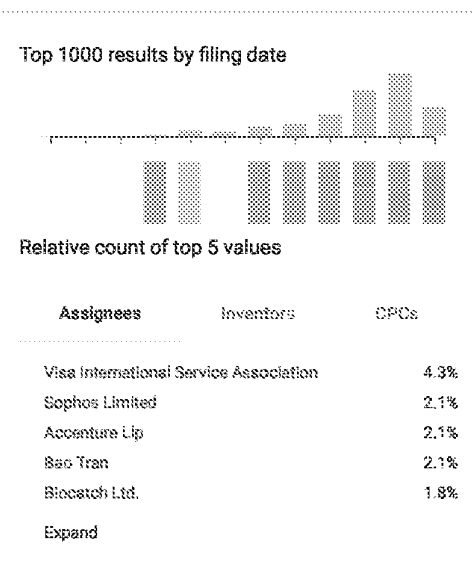
US • US20190213428A1 • Akil Adjoute • Brighterion, Inc.
Priority 2014-04-02 • Filed 2019-03-12 • Published 2019-07-11
Transaction risk is calculated datapoint-by-datapoint and includes velocity count expansions. The datapoint values that exceed a normative point by a threshold value increment the transaction risk. Datapoint values that do not exceed the threshold value cause the transaction risk to be decremented.

Identity and asset risk score intelligence and threat mitigation



WO US • US932411982 • Subrat Naranda SINGH • Alert Enterprise
Priority 2013-03-15 • Filed 2014-03-13 • Granted 2016-04-26 • Published 2016-04-26
, wherein generating the risk level for any entity involves two parts, wherein the first part uses a configuration performed by an administrator to a determine maximum risk score that can used as the 100, wherein this calculation is performed once before calculating the risk level for the selected ...

Next > >> About 138,908 results





About 4,222 results

Download Side-by-side

Sort by: Relevance Group by: None Deduplicate by: Family Results / page: 25

Protecting enterprise data through policy-based encryption of message ...



US • US9886225B2 • Waheed Qureshi • Citrix Systems, Inc.
 Priority 2011-10-11 • Filed 2012-10-10 • Granted 2014-11-11 • Published 2014-11-11
 Similar A system is disclosed that includes components and features for enabling enterprise users to securely access enterprise resources (documents, data, application servers, etc.) using their mobile devices. An enterprise can use some or all components of the system to, for example, securely but ...

Systems and methods for orchestrating runtime operational integrity



WO US JP KR IL • US20150246235A1 • Srinivas Kumar • Tencera, Inc.
 Priority 2012-05-01 • Filed 2015-02-16 • Published 2015-08-27
 Similar Instrumented networks and platforms having target subjects (devices, transactions, services, users, organizations) are disclosed. A security orchestration service generates runtime operational integrity profiles representing and identifying a level of threat or contextual trustworthiness, at near ...

Mobile application management



WO EP US CN JP • EP2808775B1 • Srikanth Nalluri • McAfee, LLC
 Priority 2012-10-19 • Filed 2013-10-18 • Granted 2022-01-26 • Published 2022-01-26
 Similar A computer-implemented method comprising: analyzing (2105) code of a particular application against a semantic model of a software development kit of a particular platform, the semantic model associating a plurality of application behaviors with respective application programming interface, API, ...

Risk adjusted, multifactor authentication



US CA • US9362275B2 • Robert C. Toole • Fmr Llc
 Priority 2012-11-07 • Filed 2014-07-21 • Granted 2015-06-30 • Published 2015-06-30
 Similar A computer-implemented method comprising: receiving, from a device used by a user, a request to access a resource hosted by a computer system; identifying, by the computer system, a level of risk associated with the user requesting access to the resource; adjusting, by the computer system an ...

System and method for restricting access to requested data based on user ...



US • US8818981B2 • Srikanth Mandava • Qa, Inc.
 Priority 2010-02-04 • Filed 2010-02-04 • Granted 2014-12-23 • Published 2014-12-23
 Similar A system and method for restricting access to requested data based on user location are disclosed. The method comprises receiving a data request and determining origin location information of the data request from a source providing information having accuracy to a predetermined standard. The ...

Stateless web content anti-automation



WO US • US9238143B2 • Marc R. Hansen • Shape Security, Inc.
 Priority 2013-03-15 • Filed 2013-10-16 • Granted 2016-05-10 • Published 2016-05-10
 Similar A computer-implemented method for coordinating content transformation includes receiving, at a computer server subsystem and from a web server system, computer code to be served in response to a request from a computing client over the Internet; modifying the computer code to obscure operation of ...

System and method for triggering analysis of an object for malware in response ...



US • US10133866B1 • Vineet Kumar • Fireeye, Inc.
 Priority 2015-12-30 • Filed 2015-12-30 • Granted 2018-11-20 • Published 2018-11-20
 Similar According to one embodiment, a system featuring one or more processors and memory that includes monitoring logic. In operation, the monitoring logic monitors for a notification message that identifies a state change event that represents an activity has caused a change in state of a data store ...

Communicating application information to a firewall



WO US GB • US2017102282 • Richard S. Teal • Sophos Limited
 Priority 2017-09-12 • Filed 2017-10-27 • Granted 2021-05-26 • Published 2021-05-26
 Similar A kernel driver on an endpoint is configured to monitor processes executing on the endpoint that use network communications, and to transmit process information to a firewall for the endpoint. The firewall can, in turn, use process this stream of information from individual endpoints or groups of ...

Method and system for protecting data flow at a mobile device



US • US9210154B2 • Phillip A. Porras • Sri International
 Priority 2012-06-29 • Filed 2015-05-20 • Granted 2015-12-08 • Published 2015-12-08
 Similar A method and system for evaluating and enforcing a data flow policy at a mobile computing device includes a data flow policy engine to evaluate data access requests made by security-wrapped software applications running on the mobile device and prevent the security-wrapped software applications ...

Multi-layer system for privacy enforcement and monitoring of suspicious data ...



WO US KR GB • [US8701191B2](#) • Ulf Mattsson • Protegrity Corporation

Priority 2005-02-18 • Filed 2013-02-26 • Granted 2014-04-15 • Published 2014-04-15

Similar: A method for controlling data access in a data-at-rest system includes executing a link intrusion prevention analysis between multiple layers of the data-at-rest system (for instance, at an application layer and a file layer), introducing a privacy policy at enforcement points that span multiple ...

Systems and methods for secure third-party data storage



US • [US8966287B2](#) • Walter Bogoras • Symantec Corporation

Priority 2012-03-26 • Filed 2013-03-13 • Granted 2015-02-24 • Published 2015-02-24

Similar: A computer-implemented method for secure third-party data storage may include 1) identifying, at a server-side computing device, a request from a client system to access an encrypted file stored under a user account, 2) identifying, in response to the request, an asymmetric key pair designated for ...

Integrating security protection tools with computer device integrity and ...



US • [US8347088B2](#) • Thekkethalackal Varugis Kurien • Microsoft Corporation

Priority 2006-06-20 • Filed 2011-12-30 • Granted 2013-01-01 • Published 2013-01-01

Similar: At computer device power on, the operating system of the computer device initiates a monitor. The monitor assigns a monitoring program to each program and object (collectively, "program") running on the computer device to monitor the activities of the program. When the monitoring program is ...

Secure server on a system with virtual machines



WO EP US CA • [US9848640B2](#) • Sergey Ignatchenko • Clonix Technologies Ag

Priority 2013-08-02 • Filed 2014-08-01 • Granted 2016-04-17 • Published 2016-04-17

Similar: A system, an apparatus and a method for providing a secure computing environment may be provided. In one aspect, an apparatus may comprise a communication port and a computer processor coupled to the communication port. The computer processor may be configured to initialize a hypervisor, establish ...

Technologies for authentication and single-sign-on using device security ...



US • [US9749310B2](#) • Hong Li • Intel Corporation

Priority 2015-03-27 • Filed 2015-03-27 • Granted 2017-08-29 • Published 2017-08-29

Similar: Technologies for remote device authentication include a client computing device, an identity provider, and an application server in communication over a network. The identity provider sends an authentication challenge to the client. A capability proxy of the client intercepts an authentication ...

Security systems and methods to reduce data leaks in enterprise networks



US • [US8893300B2](#) • Anurath V. RAMACHANDRAN • Georgia Tech Research Corporation

Priority 2010-09-20 • Filed 2011-09-20 • Granted 2014-11-18 • Published 2014-11-18

Similar: Disclosed are embodiments of a security system for reducing data leaks by checking information flows between resources of a network. When an information flow is attempted between a sending resource, which can be anywhere in the network, and a receiving resource residing at a specific host within ...

Enterprise network threat detection



US • [US20200304528A1](#) • Karl Ackerman • Sophos Limited

Priority 2018-08-31 • Filed 2020-06-09 • Published 2020-09-24

Similar: In a threat management platform, a number of endpoints log events in an event data recorder. A local agent filters this data and feeds a filtered data stream to a central threat management facility. The central threat management facility can locally or globally tune filtering by local agents based ...

System for detecting, analyzing, and controlling infiltration of computer and ...



WO EP US AU CA • [US8060017B2](#) • John Marino • Logos Technologies LLC

Priority 2012-02-21 • Filed 2013-02-20 • Granted 2015-06-16 • Published 2015-06-16

Similar: A method for detecting and manipulating a malicious actor/communication on a computer network or system. The method includes the steps of incorporating one or more synthetic vulnerabilities into the computer system at distinct locations, where each synthetic vulnerability presents an opportunity ...

Honeypot computing services that include simulated computing resources



US • [US10097581B1](#) • Nicholas Alexander Allen • Amazon Technologies, Inc.

Priority 2015-12-28 • Filed 2015-12-28 • Granted 2018-10-09 • Published 2018-10-09

Similar: The disclosure relates to provisioning honeypot computing services using a simulation state database to simulate a set of computing resources. One example includes a system that receives a mutating request associated with honeypot credentials, updates a simulation state database associated with ...

Rights Management Services Integration with Mobile Device Management



US • [US20170248272A1](#) • Jonathan Blake Brannon • Airwatch LLC

Priority 2013-05-16 • Filed 2016-11-01 • Published 2017-02-16

Similar: Rights management services (RMS) integration with mobile device management (MDM) may be provided. A functionality associated with a document may be restricted according to a document management policy. After the document has been transmitted to a receiving device, a request to un-restrict the at ...

System and method for providing different levels of key security for ...



US • [US8341406B2](#) • Hal S. Hildebrand • Guardian Data Storage, Llc
Priority 2001-12-12 • Filed 2011-04-04 • Granted 2012-12-25 • Published 2012-12-25
Similar With files secured by encryption techniques, keys are often required to gain access to the secured files. Techniques for providing and using multiple levels of keystores for securing the keys are disclosed. The keystores store keys that are needed by users in order to access secured files. The ...

Cognitive scoring of asset risk based on predictive propagation of security- ...



US • [US20180285797A1](#) • Xin Hu • International Business Machines Corporation
Priority 2014-03-28 • Filed 2018-06-06 • Published 2018-10-04
Similar A method (and system) of scoring asset risk including modeling an interdependence of risks of a plurality of entities within a network by modeling the network as a graph connecting different entities, the different entities are selected from a group of a user, a device, a credential, a high-value ...

Digital protection that travels with data



WO US CN • [US20200012780A1](#) • Dattatraya Kulkarni • McAfee, Llc
Priority 2013-09-27 • Filed 2019-09-16 • Published 2020-01-09
Similar The present disclosure relates to a system and method for performing anti-malware scanning of data files that is data-centric rather than device-centric. In the example, a plurality of computing devices are connected via a network. An originating device creates or first receives data, and scans ...

System, method and program for identifying and preventing malicious intrusions



US CN • [US8931089B2](#) • Jeffrey S. Laham • International Business Machines Corporation
Priority 2005-06-24 • Filed 2013-08-13 • Granted 2015-01-06 • Published 2015-01-06
Similar Computer system, method and program product for identifying a malicious intrusion. A first number of different destination IP addresses, a second number of different destination ports and a third number of different signatures of messages, are identified from a source IP address during a ...

Threat-aware provisioning and governance



US • [US9762882B1](#) • Christopher J. Hockings • International Business Machines Corporation
Priority 2016-05-17 • Filed 2016-12-20 • Granted 2017-09-12 • Published 2017-09-12
Similar A management component of a computing system evaluates end-users, end-user devices, and user accounts for access to provisioned-resources of the computing system. The management component utilizes device compliance attributes to form a device risk vector associated with an end-user device. The ...

Dynamic policy based on user experience



WO US GB • [US11087014B2](#) • Joseph H. Levy • Sophos Limited
Priority 2018-04-13 • Filed 2019-04-12 • Granted 2021-08-10 • Published 2021-08-10
Similar Entity models are used to evaluate potential risk of entities, either individually or in groups, in order to evaluate suspiciousness within an enterprise network. These individual or aggregated risk assessments can be used to adjust the security policy for compute instances within the enterprise ...

Next > >> About 4,222 results

Top 1000 results by filing date



Relative count of top 5 values

Assignees	Inventors	CPCs
Symantec Corporation		6.9%
International Business Machines Corporation		3.6%
Sophos Limited		2.2%

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L54	44	(Artificial Intelligence) More Like: US-20200302074-A1 Text: (US-10558797-B2 OR AU-2013359762-B2 OR AU-2013272211-B2 OR AU-2014240239-B2 OR WO-2022087510-A1 OR US-9485271-B1 OR CN-109597822-A OR AT-518805-A1 OR JP- 2020509511-A OR AU- 2011332881-B2 OR US-20180046796-A1 OR AU-2014259538-B2 OR US-20200007539- A1 OR US- 20180007069-A1 OR US-20200259836-A1 OR CN-111241566-A OR CN-110968888-A OR CN-110851847-A OR US-11165788-B2 OR US-20210084049- A1).did.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/06 07:10 PM
L55	13	L23 AND key	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/06 07:10 PM
L56	121	(holdback OR (hold\$ OR held OR keep\$ OR kept) ADJ back OR withheld OR withhold\$) near2 decrypt\$ NEAR key	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL,	OR	ON	ON	2022/05/06 07:10 PM

			PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L57	88	(holdback OR (hold\$ OR held OR keep\$ OR kept) ADJ back OR withheld OR withhold\$) near2 decrypt\$ NEAR key	(US-PGPUB; USPAT)	OR	ON	ON	2022/05/06 07:10 PM
L58	6238	(return\$ provid\$) near2 decrypt\$ NEAR key	(US-PGPUB; USPAT)	OR	ON	ON	2022/05/06 07:11 PM
L59	1	(return\$ provid\$) near2 decrypt\$ NEAR key WITH (scor\$ rank\$) WITH threshold	(US-PGPUB; USPAT)	OR	ON	ON	2022/05/06 07:11 PM
L60	1	(return\$ provid\$) near2 decrypt\$ NEAR key WITH (scor\$ rank\$) WITH threshold	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/06 07:11 PM
L61	7	(return\$ provid\$) near2 decrypt\$ NEAR key WITH (scor\$ rank\$)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/06 07:11 PM
L62	30	(return\$ provid\$) near2 decrypt\$ NEAR key WITH threshold	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA,	OR	ON	ON	2022/05/06 07:12 PM

			EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L63	1458	((("Fortinet") near3 ("Inc"))).AS,AANM.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/05/06 07:12 PM
L64	36	((("LITTLE") near3 ("Matthew")) OR ((("GRAVES") near3 ("Jamie")) OR ((("LEONARD") near3 ("Carson"))).INV.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2022/05/06 07:12 PM
L65	19	L33 AND (behavior NEAR pattern\$)	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/05/06 07:12 PM
L66	11	L33 AND (behavior NEAR user)	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/05/06 07:12 PM
L67	4	("20180069881" "20180351979" "8595497" "8887274").PN.	(US-PGPUB; USPAT)	OR	ON	ON	2022/05/06 07:12 PM
L68	9	(pattern\$ histor\$4) near2 user near2 (behavior behaviour) with (file near2 access)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/06 07:13 PM
L69	48	(pattern\$ histor\$4) near2 (behavior behaviour) with (file near2 access)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/06 07:14 PM
L70	123	user near2 (behavior behaviour) with (file near2 access)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/06 07:14 PM
L71	1	(cryptograph\$2 crypto) with wrapper with encapsulat\$3 with file with encrypt\$3	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/06 07:14 PM
L72	2	(cryptograph\$2 crypto) with wrapper with encapsulat\$3 with file	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/06 07:14 PM
L73	30	(cryptograph\$2 crypto) with wrapper with file	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/06 07:14 PM
L74	55	(pattern\$ histor\$4) with user with (behavior behaviour) with (file	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	ON	2022/05/06 07:14 PM

		near2 access)	IBM_TDB)				
L75	235367	(G06F21/6218 or G06F16/182 or G06N20/00 or H04L9/0819 or G06F21/602 or G06F21/316).cpc.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/06 07:14 PM
L76	12	L44 AND L45	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/06 07:14 PM
L77	118	(pattern\$ histor\$4) with user with (behavior behaviour) same (file near2 access)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/06 07:14 PM
L78	42	L47 AND L45	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/06 07:14 PM
L79	5	user same (access near2 request) same (file near2 access) same (risk near2 score)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/06 07:14 PM
L80	264	determin\$6 with user near4 locat\$3 with based with ip near address with request	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/06 07:15 PM
L81	22	determin\$6 with user near4 locat\$3 with based with ip near address with (access near2 request)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/06 07:15 PM
L82	60	determin\$6 with locat\$3 with based with ip near address with (access near2 request)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/06 07:15 PM
L83	0	correlat\$3 with locat\$3 with based with ip near address with (access near2 request)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/05/06 07:15 PM

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N1	34	((("LITTLE") near3 ("Matthew")) OR (("GRAVES") near3 ("Jamie")) OR (("LEONARD") near3 ("Carson"))).INV.	(US-PGPUB; USPAT)	OR	ON	ON	2022/05/06 07:17 PM
N2	96224	(G06F21/6218 OR G06F16/182 OR G06N20/00 OR	(US-PGPUB; USPAT)	OR	ON	ON	2022/05/06 07:17 PM

		H04L9/0819 OR G06F21/602 OR G06F21/316).cpc.					
N3	11	((holdback OR (hold\$ OR held OR keep\$ OR kept) ADJ back OR withheld OR withhold\$) near2 decrypt\$ NEAR key).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2022/05/06 07:36 PM
N4	1	N3 AND N1	(US-PGPUB; USPAT)	OR	ON	ON	2022/05/06 07:36 PM
N5	1	N3 AND N2	(US-PGPUB; USPAT)	OR	ON	ON	2022/05/06 07:37 PM
N6	1030	((return\$ provid\$) near2 decrypt\$ NEAR key).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2022/05/06 07:38 PM
N7	1	N6 AND N1	(US-PGPUB; USPAT)	OR	ON	ON	2022/05/06 07:38 PM
N8	189	N6 AND N2	(US-PGPUB; USPAT)	OR	ON	ON	2022/05/06 07:38 PM
N9	12	((return\$ provid\$) near2 decrypt\$ NEAR key).clm. AND (limit\$ near2 access).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2022/05/06 07:39 PM
N10	1	N9 AND N2	(US-PGPUB; USPAT)	OR	ON	ON	2022/05/06 07:41 PM
N11	9	(user near2 (behavior behaviour) WITH (file near2 access)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2022/05/06 07:42 PM
N12	4	N11 AND N2	(US-PGPUB; USPAT)	OR	ON	ON	2022/05/06 07:43 PM
N13	3	((pattern\$ histor\$4) WITH user WITH (behavior behaviour) SAME (file near2 access)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2022/05/06 07:53 PM

1 - 50

☐ Rule based trust evaluation using fuzzy logic in cloud computing

Presently, the cloud computing is a regarded research both in scholars and enterprise, because of its unique features such as low expenditure, easy maintenance, flexibility, fast deployment and reliable service. However to administer cloud computing, improvement in academic, legal and institutional...

IEEE Xplore : IEEE Conferences : 2017-09-01 : 4 : 2017 8th International Conference on Reliability, Inform. Technologies and Optimization (Trends and Future Directions) (ICRITO) (Page(s): 510-514)

☐ CloudSky: A Controllable Data Self-Destruction System for Untrusted Cloud Storage Networks

In cloud services, users may frequently be required to reveal their personal private information which could be stored in the cloud to used by different parts for different purposes. However, in a cloud-wide storage network, the servers are easily under strong attacks and also commonly experience...

IEEE Xplore : IEEE Conferences : 2015-06-01 : 4 : 2015 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (Page(s): 352-361)

☐ Agile Composition of Compliant Data Analytics Platforms

Sensitive data such as health records and financial transactions are increasingly being stored and processed in the cloud. Correspondingly, laws and regulations have been established to protect such data. For a cloud-based analytics service provider, it is of paramount importance to protect these sensitive...

IEEE Xplore : IEEE Conferences : 2017-04-01 : 4 : 2017 IEEE International Conference on Cloud Engineering (IC2E) (Page(s): 51-56)

☐ Insider attack and real-time data mining of user behavior

Early detection of employees' improper access to sensitive or valuable data is critical to limiting negative financial impacts to an organization, including regulatory penalties for misuse of customer data that results from these insider attacks. Implementing a system for detecting insider attacks...

IEEE Xplore : IBM Periodicals : 2007-05-01 : 4 : IBM Journal of Research and Development

☐ Turning Data into Insight with IBM Machine Learning for z/OS

The exponential growth in data over the last decade coupled with a drastic drop in cost of storage has enabled organizations to amass a large amount of data. This vast data becomes the new natural resource that these organizations must tap in to innovate and stay ahead of the competition, and they...

5024842100 : IBM Redbooks : 2018-09-11 : 4

☐ The Study and Design on Secure-Intranet Storage System

For the security issue in intranet storage systems, we design a data security storage system, which integrates information isolation, accessing control, virus detection, metadata safeguard of crucial data and fast-speed retrieval. This system can provide a solid foundation for data protection and...

IEEE Xplore : IEEE Conferences : 2010-10-01 : 4 : 2010 Third International Symposium on Information Processing (Page(s): 537-541)

☐ A Survey on Detection Techniques for Cryptographic Ransomware

Crypto-ransomware is a type of malware that encrypts user files, deletes the original data, and asks for a ransom to recover the hijacked documents. It is a cyber threat that targets both companies and residential users, and has spread in recent years because of its lucrative results. Several...

IEEE Xplore : IEEE Periodicals : 2019-01-01 : 4 : IEEE Access

☐ Security Architecture and Protocol for Trust Verifications Regarding the Integrity of Files Stored in Cloud Services †

Cloud computing is considered an interesting paradigm due to its scalability, availability and virtually unlimited storage capacity. However, it is challenging to organize a cloud storage service (CSS) that is safe from the client point-of-view and to implement this CSS in public clouds since it is...

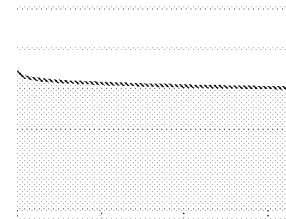
PM25876326 : PubMed Central : 2015-03-02 : 4 : Sensors (Basel, Switzerland), 15(3), 753

☐ Reduce Risk and Improve Security on IBM Mainframes. Volume 1 Architecture and Platform Security

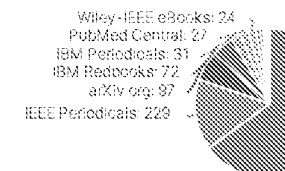
This IBM® Redbooks® publication documents the strength and value of the IBM security strategy with IBM System z® hardware and software. In an age of increasing security consciousness, IBM System z provides the capabilities to address the needs of today's business security challenges. This...

5024780301 : IBM Redbooks : 2014-12-08 : 4

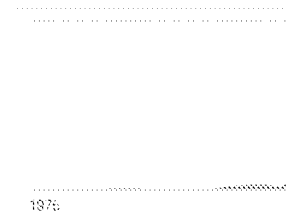
Relevance



Collections



Publication Date



Charts based on top 1500 results

Threats come from a variety of sources. Insider threats, as well as malicious hackers, are not only difficult to detect and prevent, but many times the authors of these threats are using resources without anybody being aware that those threats are there. Threats would not be harmful if there were no...

5024758101 : IBM Redbooks : 2011-02-17 : 4

Countering Network-Centric Insider Threats through Self-Protective Autonomic Rule Generation

Insider threats are a growing problem in today's organizations. Detecting such attacks is especially challenging because most system owners and system administrators use networks to remotely manage the systems they are responsible for. In previous work, we introduced the Autonomic Violation...

IEEE Xplore : IEEE Conferences : 2012-06-01 : 4 : 2012 IEEE Sixth International Conference on Software Security and Reliability (Page(s): 273-282)

Securing Data in Storage: A Review of Current Research

Protecting data from malicious computer users continues to grow in importance. Whether preventing unauthorized access to personal photographs, ensuring compliance with federal regulations, or ensuring the integrity of corporate secrets, all applications require increased security to protect data...

cs3408034 : arXiv.org : 2004-09-17 : 4

Gargoyle: A Network-based Insider Attack Resilient Framework for Organizations

Anytime, Anywhere' data access model has become a widespread IT policy in organizations making insider attacks even more complicated to model, predict and deter. Here, we propose Gargoyle, a network-based insider attack resilient framework against the most complex insider threats within a pervasive...

IEEE Xplore : IEEE Conferences : 2016-10-01 : 4 : 2016 IEEE 43rd Conference on Local Computer Networks (LCN) (Page(s): 553-561)

Passive security intelligence to analyze the security risks of mobile/BYOD activities

As enterprises embrace mobile technologies and enable their employees to bring their own devices, traditional security mechanisms are challenged by the co-location of personal and business activities on employee-owned mobile devices on the enterprise network. This presents a new risk to enterprises...

IEEE Xplore : IBM Periodicals : 2016-07-01 : 4 : IBM Journal of Research and Development

Design and implementation of an improved cloud storage system

The detailed designs, technologies and implementations of cloud storage are presented, including the multi-tenant concurrency, separated framework between buffer and business etc. Master/Workers partition algorithm is adopted to improve the reading and writing efficiency for big data in the cloud...

IEEE Xplore : IEEE Conferences : 2016-06-01 : 4 : 2016 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD) (Page(s): 1616-1623)

Design Issues of Trustworthy Cloud Platform Based on IP Monitoring and File Risk

With the rising popularity of Web applications and cloud computing technology, a secure cloud computing environment is one of the main concerns. Currently, enterprise cloud platforms often rely on their maintenance and operation, and medium and small companies cannot effectively save manpower...

IEEE Xplore : IEEE Conferences : 2016-09-01 : 4 : 2016 IEEE Fifth International Conference on Big Data and Cloud Computing (Page(s): 110-117)

A survey on miscellaneous attacks in Hadoop framework

The world is progressing towards innovative advancement step by step bringing about an exponential rise in data. This enormous volume of data has presented the possibility of Big data, which has caught the consideration of business and IT researchers as a gift and a source of various opportunities...

IEEE Xplore : IEEE Conferences : 2016-01-01 : 4 : 2016 2nd International Conference on Inventive Systems and Control (ICISCI) (Page(s): 1043-1046)

Security intelligence for cloud management infrastructures

In this paper, we address the problem of protecting cloud infrastructures and customer workloads via smart auditing and logging, satisfying regulatory and compliance requirements. We observe that traditional approaches of logging and auditing events in cloud-scale infrastructures will not be...

IEEE Xplore : IBM Periodicals : 2016-07-01 : 4 : IBM Journal of Research and Development

Multitenant Access Control for Cloud-Aware Distributed Filesystems

In a virtualization environment that serves multiple tenants (independent organizations), storage consolidation at the filesystem level is desirable because it enables data sharing, administration efficiency, and performance optimizations. The scalable deployment of filesystems in such environments...

IEEE Xplore : IEEE Periodicals : 2017-06-15 : 4 : IEEE Transactions on Dependable and Secure Computing

computing

Context Integrity Measurement Architecture (CI-MIA) was inspired by risk assessments used by credit card companies. These assessments flag excursions from "normal" or "typical" behavior. If an excursion exceeds some threshold level, the card companies require additional proof of identity before...

IEEE Xplore : IEEE Conferences : 2016-10-01 : 4 : 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCCON) (Page(s): 1-10)

☐ Computer Software Security

This chapter contains sections titled: Specific Operating Systems (OSS) Applications Example Detailed Security Requirements for Specific Operating Systems and Applications Chapter Summary Further Reading and Resources Questions Exercises

IEEE Xplore : Wiley-IEEE eBooks : 2011-01-01 : 4 : Wiley-IEEE Press 2011 (Edition: 1, Pages: 512)

☐ Deployment Guide for InfoSphere Guardium

IBM® InfoSphere® Guardium® provides the simplest, most robust solution for data security and data privacy by assuring the integrity of trusted information in your data center. InfoSphere Guardium helps you reduce support costs by automating the entire compliance auditing process across heterogeneous...

5024812500 : IBM Redbooks : 2014-03-19 : 4

☐ IEEE Standard for information Technology: Hardcopy Device and System Security

This standard defines security requirements (all aspects of security including but not limited to authentication, authorization, privacy, integrity, device management, physical security and information security) for manufacturers, users, and others on the selection, installation, configuration and...

IEEE Xplore : IEEE Standards : 2006-06-30 : 4 : IEEE Std 2600-2006 (Page(s): 1-177)

☐ FileWall: A Firewall for Network File Systems

Access control in network file systems relies on primitive mechanisms like access control lists and permission bits, which are not enough when operating in a hostile network environment. Network middleboxes, e.g., firewalls, completely ignore file system semantics when defining policies. Therefore,...

IEEE Xplore : IEEE Conferences : 2007-09-01 : 4 : Third IEEE International Symposium on Dependable, Autonomic and Secure Computing (DA-SC 2007) (Page(s): 153-162)

☐ Detecting and Preventing Cyber Insider Threats: A Survey

Information communications technology systems are facing an increasing number of cyber security threats, the majority of which are originated by insiders. As insiders reside behind the enterprise-level security defence mechanisms and often have privileged access to the network, detecting and...

IEEE Xplore : IEEE Periodicals : 2018-01-31 : 4 : IEEE Communications Surveys & Tutorials

☐ The study and design on secure-cloud storage system

For the security issue in cloud storage systems, we design a cloud security storage system (for short CSSS). Firstly, The CSSS integrates information isolation, accessing control, virus detection, metadata safeguard of crucial data and fast-speed retrieval; Secondly, with the help of connect control...

IEEE Xplore : IEEE Conferences : 2011-08-01 : 4 : 2011 International Conference on Electrical and Control Engineering (Page(s): 5120-5126)

☐ Software agents and computer network security

Preventing unauthorised access to corporate information systems is essential for many organisations. To address this problem we built a security enhancement software system using software agents, in which a core software agent resides on a server and user end software agents reside at each user...

IEEE Xplore : IEEE Conferences : 2000-01-01 : 4 : Proceedings Seventh IEEE International Conference and Workshop on the Engineering of Computer-Based Systems (ECBS 2000) (Page(s): 211-217)

☐ EndBox: Scalable Middlebox Functions Using Client-Side Trusted Execution

Many organisations enhance the performance, security, and functionality of their managed networks by deploying middleboxes centrally as part of their core network. While this simplifies maintenance, it also increases cost because middlebox hardware must scale with the number of clients. A promising...

IEEE Xplore : IEEE Conferences : 2018-06-01 : 4 : 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (Page(s): 1-10)

[More V](#)

Main Concept Document

=====

US20200302074

Title: File access control based on analysis of user behavior patterns

(No Concept Modifiers)

=====

Filters (1)

=====

Publication Date: To 2019-03-22

Options

=====

De-dup: None

Cut-off: None

Sort: Relevance

Content: Non-Patent Literature (23)

=====

IEEE Xplore Publications: IEEE Periodicals

IEEE Xplore Publications: IEEE Conferences

IEEE Xplore Publications: IEEE Standards

IEEE Xplore Publications: IEEE Early Access

IEEE Xplore Publications: SMPTE Periodicals

IEEE Xplore Publications: SMPTE Conferences

IEEE Xplore Publications: SMPTE Standards

IEEE Xplore Publications: MIT Press eBooks

IEEE Xplore Publications: Wiley-IEEE eBooks

IEEE Xplore Publications: IBM Periodicals

IEEE Xplore Publications: URSI Periodicals

IEEE Xplore Publications: VDE Conferences

IEEE Xplore Publications: Periodicals from China

IP.com Prior Art Database: The IP.com Journal

IP.com Prior Art Database: Internet Society RFC

IP.com Prior Art Database: IBM TDB Archive

IP.com Prior Art Database: Legacy Journals

IP.com Prior Art Database: Software Patent Institute

OnePetro.org: Periodicals at OnePetro.org

OnePetro.org: Conferences at OnePetro.org

Other Literature: IBM Redbooks

IQSearchText-202205062255.txt

Other Literature: PubMed Central

Other Literature: arXiv.org

1 - 50

☐ Mechanisms for anomaly detection and access management

The present disclosure relates generally to threat detection, and more particularly, to techniques for managing user access to resources in an enterprise environment. Some aspects are directed to the concept of managing access to a target resource based on a threat perception of a user that is...

ORACLE INTL CORP

US20200267162 : US Applications : 2020-08-20 : 4

☐ System and method to identify abnormalities to continuously measure transaction risk

Aspects of the disclosure provide techniques for using behavior based information for providing and restricting access to a secure website, or computer network and its assets to a user. Components of the system may include the following. Client remote computing device, network and browser unique...

SECUREAUTH CORP

US11065809 : US Patents : 2021-05-11 : 4

☐ System, method, and apparatus for data cognition incorporating autonomous security protection

A method, apparatus and computer readable medium for data cognition incorporating autonomous security protection including, a data file stored on a storage medium, and having stored instructions for an embedded autonomous executable program which is executed each time there is an attempt to access, ...

AZOS AI LLC

US20120151553 : US Applications : 2012-05-14 : 4

☐ Cybersecurity detection and mitigation system using machine learning and advanced data correlation

Computer system security is often implemented using rules-based systems (e.g., allow traffic to this network port, deny it for those network ports; user A is allowed access to these files, but not those files). In enterprises, multiple such systems may be deployed, but fail to be able to ...

PAYPAL INC

US20220124111 : US Applications : 2022-04-21 : 4

☐ Data-defined architecture for network data management

Techniques are disclosed relating to data management. A computer system may evaluate network traffic to extract and group data objects based on their content satisfying similarity criteria, and to identify baseline behavior with respect to those data objects. The computer system may generate...

HELIOS DATA INC

US201903260767 : US Applications : 2019-08-22 : 4

☐ Permissions policy manager to configure permissions on computing devices

For increased device security, a security policy manager is used to configure permissions for applications installed on mobile computing devices. In one approach, an evaluation server receives data associated with a context for a computing device. Based on the received data, a policy that is...

LOOKOUT INC

EP3920084A1 : EPO Applications : 2021-12-08 : 4

☐ Distributed Security Analysis for Shared Content

Methods and systems for providing a cost effective and robust security solution for shared files stored by file sharing software solutions are described herein. The methods and systems for generating a ledger associated with shared files, which may include scanning data received from applications...

CITRIX SYS INC

US20220089209 : US Applications : 2022-03-24 : 4

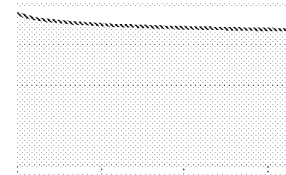
☐ Enterprise information asset protection through insider attack specification, monitoring and mitigation

The present invention provides a policy specification framework to enable an enterprise to specify a given insider attack using a holistic view of a given data access, as well as the means to specify and implement one or more intrusion mitigation methods in response to the detection of such an

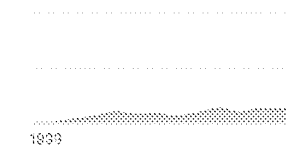
IBM TECH CORP

US8880893 : US Patents : 2014-11-04 : 4

Relevance



Publication Date



First Our Assignees by Relevance

ORACLE INTL CORP	(21)
SECUREAUTH CORP	(2)
AZOS AI LLC	(1)
PAYPAL INC	(4)
HELIOS DATA INC	(3)
LOOKOUT INC	(11)
CITRIX SYS INC	(71)
IBM TECH CORP	(1)

Charts based on top 1500 results

A system for contextual and risk-based multi-factor authentication having a multi-dimensional time series data server configured to monitor and record a network's traffic data and to serve the traffic data to other modules and a directed computation graph module configured to receive network traffic...

COMPLX INC

US20180158852 : US Applications : 2018-06-07 : 4

☐ Network security

A security platform that iteratively adapts to a changing security environment by creating and updating entity models based on observed activities and detecting patterns of events that deviate from these entity models.

SOPHOS LTD

WO2019200917A1 : WIPO Applications : 2019-10-17 : 4

☐ Data management platform

Techniques are disclosed relating to the management of data. A data provider computer system may store particular data of a user. The data provider computer system may commence sharing of a portion of the particular data with a data consumer computer system. The data provider computer system may...

HELIOS DATA INC

US20200238143 : US Applications : 2020-07-23 : 4

☐ Data segmentation

Techniques are disclosed relating to data management. A computer system may evaluate network traffic to extract and group data objects based on their content satisfying similarity criteria, and to identify baseline behavior with respect to those data objects. The computer system may generate...

HELIOS DATA INC

US20200238124 : US Applications : 2020-07-23 : 4

☐ Access control system for enterprise cloud storage

Systems and corresponding computer-implemented methods for context-based rule evaluation in an electronic data storage system are described. A request to perform an operation with respect to a resource is received from a client device, with the request including various attributes associated with...

BOX INC

US20170063867 : US Applications : 2017-03-30 : 4

☐ Key throttling to mitigate unauthorized file access

A file system extension for an endpoint controls access to files by selectively decrypting files under certain conditions. Where a pattern of access to the files suggests malicious and/or automated file access activity, the file system extension may limit the rate of file access by regulating the

SOPHOS LTD

US20200038747 : US Applications : 2020-01-30 : 4

☐ Key throttling to mitigate unauthorized file access

A file system extension for an endpoint controls access to files by selectively decrypting files under certain conditions. Where a pattern of access to the files suggests malicious and/or automated file access activity, the file system extension may limit the rate of file access by regulating the

SOPHOS LTD

US10488522 : US Patents : 2019-11-05 : 4

☐ Emotion-based database security

A computer-implemented method is provided. The method may include determining a behavioral pattern of a user based on historical data access events and historical data access conditions corresponding to the historical data access events, wherein the data access events are associated with a computer

INTEL BUSINESS MACHINES CORP

US11062004 : US Patents : 2021-07-13 : 4

☐ Cloud based security monitoring using unsupervised pattern recognition and deep learning

Provided are systems and methods for a cloud security system that learns patterns of user behavior and uses the patterns to detect anomalous behavior in a network. Techniques discussed herein include obtaining activity data from a service provider system. The activity data describes actions...

ORACLE INTL CORP

US11185850 : US Patents : 2021-11-02 : 4

Data is collected from a set of devices according to a data collection policy. The data is associated with at least one of: device configuration, device state, or device behavior. A norm is established using the collected data. A different data collection policy is established based on the norm...

LOOKOUT INC

US20200308702 : US Applications : 2020-11-19 : 4

☐ Data security in a disconnected environment

Systems and methods are provided for the detection and prevention of intrusions in data at rest systems such as file systems and web servers. The systems and methods regulate access to sensitive data with minimal dependency on a communications network. Data access is quantitatively limited to...

PROTECTOR USA INC

US20140337623 : US Applications : 2014-11-13 : 4

☐ Ransomware file modification prevention technique

A computerized system and method to detect ransomware cyber-attacks is described. The approach entails analyzing the features associated with a file access event by a process operating on a computing device, to ascertain whether the process is associated with a ransomware cyber-attack.

MANDIANT INC

US10893068 : US Patents : 2021-01-12 : 4

☐ Technology for the safety for finding and managing application

Disclose the technology for application to be found and managed in the computing environment of tissue. The use that safety management system discovery is applied in a computing environment is to manage the access to application, the security threat and risk in computing environment to minimize...

ORACLE INTL CORP

CN108702367A : China Applications : 2018-10-23 : 4

☐ Systems and methods of secure self-service access to content

In one embodiment, a method is performed by a computer system. The method includes receiving a request from a user to access particular content. The method further includes determining a trust measure of the user, wherein the trust measure is based, at least in part, on an analysis of logged...

QUEST SOFTWARE INC

US9842230 : US Patents : 2017-12-12 : 4

☐ User Authentication by Endpoint Device Using Local Policy Engine and Endpoint Data

Techniques are provided for authenticating a user using an endpoint device of the user with a local policy and endpoint data. One method comprises obtaining, at an endpoint device of a given user, behavioral anomalies from a remote engine that generates the behavioral anomalies based on behavior of...

DELL EMC

US20200242222 : US Applications : 2020-07-30 : 4

☐ Gracefully handling endpoint feedback when starting to monitor

A method, system and computer-readable medium for adaptively assessing risk associated with an endpoint, comprising: determining a risk level corresponding to an entity associated with an endpoint; selecting a frequency and a duration of an endpoint monitoring interval; collecting user behavior to...

FORCEPOINT FEDERAL HLDG LLC

US10842987 : US Patents : 2020-06-05 : 4

☐ Labeling computing objects for improved threat detection

Processes executing on an endpoint are labelled as either "in", wherein the processes conform to a compliance policy administered for the endpoint from a remote threat management facility, or the processes are "out", wherein the processes do not conform to the compliance policy, thereby providing a...

SOPHOS LTD

GB2565734A : Great Britain Applications : 2019-02-20 : 4

☐ Systems and methods for event-based authentication

[More V](#)[Result 1](#)

Main Concept Document

=====

US20200302074

Title: File access control based on analysis of user behavior patterns

(No Concept Modifiers)

=====

Filters (1)

=====

Earliest Priority Date: To 2019-03-22

Options

=====

De-dup: Extended Family Numbers

Cut-off: None

Sort: Relevance

Content: Patent Publications (166)

=====

US Patents

US Designs

US Applications

EPO Patents

EPO Applications

China Patents

China Applications

Japan Patents

Japan Applications

Korea Patents

Korea Applications

WIPO Applications

Argentina Patents

Argentina Applications

Brazil Patents

Brazil Applications

Canada Patents

Canada Applications

Chile Patents

Chile Applications

Colombia Applications

Costa Rica Applications
Cuba Patents
Cuba Applications
Dominican Republic Applications
Ecuador Patents
Ecuador Applications
El Salvador Applications
Guatemala Applications
Honduras Applications
Mexico Patents
Mexico Applications
Nicaragua Patents
Panama Applications
Peru Applications
Trinidad & Tobago Patents
Uruguay Applications
Austria Patents
Austria Applications
Belarus Patents
Belgium Patents
Belgium Applications
Bosnia & Herzegovina Patents
Bosnia & Herzegovina Applications
Bulgaria Patents
Bulgaria Applications
Croatia Patents
Croatia Applications
Czech Republic Patents
Czech Republic Applications
Czechoslovakia Patents
Czechoslovakia Applications
Denmark Patents
Denmark Applications
Estonia Patents
Estonia Applications
EUIPO Patents
Finland Patents
Finland Applications
France Patents
France Applications
Germany Patents
Germany Applications
Great Britain Patents
Great Britain Applications
Greece Patents
Greece Applications

Hungary Patents
Hungary Applications
Iceland Patents
Iceland Applications
Ireland Patents
Ireland Applications
Italy Patents
Italy Applications
Latvia Patents
Latvia Applications
Lithuania Patents
Lithuania Applications
Luxembourg Patents
Malta Patents
Monaco Patents
Montenegro Patents
Montenegro Applications
Netherlands Patents
Netherlands Applications
Norway Patents
Norway Applications
Poland Patents
Poland Applications
Portugal Patents
Portugal Applications
Republic of Moldova Patents
Republic of Moldova Applications
Romania Patents
Romania Applications
San Marino Patents
San Marino Applications
Serbia Patents
Serbia Applications
Slovakia Patents
Slovakia Applications
Slovenia Patents
Spain Patents
Spain Applications
Sweden Patents
Sweden Applications
Switzerland Patents
Switzerland Applications
Ukraine Patents
Yugoslavia/Serbia and Montenegro Patents
Yugoslavia/Serbia and Montenegro Applications
Armenia Patents

Australia Patents
Australia Applications
Cyprus Patents
Gulf Cooperation Council Patents
Hong Kong Patents
India Patents
India Applications
Indonesia Patents
Indonesia Applications
Israel Applications
Jordan Patents
Jordan Applications
Kyrgyzstan Patents
Macao Applications
Malaysia Patents
Mongolia Patents
New Zealand Patents
Philippines Patents
Philippines Applications
Saudi Arabia Patents
Saudi Arabia Applications
Singapore Patents
Singapore Applications
Taiwan Patents
Taiwan Applications
Tajikistan Patents
Tajikistan Applications
Thailand Applications
Uzbekistan Patents
Vietnam Patents
Algeria Patents
ARIPO Patents
ARIPO Applications
Egypt Patents
Kenya Patents
Malawi Patents
Morocco Patents
Morocco Applications
OAPI Patents
South Africa Patents
Tunisia Applications
Zambia Patents
Zimbabwe Patents
EAPO Patents
EAPO Applications
Georgia Patents

Georgia Applications
Kazakhstan Patents
Kazakhstan Applications
Russia Patents
Russia Applications
Turkey Patents
Turkey Applications

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA VA 22313-1451

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE PAID
POSTEDIGITAL
NNNNN

Douglas M. Hamilton
HDC Fortinet
224 S. Main Street, 114
Springville, UT 84663



**Courtesy Reminder for
Application Serial No: 16/362,167**

Attorney Docket No: FORT-031800(18167)
Customer Number: 176502
Date of Electronic Notification: 05/18/2022

This is a courtesy reminder that new correspondence is available for this application. If you have not done so already, please review the correspondence. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:

miquelchamilton@hamiltonshome.com
dhamilton@hdciplaw.com

To view your correspondence online or update your email addresses, please visit us anytime at **<https://ppair-my.uspto.gov/pair/PrivatePair>**.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov or call 1-866-217-9197.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

176502 7590 05/18/2022
Douglas M. Hamilton
HDC Fortinet
224 S. Main Street, 114
Springville, UT 84663

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/362,167	03/22/2019	Matthew J. Little	FORT-031800(18167)	6553

TITLE OF INVENTION: FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1200	\$0.00	\$0.00	\$1200	08/18/2022

EXAMINER	ART UNIT	CLASS-SUBCLASS
YANG, HAN	2493	713-165000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

- (1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

HDC Intellectual Property
1 Law, LLP
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

Fortinet, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Sunnyvale, CA

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☒ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

☒ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. Change in Entity Status (from status indicated above)

- ☐ Applicant certifying micro entity status. See 37 CFR 1.29
- ☐ Applicant asserting small entity status. See 37 CFR 1.27
- ☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Douglas M. Hamilton/
Douglas M. Hamilton
Typed or printed name _____

Date 8/15/2022
47,629
Registration No. _____

Electronic Patent Application Fee Transmittal				
Application Number:		16362167		
Filing Date:		22-Mar-2019		
Title of Invention:		FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS		
First Named Inventor/Applicant Name:		Matthew J. Little		
Filer:		Douglas M. Hamilton		
Attorney Docket Number:		FORT-031800(18167)		
Filed as Large Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	1501	1	1200	1200

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				1200

Electronic Acknowledgement Receipt	
EFS ID:	46414583
Application Number:	16362167
International Application Number:	
Confirmation Number:	6553
Title of Invention:	FILE ACCESS CONTROL BASED ON ANALYSIS OF USER BEHAVIOR PATTERNS
First Named Inventor/Applicant Name:	Matthew J. Little
Customer Number:	176502
Filer:	Douglas M. Hamilton
Filer Authorized By:	
Attorney Docket Number:	FORT-031800(18167)
Receipt Date:	15-AUG-2022
Filing Date:	22-MAR-2019
Time Stamp:	17:44:24
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$ 1200
RAM confirmation Number	E20228EH46251154
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	FORT-031800ExecutedIssueFee.pdf	87166	no	1
			f8caae9b97935c1ae8a663a47e36d8d5de7b9e69		
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	38089	no	2
			7fe311b1aea5924125d00b7eaf9a615532b775c8		
Warnings:					
Information:					
Total Files Size (in bytes):			125255		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/362,167	09/20/2022	11449623	FORT-031800(18167)	6553

176502 7590 08/31/2022
Douglas M. Hamilton
HDC Fortinet
224 S. Main Street, 114
Springville, UT 84663

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 683 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Patents Stakeholder Experience (OPSE), Stakeholder Support Division (SSD) at (571)-272-4200.

INVENTOR(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional inventors):

Matthew J. Little, Loanhead, UNITED KINGDOM;
Jamie R. Graves, Edinburgh, UNITED KINGDOM;
Carson Leonard, Edinburgh, UNITED KINGDOM;

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Fortinet, Inc., Sunnyvale, CA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

IR103 (Rev. 10/09)