

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

TAASERA LICENSING LLC,

Plaintiff,

v.

TREND MICRO INCORPORATED,

Defendant.

§
§
§
§
§
§
§
§
§
§
§

Case No. 2:21-cv-00441-JRG-RSP

JURY TRIAL DEMANDED

**PLAINTIFF’S DISCLOSURE OF ASSERTED CLAIMS
AND INFRINGEMENT CONTENTIONS**

Plaintiff Taasera Licensing LLC (“Taasera”) hereby makes the following infringement disclosures under the Patent Local Rules with respect to United States Patent Nos. 6,842,796 (the “’796 Patent”), 7,673,137 (the “’137 Patent”), 8,327,441 (the “’441 Patent”), 8,850,517 (the “’517 Patent”), 8,955,038 (the “’038 Patent”), 8,990,948 (the “’948 Patent”), 9,092,616 (the “’616 Patent”), 9,608,997 (the “’997 Patent”), and 9,923,918 (the “’918 Patent”) (collectively, “Taasera Patents”). Taasera’s investigation is ongoing, and discovery has not yet commenced. Accordingly, these disclosures are based on information available to Taasera at this time. Taasera reserves the right to supplement this disclosure after further discovery from Defendants and non-parties, particularly documents and other discovery regarding Defendants’ Accused Products. Taasera also reserves the right to assert additional claims of the Taasera Patents, accuse different products, or find alternative literal and/or equivalent infringing elements in Defendants’ products.

**I. DISCLOSURE OF ASSERTED CLAIMS AND INFRINGEMENT CONTENTIONS
PURSUANT TO PATENT LOCAL RULE 3-1**

A. ASSERTED CLAIMS

Defendant Trend Micro Incorporated (“Trend Micro” or “Defendant”) has infringed and continues to infringe at least the following claims of the Taasera Patents in connection with the Accused Products set forth below:

- Claims 1, 2, 4, 7, 8, 10, 12, 13, 15, 18, 19, 21, and 23–25 of the ’796 Patent;
- Claims 1-4, 6-14, 16-18, 20, 22, 23-25, and 29 of the ’137 Patent;
- Claims 1-7 and 9 of the ’441 Patent;
- Claims 1-10, 12-22, and 24 of the ’517 Patent;
- Claims 1–33 of the ’038 Patent;
- Claims 1–5 of the ’948 Patent;
- Claims 1, 6–9, 10, 12–15, 17, 20, and 22 of the ’518 Patent;
- Claims 1–7 of the ’616 Patent;
- Claims 1–30 of the ’997 Patent; and
- Claims 1–24 of the ’918 Patent.

Taasera reserves the right to seek leave of court to add, delete, substitute, or otherwise amend this list of asserted claims should further discovery, the Court’s claim construction, or other circumstances so merit.

B. ACCUSED INSTRUMENTALITIES

Taasera is currently aware that the following integrated Data Loss Prevention (iDLP) products infringe the ’796 Patent:

Trend Micro Endpoint Security (OfficeScan)

SaaS Application Security (Cloud App Security)

Mail Server (ScanMail for Microsoft Exchange),
Mail Server (ScanMail for Lotus Domino),
Secure Email Gateway (InterScan Messaging Security)
Secure Web Gateway (InterScan Web Security)
Instant Messaging Security (IM Security for Microsoft™ Lync)
Collaboration Portal Protection (PortalProtect for Microsoft SharePoint)
Suites (Smart Protection for Endpoints & Complete)
Apex One
Apex One XDR
Vision One

Taasera is currently aware that the following products infringe the '137 Patent, the '441 Patent:

Apex One
Apex One XDR
Vision One

Taasera is currently aware that the following products infringe the '517 Patent:

Apex Central with Deep Discovery Inventor
Apex One with Deep Discovery Inventor
Apex One XDR with Deep Discovery Inventor
Vision One with Deep Discovery Inventor
Apex One XDR
Vision One

Taasera is currently aware that the following endpoint security products infringe the '038 Patent, the '997 Patent, and the '918 Patent:

Trend Micro Vulnerability Protection (with Apex Central)

Apex One with Vulnerability Protection

Network One with Vulnerability Protection

Apex One XDR with Vulnerability Protection

Vision One with Vulnerability Protection

Taasera is currently aware that the following endpoint security products infringe the '948 Patent and the '616 Patent:

Apex One XDR

Vision One

Taasera reserves the right to amend this list of accused instrumentalities, as well as other information contained in this document and the exhibits hereto, to incorporate new information learned during the course of discovery including, but not limited to, the inclusion of newly released products or any other equivalent devices ascertained through discovery.

C. CLAIM CHARTS

Claim charts identifying a location of every element of every asserted claim of the Taasera Patents within Accused Products are attached hereto as Appendices A-I. Taasera believes that: the DLP products cited in the claim charts are representative of all accused Trend Micro DLP products; the mobile products cited in the claim charts are representative of all accused Trend Micro mobile products; and the endpoint security products cited in the claim charts are representative of all accused Trend Micro endpoint security products. Taasera reserves the right to amend these claim charts as well as other information contained in this document and the Appendices hereto, to incorporate new information learned during the course of discovery including, but not limited to, information that is not publicly available or readily discernible without discovery. Taasera further reserves the right to

amend these claim charts, as well as other information contained in this document and the Appendices attached hereto, pursuant to Patent Local Rules 3-1(g) and 3-6.

D. LITERAL INFRINGEMENT AND DOCTRINE OF EQUIVALENTS

Taasera asserts that, under the proper construction of the asserted claims and their claim terms, the limitations of the asserted claims of the Taasera Patents are literally present in the accused DLP, mobile, and endpoint security systems as set forth in the claim charts attached hereto as Appendices A-H. Taasera contends that any and all elements found not to be literally infringed are infringed under the doctrine of equivalents because the differences between the claimed inventions and the accused instrumentalities, if any, are insubstantial.

Taasera also contends that Trend Micro directly infringes the asserted claims by making, using, offering for sale, selling, and importing into the United States the accused products as well as indirectly infringes by contributing to and/or inducing others (*e.g.*, Trend Micro's customers or its customers' customers) to directly infringe those claims by making, using, offering for sale, or selling the Trend Micro Accused Products.

Pursuant to Patent Local Rule 3-6(a)(1), Taasera reserves the right to amend its Infringement Contentions as to literal infringement or infringement under the doctrine of equivalents in light of the Court's claim construction.

E. PRIORITY DATES

Under P.R. 3-1(e):

- Each of the asserted claims of the '796 Patent is entitled to a priority date of July 3, 2001;
- Each of the asserted claims of the '137 Patent is entitled to a priority date of January 4, 2002;

- Each of the asserted claims of the '441 Patent is entitled to a priority date of February 17, 2011;
- Each of the asserted claims of the '517 Patent is entitled to a priority date of January 15, 2013;
- Each of the asserted claims of the '038 Patent, the '997 Patent, and the '918 Patent is entitled to a priority date of December 21, 2005;
- Each of the asserted claims of the '518 Patent is entitled to a priority date of July 1, 2011;
- Each of the asserted claims of the '948 Patent and the '616 Patent is entitled to a priority date of May 1, 2012;

Taasera's disclosure under P.R. 3-1(e) is made without prejudice to Taasera's right to establish an earlier date of invention based upon actions related to conception and reduction to practice of the claimed inventions.

F. TAASERA'S OWN PRODUCTS

Pursuant to P.R. 3-1(f), Taasera states that, although it is currently developing products, it does not currently have products that practice any claim of any patent. Taasera reserves the right to amend this list to add, delete, substitute, or otherwise amend this list of covered products should the Court's claim construction or other circumstances so merit.

II. PRODUCTION OF DOCUMENTS PURSUANT TO PATENT LOCAL RULE 3-2

Taasera is producing or making available for inspection documents that are in Taasera's possession, custody, or control as set forth in Patent Local Rule 3-2. A Taasera 3-2 Production Index identifying these documents is attached hereto.

This preliminary identification of documents is for convenience and is not an admission that each document falls within any exemplary categories in the Patent Local Rules, or that any document qualifies as prior art. Taasera is continuing with its investigation, particularly with respect to ESI. Thus, Taasera reserves its right to add to, delete from, or otherwise modify its disclosures in this section as its investigation proceeds.

Production of these documents is governed by Patent Local Rule 2-2, and, with the exception of documents produced pursuant to P.R. 3.2(c) and public documents listed in the infringement charts, are considered “Confidential – Outside Attorneys Eyes Only” and disclosure of the confidential document or information shall be limited to each parties’ outside attorney(s) of record and the employees of such outside attorney(s).

Dated: July 26, 2022

Respectfully submitted,

/s/ Alfred R. Fabricant

Alfred R. Fabricant

NY Bar No. 2219392

Email: ffabricant@fabricantllp.com

Peter Lambrianakos

NY Bar No. 2894392

Email: plambrianakos@fabricantllp.com

Vincent J. Rubino, III

NY Bar No. 4557435

Email: vrubino@fabricantllp.com

Joseph M. Mercadante

NY Bar No. 4784930

Email: jmercadante@fabricantllp.com

FABRICANT LLP

411 Theodore Fremd Avenue,
Suite 206 South

Rye, New York 10580

Telephone: (212) 257-5797

Facsimile: (212) 257-5796

Justin Kurt Truelove

Texas Bar No. 24013653

Email: kurt@truelovelawfirm.com

TRUELOVE LAW FIRM, PLLC

100 West Houston Street
Marshall, Texas 75670
Telephone: (903) 938-8321
Facsimile: (903) 215-851

**ATTORNEYS FOR PLAINTIFF
TAASERA LICENSING LLC**

CERTIFICATE OF SERVICE

I hereby certify that on July 26, 2022 a true and correct copy of the above and foregoing document has been served on all counsel of record by electronic mail.

/s/ Alfred R. Fabricant
Alfred R. Fabricant

TAASERA LICENSING 3-2 PRODUCTION INDEX

3-2(a)

None.

3-2(b)

Plaintiff is not in possession, custody, or control of any documents responsive to P.R. 3-2(b). Plaintiff states that such documents are in the possession of International Business Machines, Daedalus, and/or Taasera, Inc.

3-2(c)

Bates Start	Bates End
TAASERA-0000001	TAASERA-0002886

Public Documents Listed in Infringement Charts

Bates Start	Bates End
TAASERA-TM-0000001	TAASERA-TM-0001570

In these Infringement Contentions, Taasera Licensing contends that at least the following claims of U.S. Patent No. 8,327,441 (“’441 patent”) identified below are infringed by Trend Micro Apex One. Taasera Licensing does not concede that any claims of the ’441 patent that are not listed below are not infringed by the identified products. Moreover, the citations to certain documents and other information below are intended to be exemplary only and in no way foreclose Taasera Licensing from citing or relying on additional documents, information, source code, and/or testimony at a later time. These contentions are preliminary in nature, and an analysis of Trend Micro's products, internal documentation, source code, and/or testimony from relevant witnesses may more fully and accurately describe the infringing features of its accused products. Accordingly, Taasera Licensing reserves the right to supplement, correct, modify, and/or amend these contentions once such additional information is made available to Taasera Licensing. Furthermore, Taasera Licensing reserves the right to supplement, correct, modify, and/or amend these contentions: as discovery in this case progresses; in view of the Court’s claim construction order(s); in view of any positions taken by Defendants, including but not limited to positions on claim construction, invalidity, and/or non-infringement; and in connection with the preparation and exchange of expert reports.

Representativeness: Trend Micro Apex One, depicted in this chart, is believed to be representative of other Trend Micro endpoint and network security solutions with attestation monitoring, including at least Trend Micro XDR and Trend Micro Vision One, for the purposes of infringement of the ’441 Patent. Based on publicly available information, Taasera Licensing believes that the Trend Micro Apex One charted herein and other Trend Micro EDR and XDR solutions attestation monitoring share substantially the same structure and functionality with respect to the components which are relevant to infringement given that, among other things, all have endpoint agents that report to an attestation server. Should discovery yield documents or information demonstrating that Defendant sells other infringing endpoint and network security solutions with attestation monitoring which are not represented by the Trend Micro Apex One, Taasera Licensing reserves the right to amend its infringement contentions to include a chart mapping the claims of the ’441 Patent to the structure and function of the newly discovered endpoint/security product.

Claim	Support
[1P] A method of providing an attestation service for an application at runtime executing on a computing platform using	Trend Micro Apex One provides an attestation service (<i>e.g.</i> , runtime machine learning) for an application at runtime executing on a computing platform (<i>e.g.</i> , a computing device with an Apex One security agent) using an attestation server (<i>e.g.</i> , Apex One Server).

Claim	Support
an attestation server, comprising:	TREND MICRO APEX ONE™ Endpoint security redefined A blend of advanced threat protection techniques, combined with detection and response, delivered through a single-agent architecture to eliminate security gaps across any user activity and any endpoint. • Automated: Stop attackers sooner with the most effective protection against zero-day threats. It uses a blend of next-gen anti-malware techniques and the industry's most timely virtual patching to quickly stop attackers. • Insightful: Get exceptional visibility and control across your environment. Integrated extended detection and response (XDR) capabilities for cross-layer detection, investigation, and threat hunting. • Connected: Quickly respond to attacks with real-time and local threat intelligence updates and a broad API set for integration with third-party security tools. Flexible deployment options fit perfectly with your environment. YOU CAN HAVE IT ALL • Malware and ransomware protection: Defends endpoints against malware, ransomware, malicious scripts, and more. With advanced protection capabilities that adapt to protect against unknown and stealthy new threats. • Extensive detection and response capabilities: XDR extends detection and response capabilities with cross-layer detection, threat hunting and investigation across email, endpoints, servers, cloud workloads, and network together in one console • The industry's most timely virtual patching: Vulnerability protection applies virtual patches for protection before a patch is available or deployable. • Ransomware rollback: Detects ransomware with runtime machine learning and expert rules to block encryption processes in milliseconds. Rollback restores any files encrypted before the detection. • Connected threat defense: Trend Micro Apex One integrates with other security products via our global cloud threat intelligence, delivering sandbox rapid response updates to endpoints. • Flexible deployment: Trend Micro Apex One® as a Service saves time, money, and is always up to date with the latest protection. On-premises and hybrid deployments are also fully supported. PROTECTION AND EFFICIENCY: THE RIGHT TECHNIQUE AT THE RIGHT TIME Protection Points • Physical endpoints • Microsoft® Windows® PCs and servers • Mac computers • Point of sale (POS) and ATM endpoints Threat Detection Capabilities • High-fidelity machine learning (pre-execution and runtime) • Behavioral analysis (against scripts, injection, ransomware, memory, and browser attacks) • In-memory analysis for identification of fileless malware • Variant protection • Census check • Web reputation • Exploit prevention (host firewall, exploit protection) • Command and control (C&C) blocking • Data loss prevention (DLP) • Device and application control • Ransomware rollback • Sandbox and breach detection integration • Extended detection and response (XDR) See how we stack up https://www.trendmicro.com/en_us/business/technologies/competitive-benchmarks.html See e.g., https://www.trendmicro.com/content/dam/trendmicro/global/en/business/products/user-protection/sps/endpoint-security-apex-one/ds-apex-one.pdf.

The Apex One Server

The Apex One server is the central repository for all agent configurations, security risk logs, and updates.

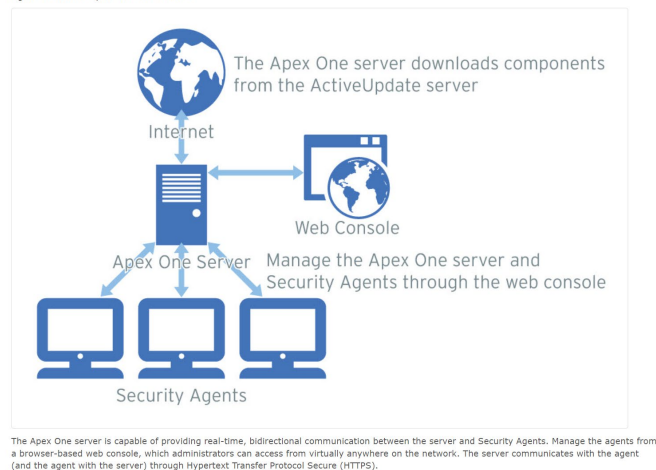
The server performs two important functions:

- Installs, monitors, and manages Security Agents
- Downloads most of the components needed by agents. The Apex One server downloads components from the Trend Micro ActiveUpdate server and then distributes them to agents.

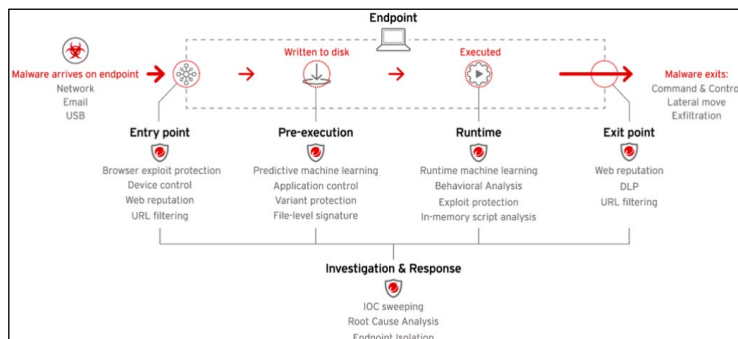
Note:

Some components are downloaded by smart protection sources. See [Smart Protection Sources](#) for details.

Figure 1. How the Apex One server works

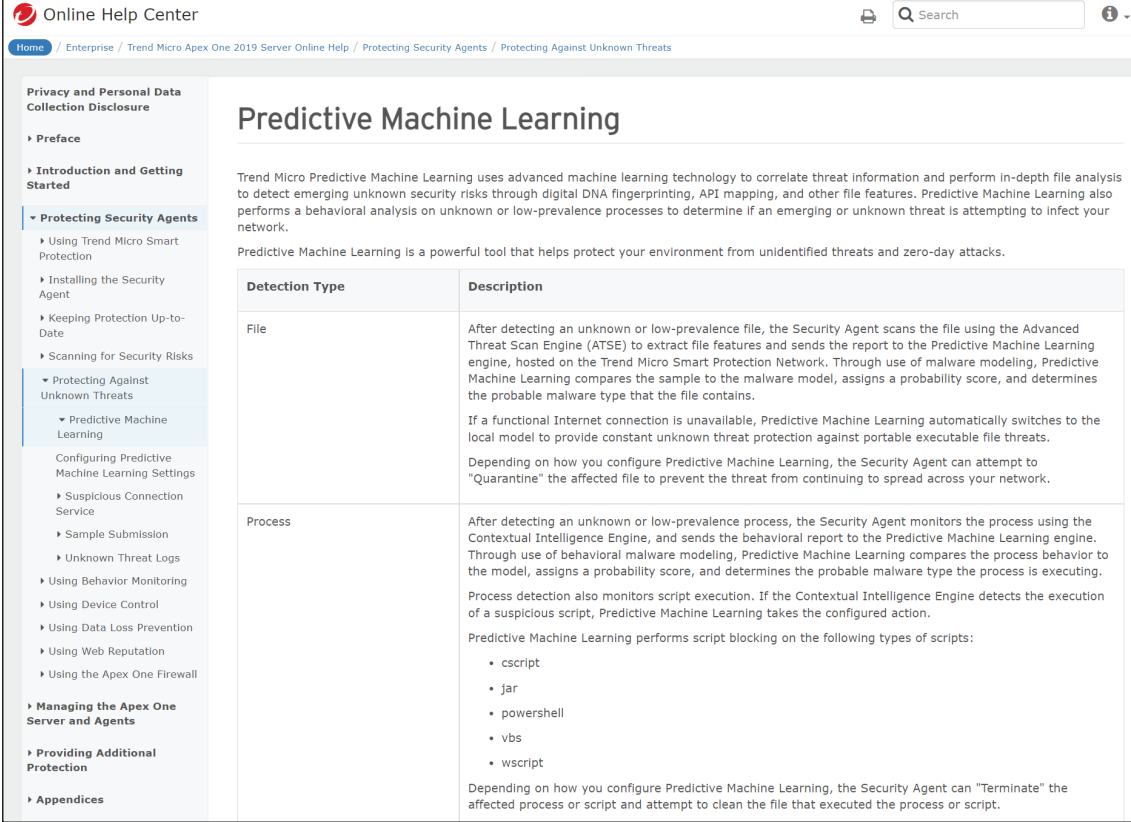


See e.g., https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-one-2019-server-online-help/introduction-and-get/introducing-product_/osce-the-product_sho.aspx.



See e.g., https://www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html.

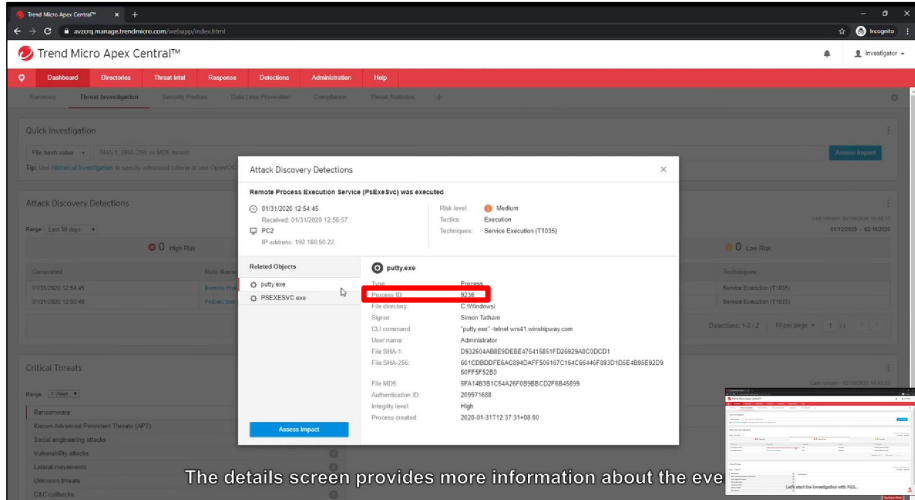
Claim	Support																
	Apex One Security Agent Feature <table><tr><th>Feature</th><th>Windows Endpoint</th><th>Windows Server</th><th>Mac Endpoint</th></tr><tr><td>Anti Malware</td><td>✓</td><td>✓</td><td>✓</td></tr><tr><td>Behavior Monitoring</td><td>✓</td><td>✓</td><td>✗</td></tr><tr><td>Predictive Machine Learning</td><td>✓</td><td>✓</td><td>✓</td></tr></table> See <i>e.g.</i>, https://success.trendmicro.com/dcx/s/solution/000151532-Apex-One-Security-Agent-features-on-different-platforms?language=en_US. Plaintiff contends that this element is literally present in the accused Trend Micro Apex One Products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses. Plaintiff reserves the right to supplement after inspection of relevant source code.	Feature	Windows Endpoint	Windows Server	Mac Endpoint	Anti Malware	✓	✓	✓	Behavior Monitoring	✓	✓	✗	Predictive Machine Learning	✓	✓	✓
Feature	Windows Endpoint	Windows Server	Mac Endpoint														
Anti Malware	✓	✓	✓														
Behavior Monitoring	✓	✓	✗														
Predictive Machine Learning	✓	✓	✓														
[1A] receiving, by the attestation server remote from the computing platform: a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of	The attestation server (<i>e.g.</i>, Apex One Server) receives a runtime execution context (<i>e.g.</i>, behavior report from the Contextual Intelligence Engine) indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application (<i>e.g.</i>, script execution). The attestation server (<i>e.g.</i>, Apex One Server) also receives a security context providing security information about the application (<i>e.g.</i>, malware analysis using predictive machine learning), wherein the security information comprises an execution analysis (<i>e.g.</i>, behavior analysis) of the one or more executable file binaries and the loaded components.																

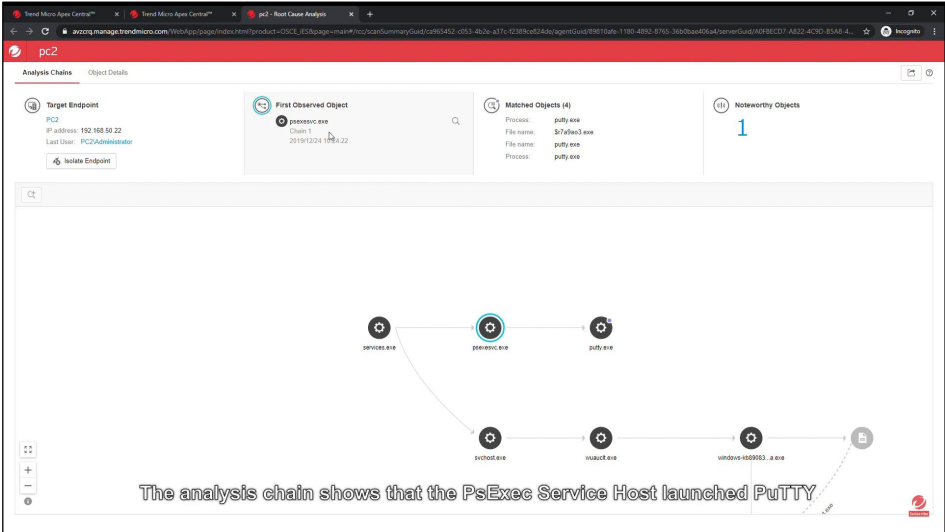
Claim	Support
the application and loaded components of the application; and a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components;	 See e.g., https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-one-2019-server-online-help/protecting-trend_cli/protecting-against-u_001/predictive-machine-l.aspx. Plaintiff contends that this element is literally present in the accused Trend Micro Apex One Products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses. Plaintiff reserves the right to supplement after inspection of relevant source code.
[1B] generating, by the attestation	Trend Micro Apex One generates a report (e.g., a log) indicating security risks (e.g., security threats) associated with the application (e.g., infected file/object or process) based on the received runtime execution context (e.g., threat identifiers) and the received security context (e.g., threat probability/type).

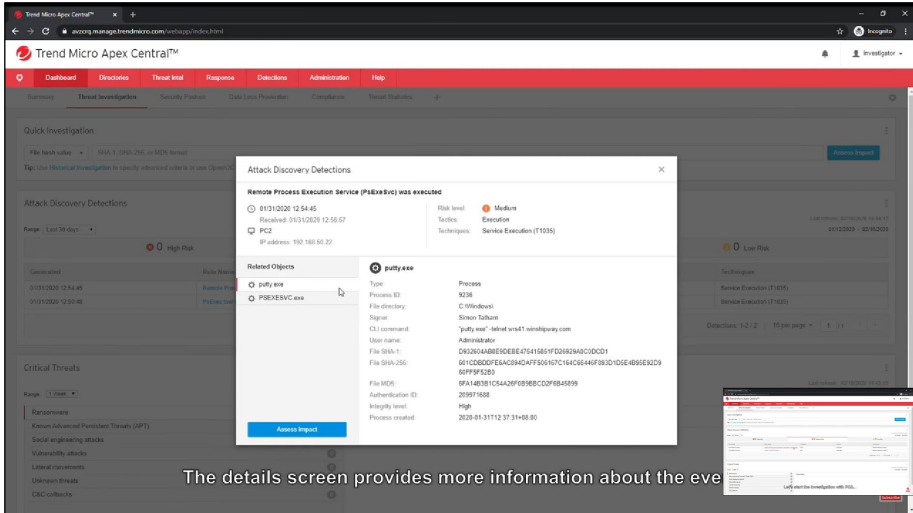
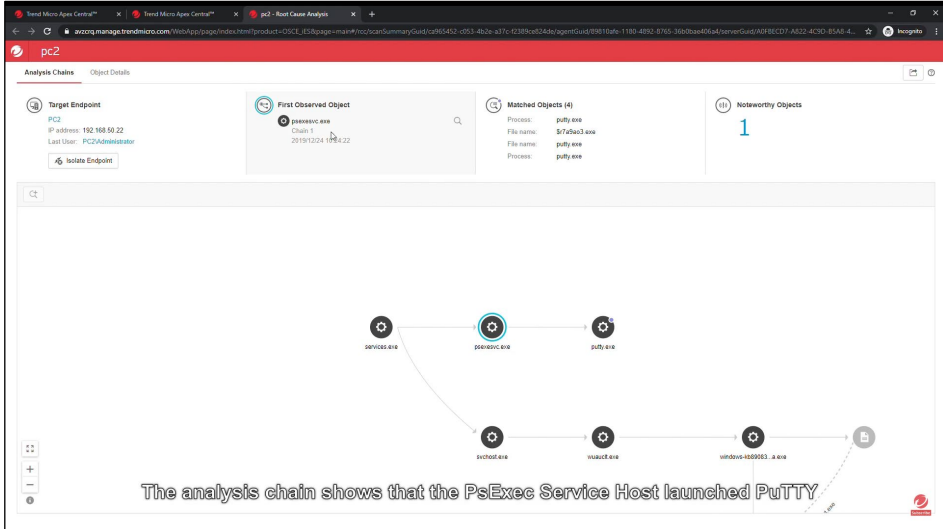
Claim	Support																						
server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result; and	Viewing Predictive Machine Learning Logs - Go to one of the following: Logs > Agents > Security Risks Agents > Agent Management - In the agent tree, click the root domain icon (🌐) to include all agents or select specific domains or agents. - Go to the Predictive Machine Learning Log Criteria screen: - From the Security Risk Logs screen, click View Logs > Predictive Machine Learning Logs. - From the Agent Management screen, click Logs > Predictive Machine Learning Logs. - Specify the log criteria and then click Display Logs. - View logs. Logs contain the following information: <table> <tr> <th>Item</th><th>Description</th></tr> <tr> <td>Date/Time</td><td>The time the detection occurred</td></tr> <tr> <td>Endpoint</td><td>The endpoint on which the detection occurred</td></tr> <tr> <td>IP Address</td><td>The IP address and port number of the source endpoint</td></tr> <tr> <td>Security Threat</td><td>The name of the security threat determined by the Predictive Machine Learning engine</td></tr> <tr> <td>Result</td><td>The result of the action taken</td></tr> <tr> <td>Infected File/Object</td><td>The name of the file object or the program that executed the process</td></tr> <tr> <td>Type</td><td>The type of object that triggered the detection ("File" or "Process")</td></tr> <tr> <td>File Path</td><td>The path of the file object or the path of the program that executed the process</td></tr> <tr> <td>Infection Channel</td><td>The channel the threat originated from</td></tr> <tr> <td>Details</td><td>A link that displays the detailed analysis for the specific detection For more information, see Predictive Machine Learning Log Details.</td></tr> </table> https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-one-2019-server-online-help/protecting-trend_cli/protecting-against-u_001/unknown-threat-logs/viewing-predictive-m.aspx	Item	Description	Date/Time	The time the detection occurred	Endpoint	The endpoint on which the detection occurred	IP Address	The IP address and port number of the source endpoint	Security Threat	The name of the security threat determined by the Predictive Machine Learning engine	Result	The result of the action taken	Infected File/Object	The name of the file object or the program that executed the process	Type	The type of object that triggered the detection ("File" or "Process")	File Path	The path of the file object or the path of the program that executed the process	Infection Channel	The channel the threat originated from	Details	A link that displays the detailed analysis for the specific detection For more information, see Predictive Machine Learning Log Details .
Item	Description																						
Date/Time	The time the detection occurred																						
Endpoint	The endpoint on which the detection occurred																						
IP Address	The IP address and port number of the source endpoint																						
Security Threat	The name of the security threat determined by the Predictive Machine Learning engine																						
Result	The result of the action taken																						
Infected File/Object	The name of the file object or the program that executed the process																						
Type	The type of object that triggered the detection ("File" or "Process")																						
File Path	The path of the file object or the path of the program that executed the process																						
Infection Channel	The channel the threat originated from																						
Details	A link that displays the detailed analysis for the specific detection For more information, see Predictive Machine Learning Log Details .																						

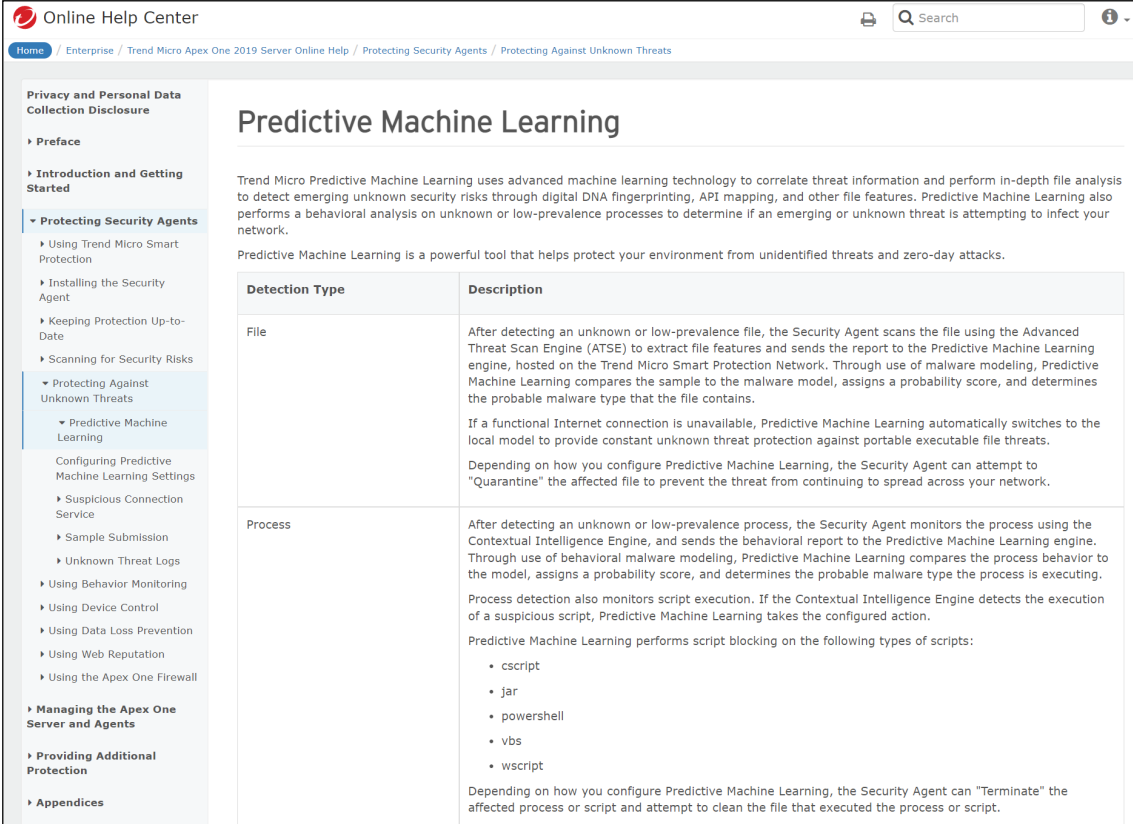
Claim	Support																		
	Predictive Machine Learning Log Details You can view a comprehensive report for each Predictive Machine Learning log detection by clicking the View link under the Details column. The Log Details screen consists of two sections: - Top banner: Specific details related to this particular log detection - Bottom tab controls: Details related to the Predictive Machine Learning threat, including threat probability scores, file information, and other endpoints across your network that have the same detection The following table discusses the information provided in the top banner. Table 1. Log Details - Top Banner <table> <tr> <th>Section</th><th>Description</th></tr> <tr> <td>Detection time / Action</td><td>Indicates when this specific log detection occurred and the action that the agent took on the threat</td></tr> <tr> <td>File name</td><td>Indicates the name of the file that triggered the detection on the specified endpoint Tip: Click Add to Exception List to quickly add the file hash value of the affected file to the global Predictive Machine Learning Exception list. View the entire exception list on the Predictive Machine Learning Settings screen. For more information, see Configuring Predictive Machine Learning Settings. Important: The detected file name for this detection may not be the same as the file name detected on other agents. Predictive Machine Learning associates detections according to file hash values, not specific file names. View the Affected Endpoints tab to verify the file name on other endpoints. </td></tr> <tr> <td>Endpoint information</td><td>Displays the logged on user at the time of the detection, the endpoint name, and the IP address of the endpoint</td></tr> <tr> <td>Channel information</td><td>Displays the channel from which the threat originated and the folder location on the endpoint the threat transferred to</td></tr> </table> The following table discusses the information provided on the bottom tabs. Table 2. Log Details - Tab Information <table> <tr> <th>Tab</th><th>Description</th></tr> <tr> <td>Threat Indicators</td><td>Provides the results of the Predictive Machine Learning analysis Threat Probability: Indicates how closely the file/process matched the malware model Probable Threat Type: Indicates the most likely type of threat contained in the file after Predictive Machine Learning compared the analysis to other known threats Threat Identifiers: Provides a list a API functions used by the file/process that may be indicative of the detected threat type Important: API function identification is only one factor in the determination of the threat type. Predictive Machine Learning uses many other file features and analysis methods to calculate the threat probability and probable threat type. Similar Known Threats: Provides a list of known threat types that exhibit similar file/process features to the detection </td></tr> <tr> <td>File Details</td><td>Provides general details related the file properties and certificate information for this specific detection log</td></tr> <tr> <td>Affected Endpoints</td><td>Displays a list of other agents on your network with the same Predictive Machine Learning detection and provides specific details about the detections on the other agents</td></tr> </table> See e.g., https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-one-2019-server-online-help/protecting-trend_cli/protecting-against-u_001/unknown-threat-logs/viewing-predictive-m/predictive-machine-l_001.aspx. Plaintiff contends that this element is literally present in the accused Trend Micro Apex One Products. Plaintiff reserves the right to rely upon the Doctrine of Equivalentents as discovery progresses.	Section	Description	Detection time / Action	Indicates when this specific log detection occurred and the action that the agent took on the threat	File name	Indicates the name of the file that triggered the detection on the specified endpoint Tip: Click Add to Exception List to quickly add the file hash value of the affected file to the global Predictive Machine Learning Exception list. View the entire exception list on the Predictive Machine Learning Settings screen. For more information, see Configuring Predictive Machine Learning Settings. Important: The detected file name for this detection may not be the same as the file name detected on other agents. Predictive Machine Learning associates detections according to file hash values, not specific file names. View the Affected Endpoints tab to verify the file name on other endpoints.	Endpoint information	Displays the logged on user at the time of the detection, the endpoint name, and the IP address of the endpoint	Channel information	Displays the channel from which the threat originated and the folder location on the endpoint the threat transferred to	Tab	Description	Threat Indicators	Provides the results of the Predictive Machine Learning analysis Threat Probability: Indicates how closely the file/process matched the malware model Probable Threat Type: Indicates the most likely type of threat contained in the file after Predictive Machine Learning compared the analysis to other known threats Threat Identifiers: Provides a list a API functions used by the file/process that may be indicative of the detected threat type Important: API function identification is only one factor in the determination of the threat type. Predictive Machine Learning uses many other file features and analysis methods to calculate the threat probability and probable threat type. Similar Known Threats: Provides a list of known threat types that exhibit similar file/process features to the detection	File Details	Provides general details related the file properties and certificate information for this specific detection log	Affected Endpoints	Displays a list of other agents on your network with the same Predictive Machine Learning detection and provides specific details about the detections on the other agents
Section	Description																		
Detection time / Action	Indicates when this specific log detection occurred and the action that the agent took on the threat																		
File name	Indicates the name of the file that triggered the detection on the specified endpoint Tip: Click Add to Exception List to quickly add the file hash value of the affected file to the global Predictive Machine Learning Exception list. View the entire exception list on the Predictive Machine Learning Settings screen. For more information, see Configuring Predictive Machine Learning Settings. Important: The detected file name for this detection may not be the same as the file name detected on other agents. Predictive Machine Learning associates detections according to file hash values, not specific file names. View the Affected Endpoints tab to verify the file name on other endpoints.																		
Endpoint information	Displays the logged on user at the time of the detection, the endpoint name, and the IP address of the endpoint																		
Channel information	Displays the channel from which the threat originated and the folder location on the endpoint the threat transferred to																		
Tab	Description																		
Threat Indicators	Provides the results of the Predictive Machine Learning analysis Threat Probability: Indicates how closely the file/process matched the malware model Probable Threat Type: Indicates the most likely type of threat contained in the file after Predictive Machine Learning compared the analysis to other known threats Threat Identifiers: Provides a list a API functions used by the file/process that may be indicative of the detected threat type Important: API function identification is only one factor in the determination of the threat type. Predictive Machine Learning uses many other file features and analysis methods to calculate the threat probability and probable threat type. Similar Known Threats: Provides a list of known threat types that exhibit similar file/process features to the detection																		
File Details	Provides general details related the file properties and certificate information for this specific detection log																		
Affected Endpoints	Displays a list of other agents on your network with the same Predictive Machine Learning detection and provides specific details about the detections on the other agents																		

Claim	Support																																											
	Plaintiff reserves the right to supplement after inspection of relevant source code.																																											
[1C] sending, by the attestation server, the attestation result associated with the application.	Trend Micro Apex One sends (<i>e.g.</i>, sends to Windows NT event logs, emails) the attestation result (<i>e.g.</i>, predictive machine learning log) associated with the application and can also send a notification of the result to administrators by email and/or SNMP. Administrator Notification Settings Configure administrator notification settings to allow Apex One to successfully send notifications through email, and SNMP Trap. Apex One can also send notifications through Windows NT event log but no settings are configured for this notification channel. Apex One can send notifications to you and other Apex One administrators when the following are detected: Table 1. Detections that Trigger Administrator Notifications <table><tr><th rowspan="2">Detections</th><th colspan="3">Notification Channels</th></tr><tr><th>Email</th><th>SNMP Trap</th><th>Windows NT Event Logs</th></tr><tr><td>Viruses and malware</td><td>Yes</td><td>Yes</td><td>Yes</td></tr><tr><td>Spyware and grayware</td><td>Yes</td><td>Yes</td><td>Yes</td></tr><tr><td>Digital asset transmissions</td><td>Yes</td><td>Yes</td><td>Yes</td></tr><tr><td>C&C callbacks</td><td>Yes</td><td>Yes</td><td>Yes</td></tr><tr><td>Virus and malware outbreaks</td><td>Yes</td><td>Yes</td><td>Yes</td></tr><tr><td>Spyware and grayware outbreaks</td><td>Yes</td><td>Yes</td><td>Yes</td></tr><tr><td>Firewall violation outbreaks</td><td>Yes</td><td>No</td><td>No</td></tr><tr><td>Shared folder session outbreaks</td><td>Yes</td><td>No</td><td>No</td></tr><tr><td>C&C callback outbreaks</td><td>Yes</td><td>Yes</td><td>Yes</td></tr></table> https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-one-2019-server-online-help/managing-the-product/managing-the-product_001/administrator-notifi.aspx Plaintiff contends that this element is literally present in the accused Trend Micro Apex One Products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses. Plaintiff reserves the right to supplement after inspection of relevant source code.	Detections	Notification Channels			Email	SNMP Trap	Windows NT Event Logs	Viruses and malware	Yes	Yes	Yes	Spyware and grayware	Yes	Yes	Yes	Digital asset transmissions	Yes	Yes	Yes	C&C callbacks	Yes	Yes	Yes	Virus and malware outbreaks	Yes	Yes	Yes	Spyware and grayware outbreaks	Yes	Yes	Yes	Firewall violation outbreaks	Yes	No	No	Shared folder session outbreaks	Yes	No	No	C&C callback outbreaks	Yes	Yes	Yes
Detections	Notification Channels																																											
	Email	SNMP Trap	Windows NT Event Logs																																									
Viruses and malware	Yes	Yes	Yes																																									
Spyware and grayware	Yes	Yes	Yes																																									
Digital asset transmissions	Yes	Yes	Yes																																									
C&C callbacks	Yes	Yes	Yes																																									
Virus and malware outbreaks	Yes	Yes	Yes																																									
Spyware and grayware outbreaks	Yes	Yes	Yes																																									
Firewall violation outbreaks	Yes	No	No																																									
Shared folder session outbreaks	Yes	No	No																																									
C&C callback outbreaks	Yes	Yes	Yes																																									
[2P] The method of claim 1,	Integrated with Apex One, Apex Central controls Apex One.																																											

Claim	Support								
further comprising:	Integration with Trend Micro Products and Services Apex One integrates with the Trend Micro products and services listed in the following table. For seamless integration, ensure that the products run the required or recommended versions. TABLE 1-6. Products and Services that Integrate with Apex One <table><tr><th>PRODUCT/ SERVICE</th><th>DESCRIPTION</th><th>VERSION</th></tr><tr><td>Apex Central</td><td rowspan="2">A software management solution that provides the ability to control antivirus and content security programs from a central location—regardless of the platform or the physical location of the program.</td><td>• Any version</td></tr><tr><td>Trend Micro Control Manager</td><td>• 7.0 Patch 1</td></tr></table> See e.g., https://docs.trendmicro.com/all/ent/apex-one/patch/en-us/apexOne_p6_ag.pdf.	PRODUCT/ SERVICE	DESCRIPTION	VERSION	Apex Central	A software management solution that provides the ability to control antivirus and content security programs from a central location—regardless of the platform or the physical location of the program.	• Any version	Trend Micro Control Manager	• 7.0 Patch 1
PRODUCT/ SERVICE	DESCRIPTION	VERSION							
Apex Central	A software management solution that provides the ability to control antivirus and content security programs from a central location—regardless of the platform or the physical location of the program.	• Any version							
Trend Micro Control Manager		• 7.0 Patch 1							
[2A] generating, by the attestation server, an application artifact as a reference for changes in a subsequent execution context; and	Trend Micro Apex One (viewed through Trend Micro Apex Central) generates an application artifact (e.g., process ID) as a reference for changes in a subsequent execution context (i.e., to keep track of application instances).  The details screen provides more information about the event.								

Claim	Support
	See e.g., https://www.youtube.com/watch?v=DLiZcT7HzjU. Plaintiff contends that this element is literally present in the accused Trend Micro Apex One Products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses. Plaintiff reserves the right to supplement after inspection of relevant source code.
[2B] sending the generated application artifact such that subsequent changes to the runtime execution context are tracked based on the generated application artifact.	Trend Micro Apex One through Trend Micro Central sends (e.g., logs) the generated application artifact (e.g., recording of the first observed object associated with the analysis chain) such that subsequent changes to the runtime execution context (e.g., all associated processes/events/objects in the analysis chain) are tracked based on the application artifact (e.g., recording of the first observed object).  See e.g., https://www.youtube.com/watch?v=DLiZcT7HzjU. Plaintiff contends that this element is literally present in the accused Trend Micro Apex One Products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses. Plaintiff reserves the right to supplement after inspection of relevant source code.
3. The method according to	Trend Micro Apex One digitally signs the attestation results (e.g., Authentication ID).

Claim	Support
claim 2, further comprising digitally signing the attestation results, wherein the attributes further comprise parent-child process associations of the application.	 The details screen provides more information about the event.
	See e.g., https://www.youtube.com/watch?v=DLiZcT7HzjU. Attributes comprise parent-child process associations of the application (e.g., analysis chain components).  The analysis chain shows that the PsExec Service Host launched PuTTY See e.g., https://www.youtube.com/watch?v=DLiZcT7HzjU.

Claim	Support
	Plaintiff contends that this element is literally present in the accused Trend Micro Apex One Products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses. Plaintiff reserves the right to supplement after inspection of relevant source code.
4. The method of claim 1, wherein the received security context is an introspective security context, and wherein the execution analysis is a static, dynamic, or virtual analysis of the one or more executable file binaries and the loaded components.	The received security context (<i>e.g.</i>, malware analysis using predictive machine learning) is an introspective security analysis (<i>e.g.</i>, process behavior) of the one or more executable file binaries and the loaded components. The execution analysis (<i>e.g.</i>, behavior analysis) is a dynamic analysis of the one or more executable file binaries and the loaded components.  See <i>e.g.</i>, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-odne-2019-server-online-help/protecting-trend_cli/protecting-against-u_001/predictive-machine-l.aspx.

Claim	Support																		
	Plaintiff contends that this element is literally present in the accused Trend Micro Apex One Products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses. Plaintiff reserves the right to supplement after inspection of relevant source code.																		
5. The method of claim 4, wherein the generating of the report indicating security risks associated with the application includes generating, by the attestation server, one or more security assertions that pertain to the received runtime execution context and the received introspective security context.	The report indicating security risks associated with the application (<i>e.g.</i>, predictive machine learning log) includes one or more assertions (<i>e.g.</i>, threat probability) that pertain to the received runtime execution context. Predictive Machine Learning Log Details You can view a comprehensive report for each Predictive Machine Learning log detection by clicking the View link under the Details column. The Log Details screen consists of two sections: • Top banner: Specific details related to this particular log detection • Bottom tab controls: Details related to the Predictive Machine Learning threat, including threat probability scores, file information, and other endpoints across your network that have the same detection The following table discusses the information provided in the top banner. Table 1. Log Details - Top Banner <table> <tr> <th>Section</th><th>Description</th></tr> <tr> <td>Detection time / Action</td><td>Indicates when this specific log detection occurred and the action that the agent took on the threat</td></tr> <tr> <td>File name</td><td>Indicates the name of the file that triggered the detection on the specified endpoint Tip: Click Add to Exception List to quickly add the file hash value of the affected file to the global Predictive Machine Learning Exception list. View the entire exception list on the Predictive Machine Learning Settings screen. For more information, see Configuring Predictive Machine Learning Settings. Important: The detected file name for this detection may not be the same as the file name detected on other agents. Predictive Machine Learning associates detections according to file hash values, not specific file names. View the Affected Endpoints tab to verify the file name on other endpoints. </td></tr> <tr> <td>Endpoint information</td><td>Displays the logged on user at the time of the detection, the endpoint name, and the IP address of the endpoint</td></tr> <tr> <td>Channel information</td><td>Displays the channel from which the threat originated and the folder location on the endpoint the threat transferred to</td></tr> </table> The following table discusses the information provided on the bottom tabs. Table 2. Log Details - Tab Information <table> <tr> <th>Tab</th><th>Description</th></tr> <tr> <td>Threat Indicators</td><td>Provides the results of the Predictive Machine Learning analysis • Threat Probability: Indicates how closely the file/process matched the malware model • Probable Threat Type: Indicates the most likely type of threat contained in the file after Predictive Machine Learning compared the analysis to other known threats • Threat Identifiers: Provides a list of API functions used by the file/process that may be indicative of the detected threat type Important: API function identification is only one factor in the determination of the threat type. Predictive Machine Learning uses many other file features and analysis methods to calculate the threat probability and probable threat type. • Similar Known Threats: Provides a list of known threat types that exhibit similar file/process features to the detection </td></tr> <tr> <td>File Details</td><td>Provides general details related the file properties and certificate information for this specific detection log</td></tr> <tr> <td>Affected Endpoints</td><td>Displays a list of other agents on your network with the same Predictive Machine Learning detection and provides specific details about the detections on the other agents</td></tr> </table> See <i>e.g.</i>, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-one-2019-server-online-help/protecting-trend_cli/protecting-against-u_001/unknown-threat-logs/viewing-predictive-m/predictive-machine-l_001.aspx.	Section	Description	Detection time / Action	Indicates when this specific log detection occurred and the action that the agent took on the threat	File name	Indicates the name of the file that triggered the detection on the specified endpoint Tip: Click Add to Exception List to quickly add the file hash value of the affected file to the global Predictive Machine Learning Exception list. View the entire exception list on the Predictive Machine Learning Settings screen. For more information, see Configuring Predictive Machine Learning Settings. Important: The detected file name for this detection may not be the same as the file name detected on other agents. Predictive Machine Learning associates detections according to file hash values, not specific file names. View the Affected Endpoints tab to verify the file name on other endpoints.	Endpoint information	Displays the logged on user at the time of the detection, the endpoint name, and the IP address of the endpoint	Channel information	Displays the channel from which the threat originated and the folder location on the endpoint the threat transferred to	Tab	Description	Threat Indicators	Provides the results of the Predictive Machine Learning analysis • Threat Probability: Indicates how closely the file/process matched the malware model • Probable Threat Type: Indicates the most likely type of threat contained in the file after Predictive Machine Learning compared the analysis to other known threats • Threat Identifiers: Provides a list of API functions used by the file/process that may be indicative of the detected threat type Important: API function identification is only one factor in the determination of the threat type. Predictive Machine Learning uses many other file features and analysis methods to calculate the threat probability and probable threat type. • Similar Known Threats: Provides a list of known threat types that exhibit similar file/process features to the detection	File Details	Provides general details related the file properties and certificate information for this specific detection log	Affected Endpoints	Displays a list of other agents on your network with the same Predictive Machine Learning detection and provides specific details about the detections on the other agents
Section	Description																		
Detection time / Action	Indicates when this specific log detection occurred and the action that the agent took on the threat																		
File name	Indicates the name of the file that triggered the detection on the specified endpoint Tip: Click Add to Exception List to quickly add the file hash value of the affected file to the global Predictive Machine Learning Exception list. View the entire exception list on the Predictive Machine Learning Settings screen. For more information, see Configuring Predictive Machine Learning Settings. Important: The detected file name for this detection may not be the same as the file name detected on other agents. Predictive Machine Learning associates detections according to file hash values, not specific file names. View the Affected Endpoints tab to verify the file name on other endpoints.																		
Endpoint information	Displays the logged on user at the time of the detection, the endpoint name, and the IP address of the endpoint																		
Channel information	Displays the channel from which the threat originated and the folder location on the endpoint the threat transferred to																		
Tab	Description																		
Threat Indicators	Provides the results of the Predictive Machine Learning analysis • Threat Probability: Indicates how closely the file/process matched the malware model • Probable Threat Type: Indicates the most likely type of threat contained in the file after Predictive Machine Learning compared the analysis to other known threats • Threat Identifiers: Provides a list of API functions used by the file/process that may be indicative of the detected threat type Important: API function identification is only one factor in the determination of the threat type. Predictive Machine Learning uses many other file features and analysis methods to calculate the threat probability and probable threat type. • Similar Known Threats: Provides a list of known threat types that exhibit similar file/process features to the detection																		
File Details	Provides general details related the file properties and certificate information for this specific detection log																		
Affected Endpoints	Displays a list of other agents on your network with the same Predictive Machine Learning detection and provides specific details about the detections on the other agents																		

Claim	Support																				
	Plaintiff contends that this element is literally present in the accused Trend Micro Apex One Products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses. Plaintiff reserves the right to supplement after inspection of relevant source code.																				
6. The method according to claim 1, further comprising authenticating the application using a plurality of collaboration services.	The attestation server (<i>e.g.</i>, Apex One Server) allows for application authentication by a plurality of collaboration services (<i>e.g.</i>, IBM QRadar and Fortinet FortiSOAR). Summary Trend Micro has partnered with several prominent 3rd party solutions to offer select integration for enhanced security visibility and functionality. Below are several popular product integration links to more information for the specific solutions. This list will continue to be updated as more integration solutions become available. Trend Micro Apex Central / Control Manager <table> <tr> <th>Vendor</th><th>Description and Reference Link(s)</th></tr> <tr> <td>IBM QRadar</td><td>SNMP Traps for Control Manager (SNMPv1 or v2)</td></tr> <tr> <td>Fortinet</td><td>Apex Central Connector for FortiSOAR</td></tr> </table> Trend Micro Apex One / OfficeScan <table> <tr> <th>Vendor</th><th>Description and Reference Link(s)</th></tr> <tr> <td>IBM QRadar</td><td>DSM for OfficeScan (SNMPv2)</td></tr> </table> Trend Micro Cloud One / Deep Security <table> <tr> <th>Vendor</th><th>Description and Reference Link(s)</th></tr> <tr> <td>IBM QRadar</td><td>DSM for Trend Micro Deep Security</td></tr> <tr> <td>Fortinet</td><td>Deep Security Connector for FortiSOAR</td></tr> <tr> <td>Microsoft</td><td>Deep Security Connector for Azure Sentinel</td></tr> <tr> <td>Splunk</td><td>Trend Micro Deep Security App for Splunk</td></tr> </table> See <i>e.g.</i>, https://success.trendmicro.com/dcx/s/solution/000283019?language=en_US&sfdclFrameOrigin=null. Plaintiff contends that this element is literally present in the accused Trend Micro Apex One Products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses. Plaintiff reserves the right to supplement after inspection of relevant source code.	Vendor	Description and Reference Link(s)	IBM QRadar	SNMP Traps for Control Manager (SNMPv1 or v2)	Fortinet	Apex Central Connector for FortiSOAR	Vendor	Description and Reference Link(s)	IBM QRadar	DSM for OfficeScan (SNMPv2)	Vendor	Description and Reference Link(s)	IBM QRadar	DSM for Trend Micro Deep Security	Fortinet	Deep Security Connector for FortiSOAR	Microsoft	Deep Security Connector for Azure Sentinel	Splunk	Trend Micro Deep Security App for Splunk
Vendor	Description and Reference Link(s)																				
IBM QRadar	SNMP Traps for Control Manager (SNMPv1 or v2)																				
Fortinet	Apex Central Connector for FortiSOAR																				
Vendor	Description and Reference Link(s)																				
IBM QRadar	DSM for OfficeScan (SNMPv2)																				
Vendor	Description and Reference Link(s)																				
IBM QRadar	DSM for Trend Micro Deep Security																				
Fortinet	Deep Security Connector for FortiSOAR																				
Microsoft	Deep Security Connector for Azure Sentinel																				
Splunk	Trend Micro Deep Security App for Splunk																				
7. The method according to claim 1, further comprising	The attestation server (<i>e.g.</i>, Apex One Server) controls a user's transaction with the application (<i>e.g.</i>, whether the process could continue or was forced to terminate) by applying a set of authorization rules (<i>e.g.</i>, to terminate the process if Predictive Machine Learning determined that the application was a security risk) in accordance with the attestation results (<i>e.g.</i>, the Predictive Machine Learning determination).																				

Claim	Support						
controlling a user's transaction with the application by applying a set of authorization rules in accordance with the attestation results.	To enable Predictive Machine Learning: 1. Log on to the Apex One console. 2. Go to Agents > Agent Management. 3. In the Agent Tree, select the Apex One Server/Domain/Computer. 4. Go to Settings > Scan Settings. 5. Select "Predictive Machine Learning Settings". 6. Tick "Enable Predictive Machine Learning". 7. Under Detection Settings, select the following: ☒ Enable Predictive Machine Learning <table border="1"> <thead> <tr> <th>Type</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>☒ File</td> <td>Quarantine</td> </tr> <tr> <td>☒ Process</td> <td>Terminate</td> </tr> </tbody> </table> Apex One automatically disables Predictive Machine Learning on Windows Server platforms. Refer to the Online Help for more information. • Select to automatically Quarantine files that exhibit malware-related features based on the Predictive Machine Learning analysis. • Select to automatically Terminate processes that exhibit malware-related behaviors based on the Predictive Machine Learning analysis. Predictive Machine Learning attempts to clean the files that executed the malicious processes. If the clean action is unsuccessful, Apex One quarantines the affected files. 8. Click Apply to All Agents. See e.g., https://success.trendmicro.com/dcx/s/solution/1122594-configuring-predictive-machine-learning-settings-in-apex-one?language=en_US&sfdclFrameOrigin=null. Plaintiff contends that this element is literally present in the accused Trend Micro Apex One Products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses. Plaintiff reserves the right to supplement after inspection of relevant source code.	Type	Action	☒ File	Quarantine	☒ Process	Terminate
Type	Action						
☒ File	Quarantine						
☒ Process	Terminate						

Claim	Support																		
9. The method according to claim 1, further comprising providing confidence metrics in the attestation results indicating a level of security risk by different classifications such that a restriction on a user's transaction with the application are applied based on the level of security risk indicated by the confidence metrics in the attestation results.	Trend Micro Apex One generates a report (e.g., a log) indicating security risks (e.g., security threats) associated with the application (e.g., infected file/object or process) based on the received runtime execution context (e.g., threat identifiers) and the received security context (e.g., threat probability/type). Predictive Machine Learning Log Details You can view a comprehensive report for each Predictive Machine Learning log detection by clicking the View link under the Details column. The Log Details screen consists of two sections: - Top banner: Specific details related to this particular log detection - Bottom tab controls: Details related to the Predictive Machine Learning threat, including threat probability scores, file information, and other endpoints across your network that have the same detection The following table discusses the information provided in the top banner. Table 1. Log Details - Top Banner <table> <tr> <th>Section</th><th>Description</th></tr> <tr> <td>Detection time / Action</td><td>Indicates when this specific log detection occurred and the action that the agent took on the threat</td></tr> <tr> <td>File name</td><td>Indicates the name of the file that triggered the detection on the specified endpoint Tip: Click Add to Exception List to quickly add the file hash value of the affected file to the global Predictive Machine Learning Exception list. View the entire exception list on the Predictive Machine Learning Settings screen. For more information, see Configuring Predictive Machine Learning Settings. Important: The detected file name for this detection may not be the same as the file name detected on other agents. Predictive Machine Learning associates detections according to file hash values, not specific file names. View the Affected Endpoints tab to verify the file name on other endpoints. </td></tr> <tr> <td>Endpoint information</td><td>Displays the logged on user at the time of the detection, the endpoint name, and the IP address of the endpoint</td></tr> <tr> <td>Channel information</td><td>Displays the channel from which the threat originated and the folder location on the endpoint the threat transferred to</td></tr> </table> The following table discusses the information provided on the bottom tabs. Table 2. Log Details - Tab Information <table> <tr> <th>Tab</th><th>Description</th></tr> <tr> <td>Threat Indicators</td><td>Provides the results of the Predictive Machine Learning analysis Threat Probability: Indicates how closely the file/process matched the malware model Probable Threat Type: Indicates the most likely type of threat contained in the file after Predictive Machine Learning compared the analysis to other known threats Threat Identifiers: Provides a list a API functions used by the file/process that may be indicative of the detected threat type Important: API function identification is only one factor in the determination of the threat type. Predictive Machine Learning uses many other file features and analysis methods to calculate the threat probability and probable threat type. Similar Known Threats: Provides a list of known threat types that exhibit similar file/process features to the detection </td></tr> <tr> <td>File Details</td><td>Provides general details related the file properties and certificate information for this specific detection log</td></tr> <tr> <td>Affected Endpoints</td><td>Displays a list of other agents on your network with the same Predictive Machine Learning detection and provides specific details about the detections on the other agents</td></tr> </table> See e.g., https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-one-2019-server-online-help/protecting-trend_cli/protecting-against-u_001/unknown-threat-logs/viewing-predictive-m/predictive-machine-l_001.aspx.	Section	Description	Detection time / Action	Indicates when this specific log detection occurred and the action that the agent took on the threat	File name	Indicates the name of the file that triggered the detection on the specified endpoint Tip: Click Add to Exception List to quickly add the file hash value of the affected file to the global Predictive Machine Learning Exception list. View the entire exception list on the Predictive Machine Learning Settings screen. For more information, see Configuring Predictive Machine Learning Settings. Important: The detected file name for this detection may not be the same as the file name detected on other agents. Predictive Machine Learning associates detections according to file hash values, not specific file names. View the Affected Endpoints tab to verify the file name on other endpoints.	Endpoint information	Displays the logged on user at the time of the detection, the endpoint name, and the IP address of the endpoint	Channel information	Displays the channel from which the threat originated and the folder location on the endpoint the threat transferred to	Tab	Description	Threat Indicators	Provides the results of the Predictive Machine Learning analysis Threat Probability: Indicates how closely the file/process matched the malware model Probable Threat Type: Indicates the most likely type of threat contained in the file after Predictive Machine Learning compared the analysis to other known threats Threat Identifiers: Provides a list a API functions used by the file/process that may be indicative of the detected threat type Important: API function identification is only one factor in the determination of the threat type. Predictive Machine Learning uses many other file features and analysis methods to calculate the threat probability and probable threat type. Similar Known Threats: Provides a list of known threat types that exhibit similar file/process features to the detection	File Details	Provides general details related the file properties and certificate information for this specific detection log	Affected Endpoints	Displays a list of other agents on your network with the same Predictive Machine Learning detection and provides specific details about the detections on the other agents
Section	Description																		
Detection time / Action	Indicates when this specific log detection occurred and the action that the agent took on the threat																		
File name	Indicates the name of the file that triggered the detection on the specified endpoint Tip: Click Add to Exception List to quickly add the file hash value of the affected file to the global Predictive Machine Learning Exception list. View the entire exception list on the Predictive Machine Learning Settings screen. For more information, see Configuring Predictive Machine Learning Settings. Important: The detected file name for this detection may not be the same as the file name detected on other agents. Predictive Machine Learning associates detections according to file hash values, not specific file names. View the Affected Endpoints tab to verify the file name on other endpoints.																		
Endpoint information	Displays the logged on user at the time of the detection, the endpoint name, and the IP address of the endpoint																		
Channel information	Displays the channel from which the threat originated and the folder location on the endpoint the threat transferred to																		
Tab	Description																		
Threat Indicators	Provides the results of the Predictive Machine Learning analysis Threat Probability: Indicates how closely the file/process matched the malware model Probable Threat Type: Indicates the most likely type of threat contained in the file after Predictive Machine Learning compared the analysis to other known threats Threat Identifiers: Provides a list a API functions used by the file/process that may be indicative of the detected threat type Important: API function identification is only one factor in the determination of the threat type. Predictive Machine Learning uses many other file features and analysis methods to calculate the threat probability and probable threat type. Similar Known Threats: Provides a list of known threat types that exhibit similar file/process features to the detection																		
File Details	Provides general details related the file properties and certificate information for this specific detection log																		
Affected Endpoints	Displays a list of other agents on your network with the same Predictive Machine Learning detection and provides specific details about the detections on the other agents																		

Claim	Support
	Plaintiff contends that this element is literally present in the accused Trend Micro Apex One Products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses. Plaintiff reserves the right to supplement after inspection of relevant source code.