

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,

Petitioner,

v.

FORTINET, INC.,

Patent Owner.

PTAB Case No. IPR2023-00456

Patent No. 11,036,856 B2

PETITIONER'S DEMONSTRATIVES FOR ORAL ARGUMENT

Netskope, Inc. v. Fortinet, Inc.

IPR2023-00456

U.S. Patent No. 11,036,856

Claims 1-28

Petitioner Netskope's Demonstratives

Oral Hearing

May 31, 2024

Overview

1. “Moving” and “Copying” Are Interchangeable
2. Even If Not, “Copying” a File Is Obvious
3. A POSITA Would Have Been Motivated to Scan Files on A Network Security Device
4. Locating a Repository On a Security Device or External Storage Device Would Have Been Obvious Over Sharpe-Seese-Kamalapuram (Dependent Claims 8, 19, and 27)
5. A POSITA Would Have Been Motivated to Use Dods’ Malware Detection Techniques With Sharpe-Seese-Kamalapuram (Dependent Claims 3, 6, 11, 15, 17, 23, and 25)

Overview

1. “Moving” and “Copying” Are Interchangeable
 - A. The Intrinsic Record Shows “Moving” and “Copying” are Interchangeable
 - B. Extrinsic Evidence Shows “Moving” and “Copying” are Interchangeable
2. Even If Not, “Copying” a File Is Obvious
3. A POSITA Would Have Been Motivated to Scan Files on A Network Security Device
4. Locating a Repository On a Security Device or External Storage Device Would Have Been Obvious Over Sharpe-Seese-Kamalapuram (Dependent Claims 8, 19, and 27)
5. A POSITA Would Have Been Motivated to Use Dods’ Malware Detection Techniques With Sharpe-Seese-Kamalapuram (Dependent Claims 3, 6, 11, 15, 17, 23, and 25)

“Moving” and “Copying” Are Interchangeable

Intrinsic Record | Claim 1

1. A secure data transfer system comprising:
a non-transitory storage device having embodied therein one or more routines operable to prevent users of an enterprise network from accessing malware infected files that are stored within public cloud file stores; and one or more processors coupled to the non-transitory storage device and operable to execute the one or more routines, wherein the one or more routines include:
an untrusted file processing module, which when executed by the one or more processors:
accesses an untrusted file stored within a first repository of a public cloud file store, wherein the public cloud file store is natively mounted on a network security device that is protecting the enterprise network and wherein the users do not have read access to the first repository of the public cloud file store; and
causes the network security device to make a determination regarding whether the untrusted file is a clean file that is free of malicious content by applying one or more security checks to the untrusted file; and
a clean file transfer module, which when executed by the one or more processors, makes the clean file accessible to the users by, when a result of the determination is affirmative, copying the clean file from the first repository to a second repository that is accessible to the users.

“Moving” and “Copying” Are Interchangeable

Intrinsic Record | PO’s Characterization of the ’856 Patent

The insight disclosed in the ’856 patent, which is the reason for the claiming “copying” of files and which is entirely absent from Burdett, is reflected in Figure 1B. Ex. 2004 ¶¶ 56-58. Whereas in Figure 1A both the “clean” and “dirty” file store are part of the same “public cloud file store,” in Figure 1B the “clean file store” is not part of the same “public cloud file store” as the original “dirty file store.” ’856 patent at 9:17:23 (“[C]lean file store 110 may not be a part of public cloud store 104. For instance, the clean file store 110 can be a part of network security device 108 or can be a part of an external storage that forms part of the enterprise network such that users of the enterprise network can seamlessly access clean file store 110.”). When files are moved between physical storage devices, “moving” files without “copying” is not a practical option, and it becomes necessary to “copy” files, as claimed. Ex. 2004 ¶¶ 55, 58. Due to its recognition of this use case, the ’856 patent specifically claims “copying” files, while disclosing how that “copying” can be used to move files from a “public cloud file store” to outside that “public file store.”

“Moving” and “Copying” Are Interchangeable

Intrinsic Record | The Board’s Preliminary Finding

The patent ascribes no significance to copying or moving files. It uses both methods and applies the terms “copying,” “sharing,” “transferring,” and “move” *interchangeably*. Ex. 1001, 2:54–57 (*copying* a clean file to second repository), 3:24–36 (*copying* clean files to sanitized storage area), 5:52–57 (*copying* clean file from first to second repository), 6:5–10 (*copying* file by *sharing* via NFS, FTP, CIFS), 6:59–62 (*copying* a clean file from first to second repository), 8:53–57 (*copying and/or transferring* clean file from dirty file store 106 to clean file store 110), 10:28–33 (*copying* file by *sharing* via NFS, FTP, CIFS), 11:64–12:7 (clean file is *moved* to clean bucket).

As a further example, Figure 1A of the ’856 patent describes this process as “Clean Files are *Moved* to Clean File Store” (emphasis added). The description of Figure 1A states, “upon determining that the file at issue is clean, that is, free from malware, network security device 108 can make the clean file accessible to the users by *copying and/or transferring* the clean file from dirty file store 106 to clean file store 110 that is accessible to the users.” Ex. 1001, 8:53–57 (emphasis added); *id.* at Fig. 1B (“Clean Files are *Moved* to Clean File Store” (emphasis added)). Once again, the ’856 patent uses the terms “moving,” “copying,” and “transferring” *interchangeably*.

“Moving” and “Copying” Are Interchangeable

Intrinsic Record | Claim 5 Recites “Copying by Sharing”

5. The secure data transfer system of claim 1, wherein the network security device copies the file to the second repository by sharing it by means of any or a combination of network file system (NFS), file transfer protocol (FTP), common Internet file system (CIFS), Internet Small Computer Systems Interface (iSCSI), Storage Area Network (SAN), and local storage.

'856 Patent, Claim 5

“Moving” and “Copying” Are Interchangeable

Intrinsic Record | Claims 1 and 12 Use the Terms Interchangeably

1. A secure data transfer system comprising:
a non-transitory storage device having embodied therein one or more routines operable to prevent users of an enterprise network from accessing malware infected files that are stored within public cloud file stores; and one or more processors coupled to the non-transitory storage device and operable to execute the one or more routines, wherein the one or more routines include:
an untrusted file processing module, which when executed by the one or more processors:
accesses an untrusted file stored within a first repository of a public cloud file store, wherein the public cloud file store is natively mounted on a network security device that is protecting the enterprise network and wherein the users do not have read access to the first repository of the public cloud file store; and
causes the network security device to make a determination regarding whether the untrusted file is a clean file that is free of malicious content by applying one or more security checks to the untrusted file; and
a clean file transfer module, which when executed by the one or more processors, makes the clean file accessible to the users by, when a result of the determination is affirmative, copying the clean file from the first repository to a second repository that is accessible to the users.

'856 Patent, Claim 1

12. The secure data transfer system of claim 1, wherein the network security device makes said determination regarding whether the untrusted file is a clean file that is free of malicious content by first moving the untrusted file from the first repository to a third repository, and then applying one or more security checks to the untrusted file in the third repository, and moving back the checked file as a clean file into the first repository for onward copying to the second repository or moving the checked file as a clean file directly from the third repository to the second repository.

'856 Patent, Claim 12

“Moving” and “Copying” Are Interchangeable

Intrinsic Record | PO’s Interpretation Renders Claims Nonsensical

1. A secure data transfer system comprising:
a non-transitory storage device having embodied therein one or more routines operable to prevent users of an enterprise network from accessing malware infected files that are stored within public cloud file stores; and one or more processors coupled to the non-transitory storage device and operable to execute the one or more routines, wherein the one or more routines include:
an untrusted file processing module, which when executed by the one or more processors:
accesses an untrusted file stored within a first repository of a public cloud file store, wherein the public cloud file store is natively mounted on a network security device that is protecting the enterprise network and wherein the users do not have read access to the first repository of the public cloud file store; and
causes the network security device to make a determination regarding whether the untrusted file is a clean file that is free of malicious content by applying one or more security checks to the untrusted file; and
a clean file transfer module, which when executed by the one or more processors, makes the clean file accessible to the users by, when a result of the determination is affirmative, copying the clean file from the first repository to a second repository that is accessible to the users.

’856 Patent, Claim 1

12. The secure data transfer system of claim 1, wherein the network security device makes said determination regarding whether the untrusted file is a clean file that is free of malicious content by first moving the untrusted file from the first repository to a third repository, and then applying one or more security checks to the untrusted file in the third repository, and moving back the checked file as a clean file into the first repository for onward copying to the second repository or moving the checked file as a clean file directly from the third repository to the second repository.

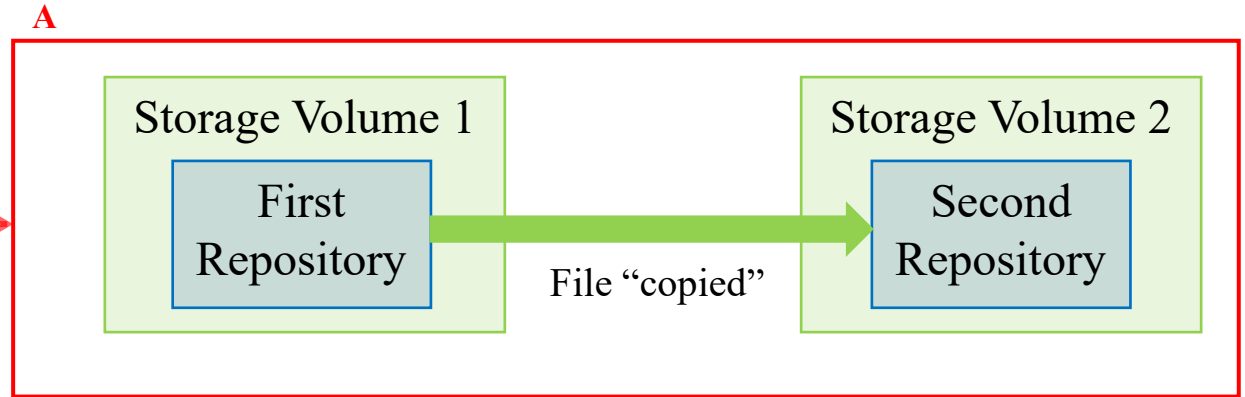
’856 Patent, Claim 12

“Moving” and “Copying” Are Interchangeable

Intrinsic Record | PO’s Interpretation Renders Claims Nonsensical

a clean file transfer module, which when executed by the one or more processors, makes the clean file accessible to the users by, when a result of the determination is affirmative, copying the clean file from the first repository to a second repository that is accessible to the users.

’856 Patent, Claim 1 (partial)

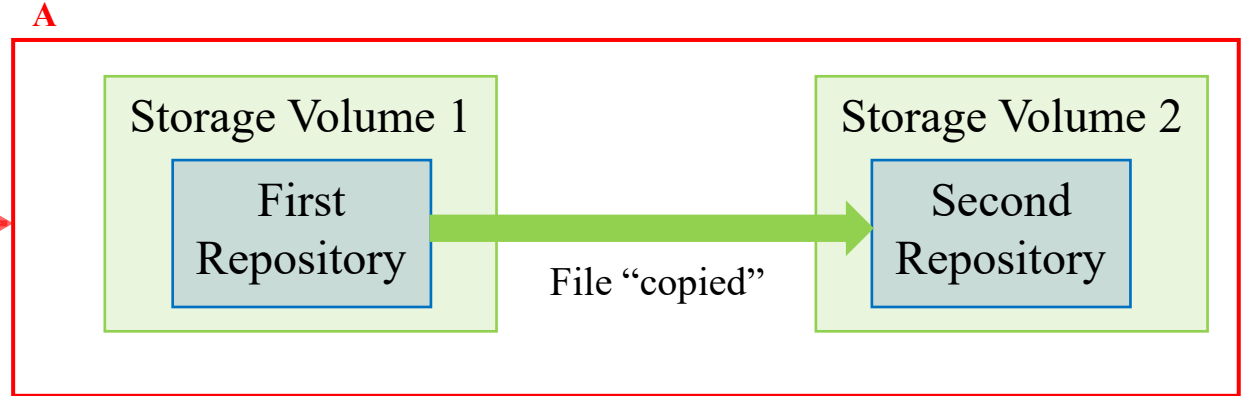


“Moving” and “Copying” Are Interchangeable

Intrinsic Record | PO’s Interpretation Renders Claims Nonsensical

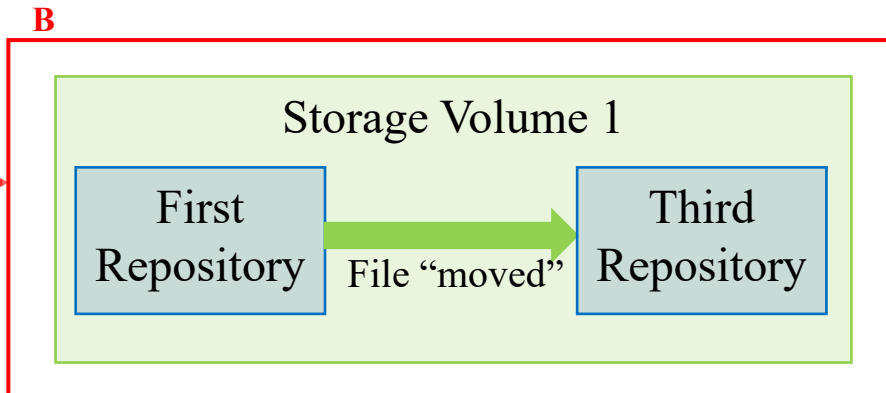
a clean file transfer module, which when executed by the one or more processors, makes the clean file accessible to the users by, when a result of the determination is affirmative, copying the clean file from the first repository to a second repository that is accessible to the users.

’856 Patent, Claim 1 (partial)



12. The secure data transfer system of claim 1, wherein the network security device makes said determination regarding whether the untrusted file is a clean file that is free of malicious content by first moving the untrusted file from the first repository to a third repository, and then applying one or more security checks to the untrusted file in the third repository, and moving back the checked file as a clean file into the first repository for onward copying to the second repository or moving the checked file as a clean file directly from the third repository to the second repository.

’856 Patent, Claim 12

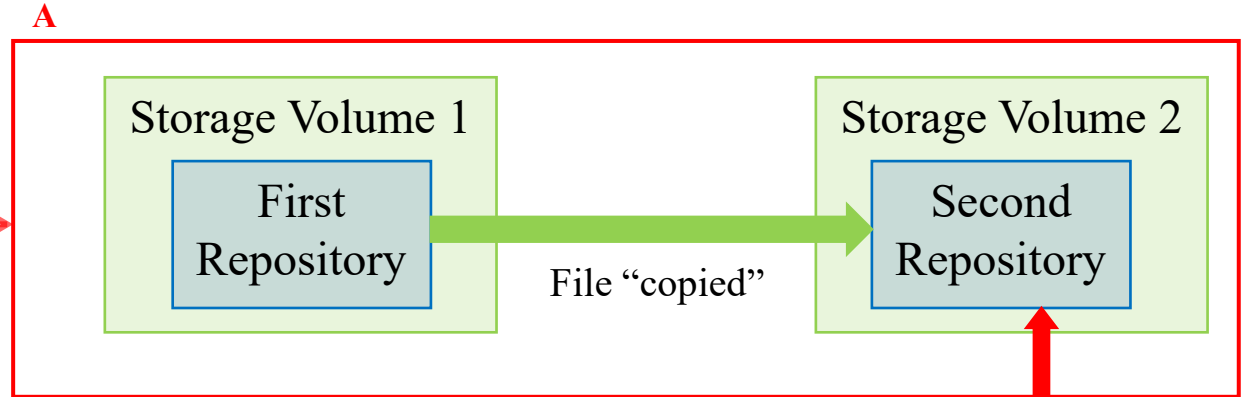


“Moving” and “Copying” Are Interchangeable

Intrinsic Record | PO's Interpretation Renders Claims Nonsensical

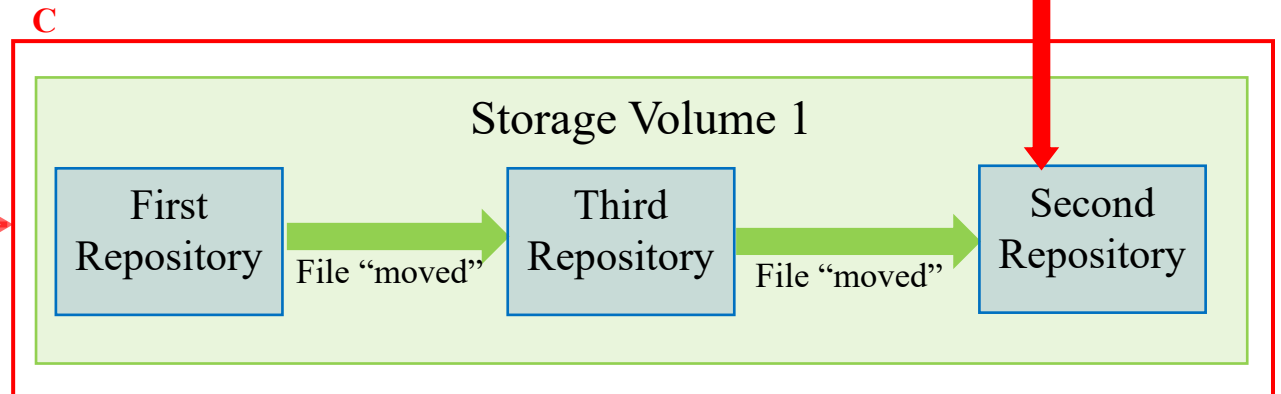
a clean file transfer module, which when executed by the one or more processors, makes the clean file accessible to the users by, when a result of the determination is affirmative, copying the clean file from the first repository to a second repository that is accessible to the users.

'856 Patent, Claim 1 (partial)



12. The secure data transfer system of claim 1, wherein the network security device makes said determination regarding whether the untrusted file is a clean file that is free of malicious content by first moving the untrusted file from the first repository to a third repository, and then applying one or more security checks to the untrusted file in the third repository, and moving back the checked file as a clean file into the first repository for onward copying to the second repository or moving the checked file as a clean file directly from the third repository to the second repository.

'856 Patent, Claim 12



“Moving” and “Copying” Are Interchangeable

Intrinsic Record | The Specification Uses “Moving” and “Copying” Interchangeably

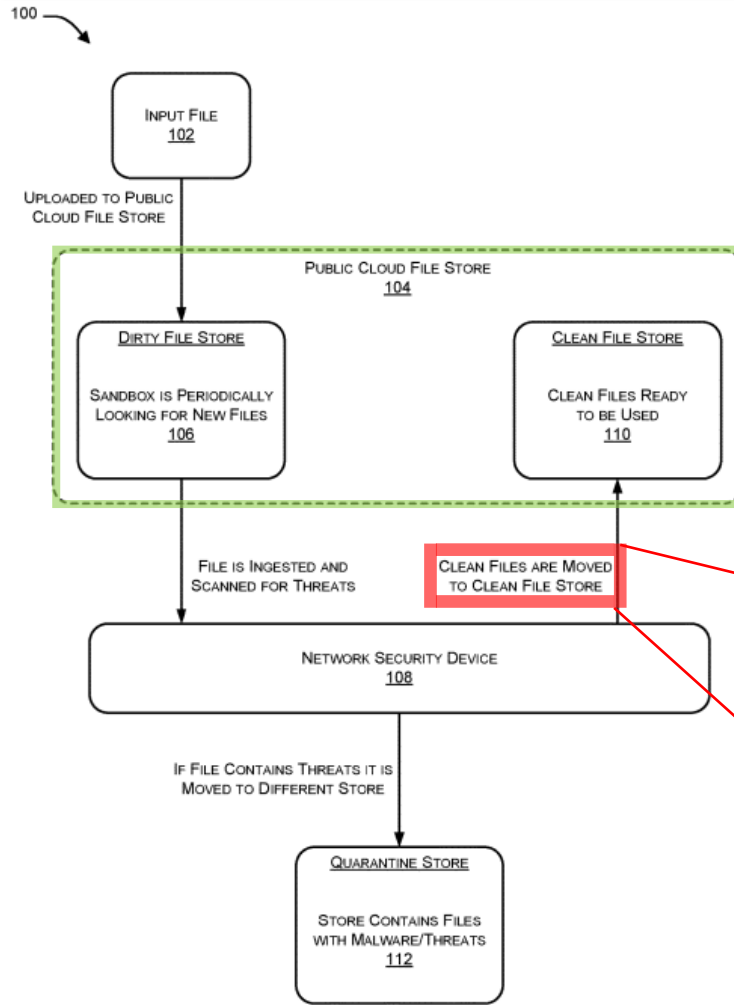


FIG. 1A

**CLEAN FILES ARE MOVED
TO CLEAN FILE STORE**

'856 Patent, Figs. 1A and 1B

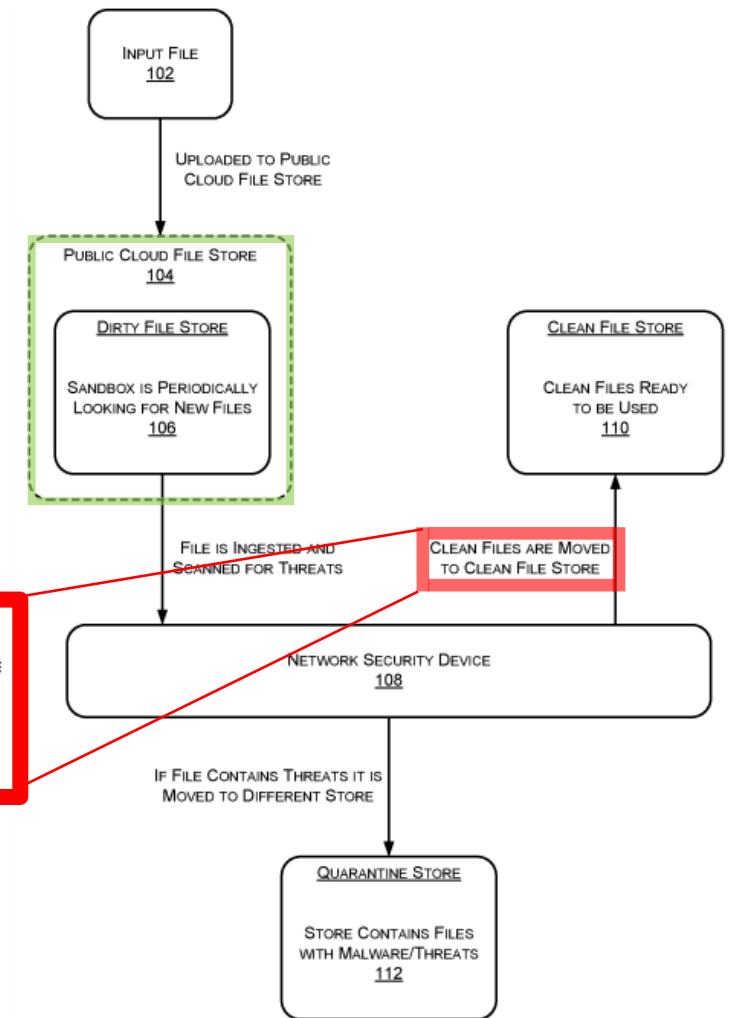


FIG. 1B

“Moving” and “Copying” Are Interchangeable

Intrinsic Record | The Specification Uses “Moving” and “Copying” Interchangeably

As noted above, upon determining that the file at issue is clean, that is, free from malware, network security device **108** can make the clean file accessible to the users by copying and/or transferring the clean file from dirty file store **106** to clean file store **110** that is accessible to the users.

'856 Patent, 8:53-57

that is inaccessible to end users and then after the untrusted files have been verified as being free of malware (clean) by a secure data transfer system, the verified clean files are transferred to a data location that is accessible to end users.

'856 Patent, 3:40-43

In an embodiment, the network security device can copy the file to the second repository by sharing it by means of any or a combination of network file system (NFS) file transfer protocol (FTP), common Internet file system (CIFS), Internet Small Computer Systems Interface (iSCSI), Storage Area Network (SAN), and local storage.

'856 Patent, 6:5-10

Overview

1. “Moving” and “Copying” Are Interchangeable
 - A. The Intrinsic Record Shows “Moving” and “Copying” are Interchangeable
 - B. Extrinsic Evidence Shows “Moving” and “Copying” are Interchangeable
2. Even If Not, “Copying” a File Is Obvious
3. A POSITA Would Have Been Motivated to Scan Files on A Network Security Device
4. Locating a Repository On a Security Device or External Storage Device Would Have Been Obvious Over Sharpe-Seese-Kamalapuram (Dependent Claims 8, 19, and 27)
5. A POSITA Would Have Been Motivated to Use Dods’ Malware Detection Techniques With Sharpe-Seese-Kamalapuram (Dependent Claims 3, 6, 11, 15, 17, 23, and 25)

“Moving” and “Copying” Are Interchangeable

Extrinsic Evidence | PO Uses “Moving” and “Copying” Interchangeably

Administration Guide, FortiSandbox 4.2.4

June 12, 2023

Enable copying or moving clean files to a sanitized location

Copy or move files with a Clean rating to another location.

By default, a new folder is created for each scheduled scan job in the sanitized location and all clean files are copied into it with the original folder structure. To save space, uncheck *Keep a complete copy of clean files for every scheduled scan* so that files of the same path have only one copy in the sanitized location.

Ex. 2003, 76



When a file is moved, to leave a copy in its original location, go to the Quarantine edit page or sanitized share and select the *Keep Original File At Current Location*.

Ex. 2003, 76

Keep Original File At Current Location

Select to keep the original file at the current location when a file is quarantined from a network share. By default, the original file is kept at its current location when being moved.

Ex. 2003, 79

Enable moving clean files to a sanitized location

Select to move Clean rating files to another location. By default, a new folder is created for each scheduled scan job in the sanitized location and all clean files are copied under it with the original folder structure. To save storage size, the user can un-check *Keep a complete copy of clean files for every scheduled scan*, then files of the same path will have only one copy saved in the sanitized location.

Ex. 2003, 99

Overview

1. “Moving” and “Copying” Are Interchangeable
2. Even If Not, “Copying” a File Is Obvious
 - A. Burdett Renders Obvious “Copying”
 - B. Kamalapuram Renders Obvious “Copying”
3. A POSITA Would Have Been Motivated to Scan Files on A Network Security Device
4. Locating a Repository On a Security Device or External Storage Device Would Have Been Obvious Over Sharpe-Seese-Kamalapuram (Dependent Claims 8, 19, and 27)
5. A POSITA Would Have Been Motivated to Use Dods’ Malware Detection Techniques With Sharpe-Seese-Kamalapuram (Dependent Claims 3, 6, 11, 15, 17, 23, and 25)

Even If Not Interchangeable with “Moving,” “Copying” a File Is Obvious

5 Q. And when you said moving could be much
6 more significant undertaking, you're thinking about
7 copying?

8 A. Right. So there's sort of two species of
9 moving a file, right? And one is that it moves
10 within the same file system. And in that case, the
11 file contents are untouched, but the metadata that
12 describes where the file lives, you might change
13 its name or change its location within the file
14 system. And this is an almost instantaneous step.
15 You just go to this -- in Linux, it's called an
16 inode. You go to this inode, and you say cross out
17 the old location, put it in the new location. It's
18 moved in a sense, but the contents of the file on
19 the disk hasn't been touched. It remains in its
20 place.

21 But there's the second species of move,
22 which is a much more significant step, which you

1 can think of it as a copy and an erasure of the
2 original. And you wouldn't want to do that unless
3 you had to, because it's going to take a lot of
4 time and consume a lot of resources and perhaps
5 expose you to some security risks. So in that
6 case, you only do it when it's not possible to
7 simply update the metadata. You don't have any
8 other choice, because you're moving it to a
9 different file system, perhaps even across the
10 network or something. Your only choice really,
11 then, is to do a copy, and then erase the original.

Black Dep. Tr., 9:5-10:11

Even If Not Interchangeable with “Moving,” “Copying” a File Is Obvious

Burdett

The scanning service **304** accesses files to be scanned directly from the cloud data store **306** that is used by the virtual machine instances, which avoids overhead and performance delay. The use of virtual machine instances for the scanning that are different from the virtual machine instances of the application facilitate management and reduce complexity. In some implementations, the scanning service provides alerts to an administrator, but does not attempt to control access to files. In some implementations, the scanning service may move files or change the name of files in order to control access. For example, to prevent access to a file, the scanning service may change the name or the location (e.g., path in a file system) of a file in order to prevent access. In some implementations, the scanning service **304** may replace a file with another file that is “clean.”

Burdett, 25:18-33

Even If Not Interchangeable with “Moving,” “Copying” a File Is Obvious *Burdett*

Burdett’s disclosure is not limited to moving a file within the same file system
– the “moving without copying” species described by PO.

Reply, 18

Referring now to FIG. 3, an example system 300 includes a cloud infrastructure 302 that includes a scanning service 304 and virtual machines running on one or more virtual private clouds 314. Applications instantiated on virtual machines within the virtual private clouds 314 may access one or more cloud data stores 306 for storage of data. Administrators may configure the virtual private clouds in zones, and may architect applications to store in and receive data from the cloud data store 306 so as to provide fault tolerance and availability.

Burdett, 23:34-42

In decision block 410, the security manger determines whether the scanning service can scan for multiple data stores (e.g., multiple S3 buckets). For example, the scanning service may be associated with multiple data stores, cloud infrastructure zones, applications, etc. For example, these may be configured or selected using the security manager.

Burdett, 28:1-6

Overview

1. “Moving” and “Copying” Are Interchangeable
2. Even If Not, “Copying” a File Is Obvious
 - A. Burdett Renders Obvious “Copying”
 - B. Kamalapuram Renders Obvious “Copying”**
3. A POSITA Would Have Been Motivated to Scan Files on A Network Security Device
4. Locating a Repository On a Security Device or External Storage Device Would Have Been Obvious Over Sharpe-Seese-Kamalapuram (Dependent Claims 8, 19, and 27)
5. A POSITA Would Have Been Motivated to Use Dods’ Malware Detection Techniques With Sharpe-Seese-Kamalapuram (Dependent Claims 3, 6, 11, 15, 17, 23, and 25)

Even If Not Interchangeable with “Moving,” “Copying” a File Is Obvious

Kamalapuram

Sharpe did not explicitly describe that the “clean” file would be copied to a second repository, but Kamalapuram did. In Kamalapuram, a “file may be stored *in an isolated area of the network storage system* while waiting to be scanned, and may be *moved to a general storage area* only after the file has been scanned by a security analysis system of the network storage system.” (Kamalapuram, [0122].)

Petition, 67-68

Overview

1. “Moving” and “Copying” Are Interchangeable
2. Even If Not, “Copying” a File Is Obvious
3. **A POSITA Would Have Been Motivated to Scan Files on A Network Security Device**
 - A. **Burdett and FortiSandbox**
 - B. Sharpe, Seese, and Kamalapuram
4. Locating a Repository On a Security Device or External Storage Device Would Have Been Obvious Over Sharpe-Seese-Kamalapuram (Dependent Claims 8, 19, and 27)
5. A POSITA Would Have Been Motivated to Use Dods’ Malware Detection Techniques With Sharpe-Seese-Kamalapuram (Dependent Claims 3, 6, 11, 15, 17, 23, and 25)

A POSITA Would Have Been Motivated to Scan Files on A Network Security Device

Burdett and FortiSandbox

In the Burdett-FortiSandbox combination, at least some of the operations conducted by Burdett's scanning service would have been performed by a device, like a FortiSandbox device (a network security device). A POSITA would naturally position the FortiSandbox device in a position to protect an enterprise network because that would improve Burdett's disclosed system for protecting an enterprise network. (Franz, ¶88; *see also, supra*, "enterprise network" in 1[a].)

Moreover, FortiSandbox corroborated Burdett's disclosure of scanning files in a file store. For example, once a new network share had been configured as described above, the FortiSandbox device would "scan files stored on [the] network share and optionally quarantine any malicious files." (FortiSandbox, 113.) Scans could be "scheduled or run on-demand." (*Id.*, 114.) Thus, performing Burdett's scanning service operations on the FortiSandbox device would have been a combination of prior art elements according to known methods to yield predictable results. (Franz, ¶¶85-89.)

A POSITA Would Have Been Motivated to Scan Files on A Network Security Device

Burdett and FortiSandbox

Configuring a device like the FortiSandbox system to perform Burdett's malware scans would have enabled an enterprise to preserve the privacy of its files in cloud storage while preventing enterprise users from accessing malicious files. (Franz, ¶¶69-70.)

A POSITA Would Have Been Motivated to Scan Files on A Network Security Device

Burdett and FortiSandbox

A POSITA would have found it obvious to make this combination by natively mounting the public cloud file store on the network security device. Doing so would have enabled the network security device to access files in the cloud file store and to natively communicate with the cloud file store to perform actions such as controlling file access. (Franz, ¶89.) It also would have enabled the network security device to perform scheduled or on-demand bulk scans within the cloud file store. (Burdett, 2:5-17; FortiSandbox, 114; Franz, ¶¶85-89; *see also* '856 patent, 11:66-12:4.)

A POSITA Would Have Been Motivated to Scan Files on A Network Security Device

Burdett and FortiSandbox

5 As one example, an implementation of an agentless
scanning service configured for AWS infrastructure uses S3
buckets for file storage, registers with the S3 service to
receive notifications of file activity, receives notifications of
file activity, and scans files upon receiving the notifications.
10 If the scan result is positive, action may be taken to protect
the application, such as setting permissions to make the file
unavailable, notifying an administrator, moving the file,
renaming the file, encrypting the file, etc. The agentless
15 scanning service simplifies workflow for deploying and
managing data protection (e.g., anti-malware, data loss
prevention) for applications making use of cloud resources.
Applications that are fully implemented in the cloud and
applications implemented elsewhere but that make use of
20 cloud or remote storage resources may make use of an
agentless scanning service.

Burdett, 2:5-21

Network share scans can be scheduled or run on-demand, and connectivity with the network share can be tested.

FortiSandbox, 114

Overview

1. “Moving” and “Copying” Are Interchangeable
2. Even If Not, “Copying” a File Is Obvious
3. **A POSITA Would Have Been Motivated to Scan Files on A Network Security Device**
 - A. Burdett and FortiSandbox
 - B. **Sharpe, Seese, and Kamalapuram**
4. Locating a Repository On a Security Device or External Storage Device Would Have Been Obvious Over Sharpe-Seese-Kamalapuram (Dependent Claims 8, 19, and 27)
5. A POSITA Would Have Been Motivated to Use Dods’ Malware Detection Techniques With Sharpe-Seese-Kamalapuram (Dependent Claims 3, 6, 11, 15, 17, 23, and 25)

A POSITA Would Have Been Motivated to Scan Files on A Network Security Device

Sharpe, Seese, and Kamalapuram

It would have been obvious to a POSITA to natively mount a public cloud file store, as taught by Seese and suggested by Sharpe, on a network security device as taught by Seese, as a means to enable a network security device to access files in the cloud file store and to natively communicate with the cloud file store to perform actions such as controlling access to the files. (Franz, ¶¶163-164.)

A POSITA Would Have Been Motivated to Scan Files on A Network Security Device

Sharpe, Seese, and Kamalapuram

increasing performance. Note, however, that executing a cloud controller in a cloud storage provider environment implies trust in this environment; the cloud controller needs to decrypt the files before transferring them to the anti-virus
25 service, and hence if the environment is compromised the files may be readable by other parties. If this risk is unacceptable, another substantially similar configuration could use a dedicated physical cloud controller and an anti-virus service that are located at a secure site in close network
30 proximity with the cloud storage system (and have a high-bandwidth link to the cloud storage system) to perform anti-virus scans for the distributed filesystem.

Sharpe, 98:21-32

A POSITA Would Have Been Motivated to Scan Files on A Network Security Device

Sharpe, Seese, and Kamalapuram

The Sharpe-Seese-Kamalapuram combination also would have produced a malware detection system for an enterprise that improved security. For example, the Seese's DLP server was a physical device deployed within an enterprise's network infrastructure. (Seese, [0063].) Configuring Seese's server to perform Sharpe's malware scans would have enabled an enterprise to preserve privacy of the enterprise's files stored within a cloud storage system, one of Sharpe's expressly-stated goals. (Sharpe, 98:27-32; Franz, ¶140.)

Overview

1. “Moving” and “Copying” Are Interchangeable
2. Even If Not, “Copying” a File Is Obvious
3. A POSITA Would Have Been Motivated to Scan Files on A Network Security Device
4. **Locating a Repository On a Security Device or External Storage Device Would Have Been Obvious Over Sharpe-Seese-Kamalapuram (Dependent Claims 8, 19, and 27)**
5. A POSITA Would Have Been Motivated to Use Dods’ Malware Detection Techniques With Sharpe-Seese-Kamalapuram (Dependent Claims 3, 6, 11, 15, 17, 23, and 25)

Locating a Repository On a Security Device or External Storage Device Would Have Been Obvious Over Sharpe-Seese-Kamalapuram (Dependent Claims 8, 19, and 27)

8. The secure data transfer system of claim 1, wherein the second repository is part of the network security device or part of an external storage device that forms part of the enterprise network.

Locating a Repository On a Security Device or External Storage Device Would Have Been Obvious Over Sharpe-Seese-Kamalapuram (Dependent Claims 8, 19, and 27)

Locating the second repository on the network security device or on an external storage device in an enterprise network would have therefore been within the capability of a skilled artisan and would have simply been an implementation decision by an enterprise network administrator based on, for example, the importance of the data. A POSITA would have been motivated to use such a hybrid cloud storage model in which the second repository is located on the network security device or an external storage device, since this configuration would have improved security of files associated with the enterprise. (Franz, ¶200.)

Overview

1. “Moving” and “Copying” Are Interchangeable
2. Even If Not, “Copying” a File Is Obvious
3. A POSITA Would Have Been Motivated to Scan Files on A Network Security Device
4. Locating a Repository On a Security Device or External Storage Device Would Have Been Obvious Over Sharpe-Seese-Kamalapuram (Dependent Claims 8, 19, and 27)
5. A POSITA Would Have Been Motivated to Use Dods’ Malware Detection Techniques With Sharpe-Seese-Kamalapuram (Dependent Claims 3, 6, 11, 15, 17, 23, and 25)

A POSITA Would Have Been Motivated to Use Dods' Malware Detection Techniques With Sharpe-Seese-Kamalapuram (Dependent Claims 3, 6, 11, 15, 17, 23, and 25)

6. Dependent Claims 2–7, 9–12, 14–18, 20, 22–26, and 28

Petitioner provides detailed contentions with a detailed mapping of how Burdett and FortiSandbox teach or suggest the limitations of dependent claims 2–7, 9–12, 14–18, 20, 22–26, and 28 with supporting testimony of Dr. Franz. Pet. 38–50. These contentions, which Patent Owner does not contest at this stage, are supported sufficiently by evidence of record.

On this record, we find that Petitioner has shown a reasonable likelihood that claims 2–7, 9–12, 14–18, 20, 22–26, and 28 would have been unpatentable over Burdett and FortiSandbox.

A POSITA Would Have Been Motivated to Use Dods' Malware Detection Techniques With Sharpe-Seese-Kamalapuram (Dependent Claims 3, 6, 11, 15, 17, 23, and 25)

In addition, Petitioner identifies no motivation to combine the additional cited art from Ground 3 (Dods) with the cited art from Petitioner's Ground 2. At best, Petitioner writes that "Dods described additional mechanisms to detect malware in a file that were not taught by the other references" (Pet. at 78), but does not even identify what those alleged "additional mechanisms" are, much less how they address shortcoming (if any) in Petitioner's "Sharpe-Seese-Kamalapuram combination." Ex. 2004 ¶ 84. The cited paragraph from Petitioner's expert declaration repeats that assertion almost verbatim, but adds no further explanation as to the nature of Dods' alleged "additional mechanisms" or why it would be desirable to add them to "the Sharpe-Seese-Kamalapuram combination." Ex. 1002 ¶ 211. Accordingly, Petitioner has failed to articulate any rationale for combining Dods with its other three cited art references, and thus has failed to show that claims 3, 6, 11, 15, 17, 23, and 25 of the '856 patent are rendered obvious by the combination in Ground 3. Ex. 2004 ¶ 84.

A POSITA Would Have Been Motivated to Use Dods' Malware Detection Techniques With Sharpe-Seese-Kamalapuram (Dependent Claims 3, 6, 11, 15, 17, 23, and 25)

1. Motivation to combine

Like Sharpe and Kamalapuram, Dods was directed to processing files for malware identification. (Dods, Title, Abstract.) Accordingly, a POSITA would have been motivated to combine these complementary disclosures. (Franz, ¶210.)

Adding Dods to the Sharpe-Seese-Kamalapuram combination also would have improved the resulting malware detection system. For example, Dods described additional mechanisms to detect malware in a file that were not taught by the other references. A POSITA would have been motivated to use Dods to supplement the Sharpe-Seese-Kamalapuram combination in order to improve its malware detection capabilities. (Franz, ¶211.)

A POSITA Would Have Been Motivated to Use Dods' Malware Detection Techniques With Sharpe-Seese-Kamalapuram (Dependent Claims 3, 6, 11, 15, 17, 23, and 25)

2. Claims 3/15/23

c. 3[a]:

The Sharpe-Seese-Kamalapuram combination did not disclose the features of claim 3/15/23, but Dods did. Dods disclosed a security platform that “identif[ied] [a] malicious payload within [a] file using a secure environment (e.g., a sandbox).” (Dods, 2:5-7; *see also* 4:40-42.) As taught by Dods, the security platform “include[d] one or more devices.” (*Id.*, 4:28.) Thus, Dods disclosed a sandbox appliance. (Franz, ¶¶212-213.)

A POSITA Would Have Been Motivated to Use Dods' Malware Detection Techniques With Sharpe-Seese-Kamalapuram (Dependent Claims 3, 6, 11, 15, 17, 23, and 25)

3. Claims 6/17/25: ... wherein the untrusted file processing module further removes any malware from the untrusted file that is detected by the one or more security checks when the result of said determining is negative.

The Sharpe-Seese-Kamalapuram combination did not disclose the features of claims 6/17/25, but Dods did. Dods described the security platform as being configured to “scrub the received file to remove the malicious object” after detecting malware. (Dods, 11:42-48.) (Franz, ¶215.)

A POSITA Would Have Been Motivated to Use Dods' Malware Detection Techniques With Sharpe-Seese-Kamalapuram (Dependent Claims 3, 6, 11, 15, 17, 23, and 25)

4. Claim 11:

Dods disclosed the features of claim 11. For example, Dods described the security platform determining whether a file is free of malicious content using at least “a signature-based analysis” (file signature; Dods, 10:18) and “a static analysis (analyzing the secondary file without opening the secondary file)” (file pre-scan parameters; *id.*, 10:17-18.) (Franz, ¶216.)

Fig. 1A

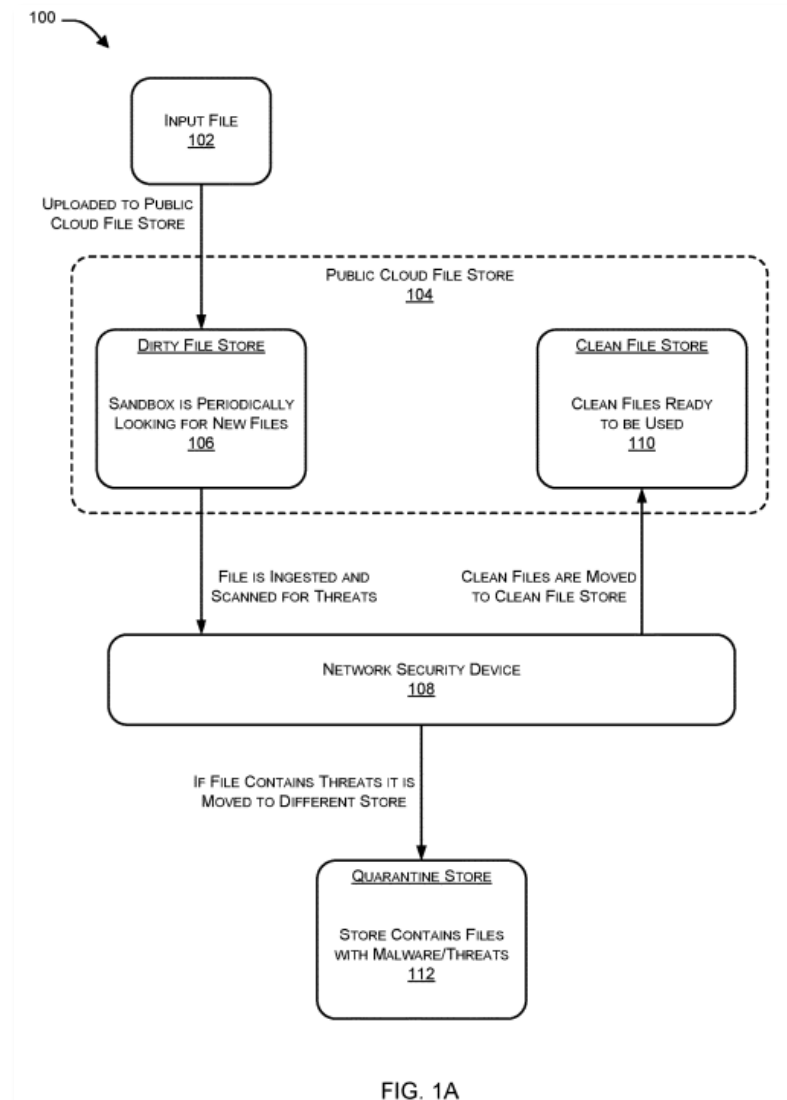
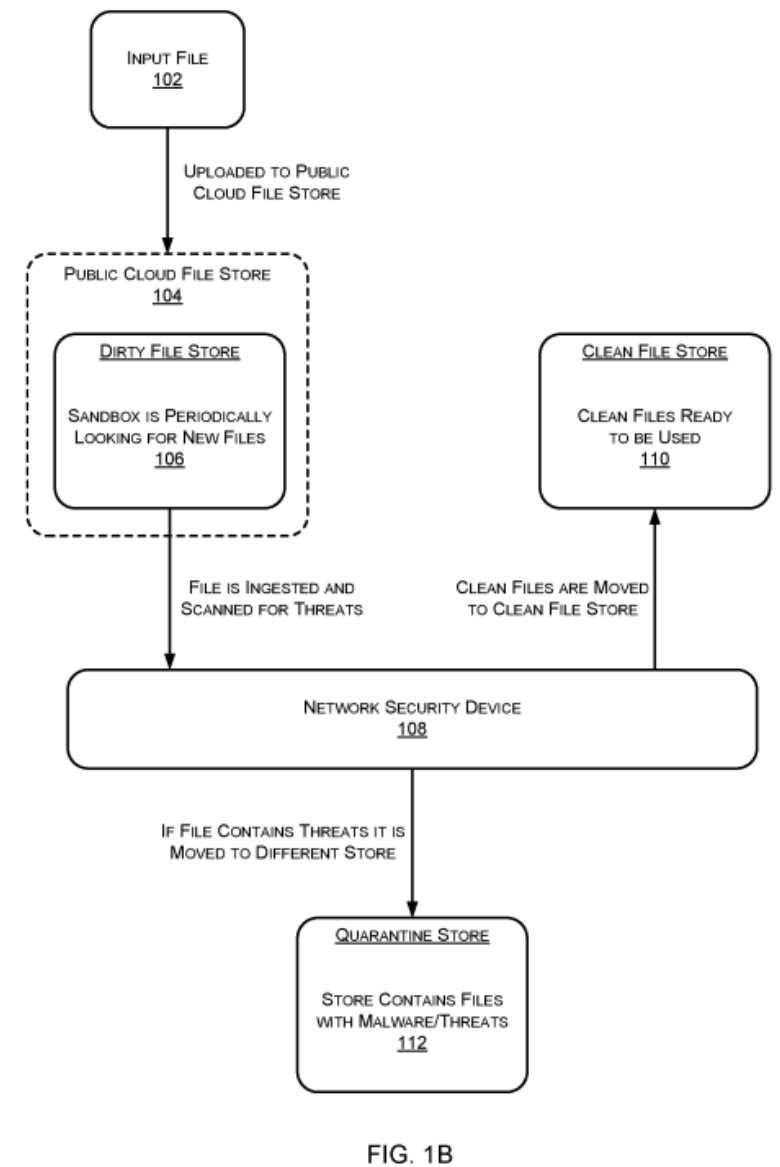
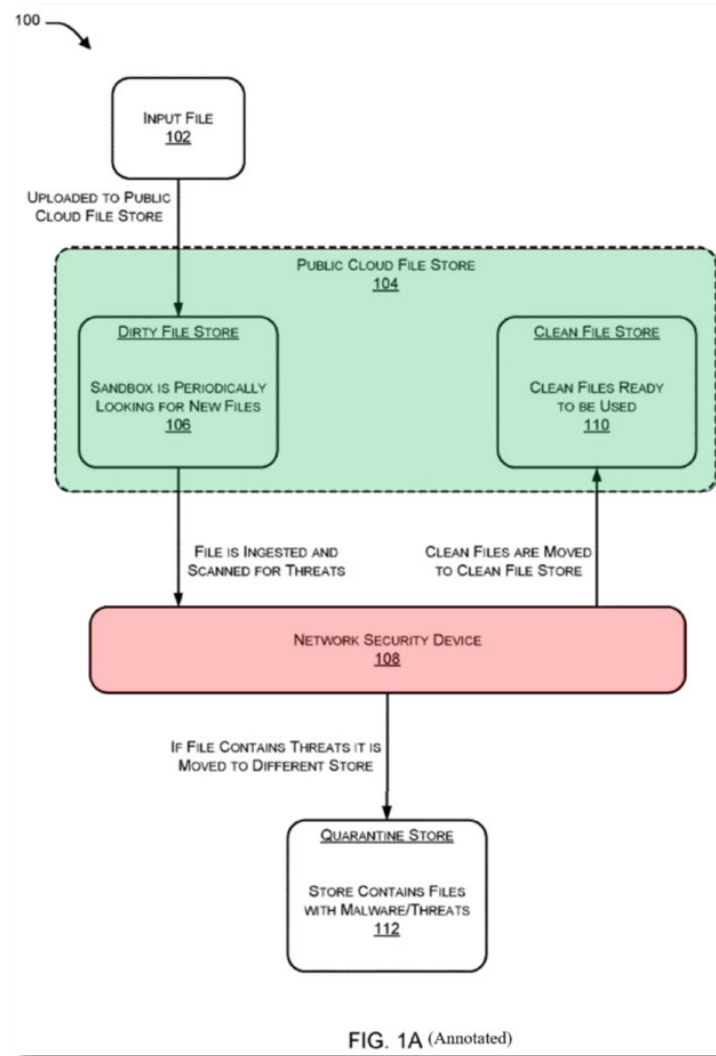


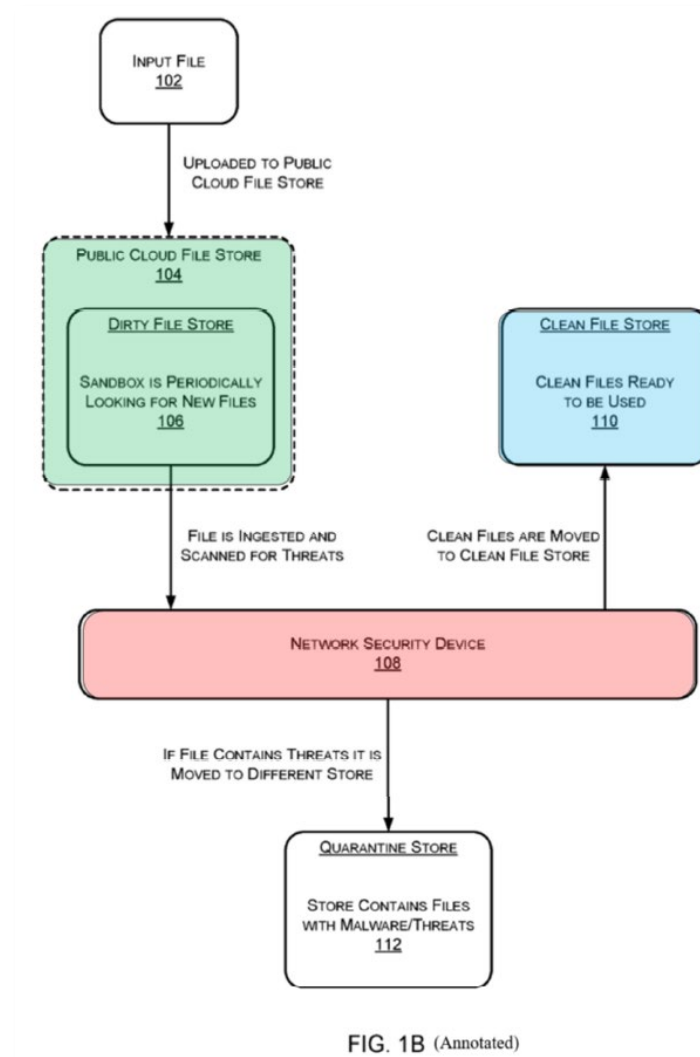
Fig. 1B

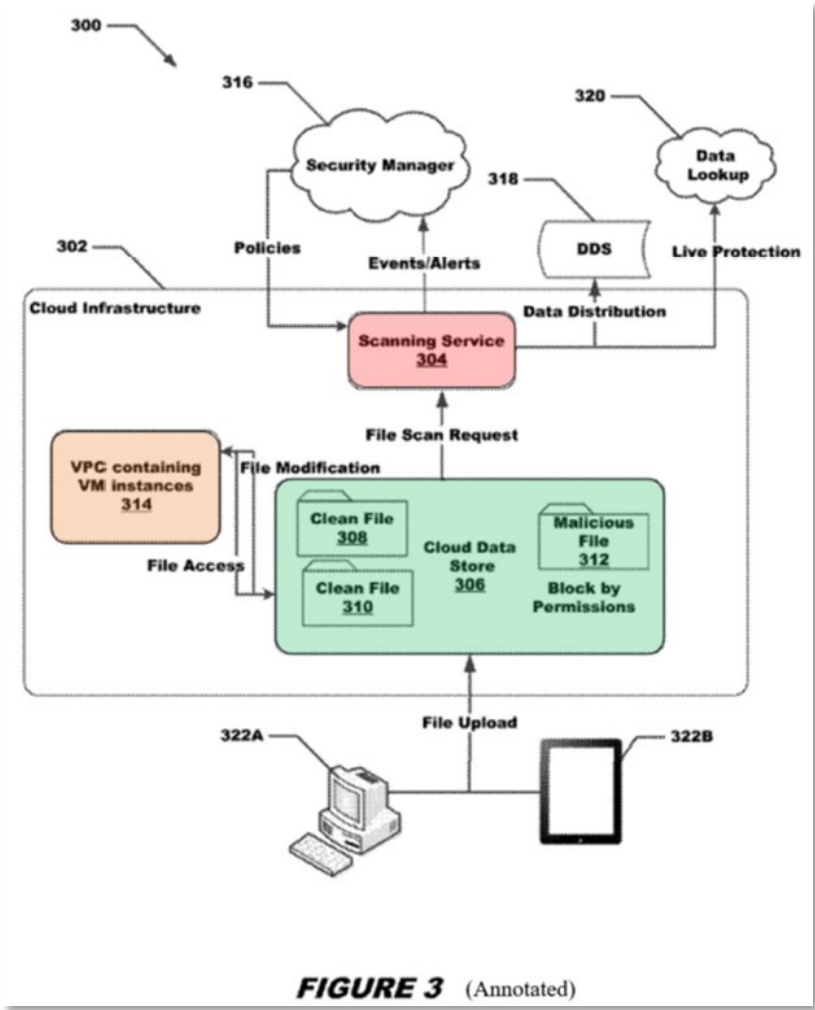


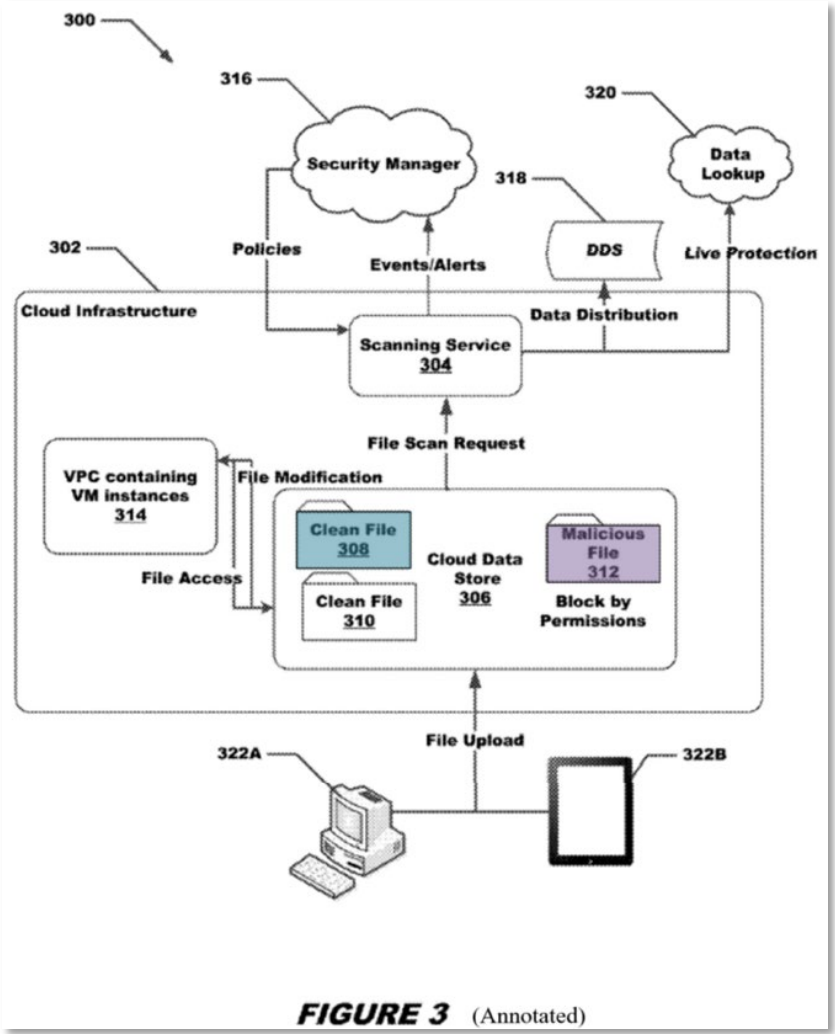
Annotated '856 Figures

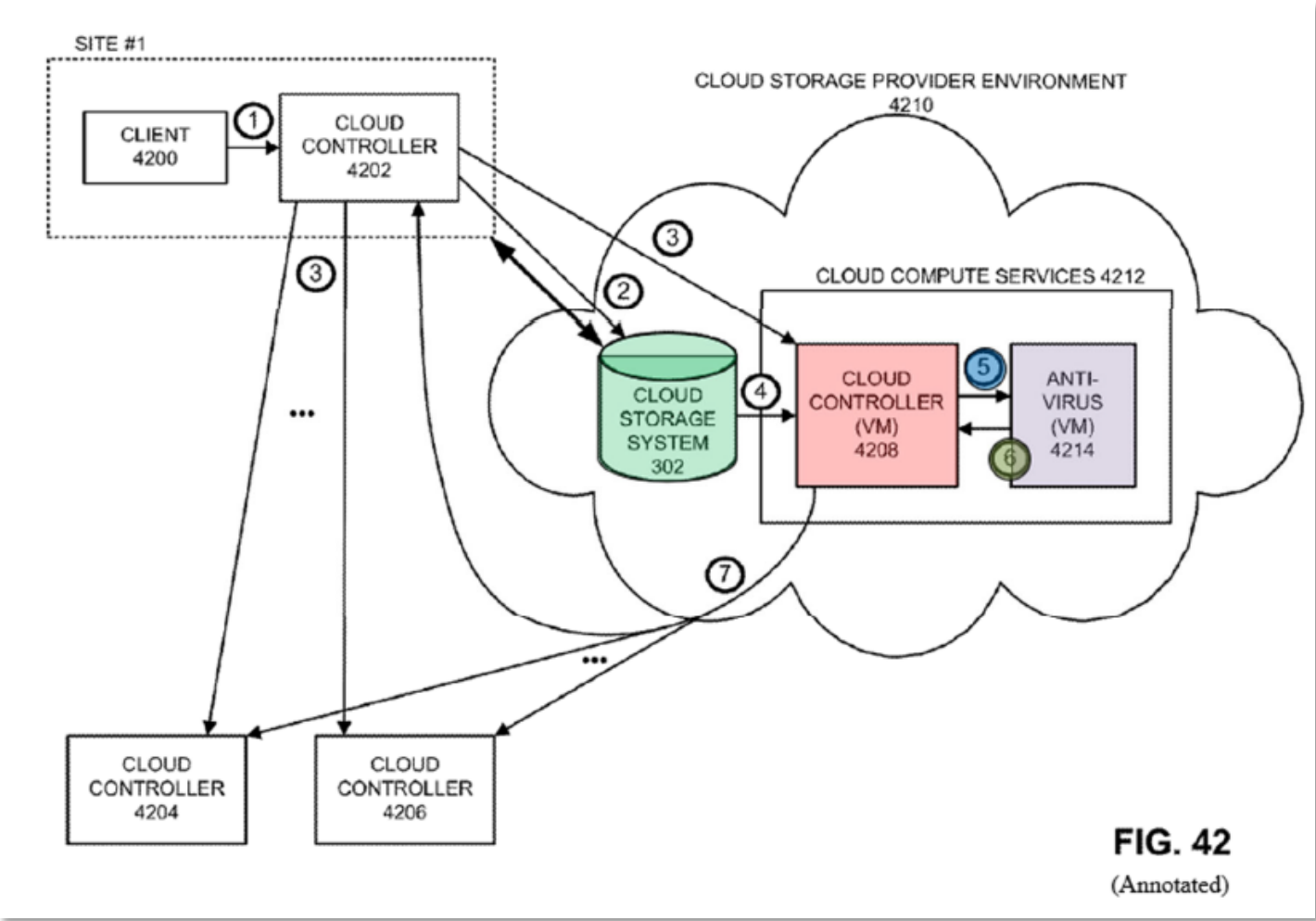


Annotated '856 Figures









PO Argues “Copying” Applies Only When Source and Destination are on Different Volumes

8 A. Right. So there's sort of two species of
9 moving a file, right? And one is that it moves
10 within the same file system. And in that case, the

...

21 But there's the second species of move,
22 which is a much more significant step, which you
1 can think of it as a copy and an erasure of the
2 original. And you wouldn't want to do that unless
3 you had to, because it's going to take a lot of
4 time and consume a lot of resources and perhaps
5 expose you to some security risks. So in that
6 case, you only do it when it's not possible to
7 simply update the metadata. You don't have any
8 other choice, because you're moving it to a
9 different file system, perhaps even across the
10 network or something. Your only choice really,
11 then, is to do a copy, and then erase the original.

Black Dep. Tr., 9:8-10; 9:21-10:11

PO Argues “Copying” Applies Only When Source and Destination are on Different Volumes

60. In his declaration, petitioner’s expert, Dr. Franz, further states Dr. Franz states only that “[a] POSITA would have found it obvious that ‘moving’ files in many circumstances (such as moving from one physical storage device to another) actually reduces to first copying the file to the new location and then deleting the original.” Ex. 1002 ¶ 96. As I have addressed above, there may be circumstances were a POSITA would implement moving files by copying them, including in the circumstances disclosed in the ’856 patent. But those are not the circumstances present in Burdett, where a POSITA would be motivated to move files without copying and would be discouraged from performing any copying, since doing so would only introduce unnecessary processing overhead.

PO’s Definition of “Copying” does not Align with Knowledge of POSITA

	Destination path is mapped to a different storage volume as the source	Destination Path is mapped to the same storage volume as the source
File-level “copy” operation	(1) The blocks of the file are duplicated to the destination medium (effort proportional to the size of the file, then a new directory entry is created to point to the newly allocated storage blocks Bits duplicated	(2) A new directory entry is created that points to the existing storage blocks of the original file Bits not duplicated
File-level “move” operation	(3) The blocks of the file are duplicated to the destination medium (effort proportional to the size of the file), then the original directory entry is modified to point to the newly allocated storage blocks Bits duplicated	(4) The original directory entry is modified and continues point to the existing storage blocks of the original file Bits not duplicated

PO's Definition of "Copying" does not Align with Knowledge of POSITA

"Copying" and "moving" data can both include updating a directory without duplicating bits. As noted by PO, a file can be "moved" within a filesystem by changing the file's location as indicated in a file system directory. (POR, 17; Franz Reb., ¶¶17-26.) But a file can also be "copied" by updating the file system directory in modern file systems that employ copy-on-write—a popular technique used in Windows Server since 2012. (Franz Reb., ¶20.) In file systems that provide copy-on-write semantics, bits of the copied file are not duplicated until one of the copies is modified, at which time differences between the copies are recorded in newly allocated disk blocks. (Franz Reb., ¶¶18-22.)

Motivation to Combine: Burdett + FortiSandbox

Based on a notification of a file event, such as a notification of an upload, download, or change to a file, the scanning service may request a copy of the file to be examined. Once the file is copied to the data store of the scanning service (along with meta-data to identify the customers' cloud account and cloud data store) the file may be added to the scan queue and process all required rules as part of the scan of the file. The scanning service may return a scan result (e.g., alert to a security manager) if triggering content is detected. This may be delivered to an administrator as configured in the security manager.

Burdett, 29:31-41

In processing block **506**, after the completion of the storage activity, the scanning service receives the file from the cloud storage service. The scanning service may copy the file from the cloud data store to another data store. The another data store may be a cloud data store. The another data store may be a local data store.

Burdett, 30:57-62

Motivation to Combine: Burdett + FortiSandbox

38. Dr. Black identifies several purported disadvantages to the combination of Burdett and FortiSandbox. I disagree with each of these.

Negative Repercussions of Burdett-FortiSandbox Combination cited by Dr. Black (Black Supp. Decl., ¶65)	Response
“Scanning service 304 cannot start processing a file until it arrives at the FortiSandbox device, injecting delay into the system.”	There is no reason why the file would need to entirely arrive at the FortiSandbox device. The device does not need to download an entire file, and it can begin scanning as soon as blocks of the file begin arriving.

Franz Reb., ¶ 38

Negative Repercussions of Burdett-FortiSandbox Combination cited by Dr. Black (Black Supp. Decl., ¶65)	Response
“The additional network traffic from transmitting files from cloud infrastructure 302 to the FortiSandbox device consumes bandwidth and may result in network congestion.”	Again, the FortiSandbox device does not necessarily need to download an entire file. For example, if the first block of the file is sufficient to determine that the file contains malware, then the rest of the file no longer needs to be considered because it won't change the overall classification of the file.

Franz Reb., ¶ 38

Motivation to Combine: Burdett + FortiSandbox

Negative Repercussions of Burdett-FortiSandbox Combination cited by Dr. Black (Black Supp. Decl., ¶65)	Response
“Transmitting files from cloud infrastructure 302 to the FortiSandbox devices results in unnecessary security risks, since there is always the possibility of a third party snooping traffic.”	If the network connection is encrypted, there is little risk of snooping. On the other hand, leaving the scan to be performed in the cloud can lead to security risks because an enterprise cannot be certain that the cloud scanner actually performs the expected functionality. A scanner under the
	operational control of the enterprise is much easier to supervise.

Franz Reb., ¶ 38

Negative Repercussions of Burdett-FortiSandbox Combination cited by Dr. Black (Black Supp. Decl., ¶65)	Response
“There are additional managerial complexities in configuring permissions on both the FortiSandbox device and cloud infrastructure 302 to permit scanning service 304 on the FortiSandbox device to access files in cloud infrastructure 302.”	Any managerial complexities that result from the combination are likely desirable, or at least outweighed by other benefits, because, as discussed above, there are advantages to the enterprise having control over the scan.

Franz Reb., ¶ 38

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true copy of the foregoing PETITIONER'S DEMONSTRATIVES FOR ORAL ARGUMENT was served in its entirety this 28th day of May, 2024 by electronic mail on the Patent Owner via its attorneys of record:

James M. Glass - jimglass@quinnemanuel.com
John T. McKee - johnmckee@quinnemanuel.com
Quincy Lu - quincylu@quinnemanuel.com
Andrew M. Holmes - drewholmes@quinnemanuel.com
Ognjen Zivojnovic - ogizivojnovic@quinnemanuel.com
Razmig H. Messerian - razmesserian@quinnemanuel.com
Sean Gloth - seangloth@quinnemanuel.com
Quinn Emanuel Urquhart & Sullivan LLP
51 Madison Ave, 22nd Floor
New York, New York 10010

Dated: May 28, 2024

Respectfully submitted,

Perkins Coie LLP
1201 Third Avenue Suite 4900
Seattle, WA 98101-3099

/Meghan Bright/

Meghan Bright
Patent Paralegal