

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,
Petitioner,

v.

FORTINET, INC.,
Patent Owner.

IPR2023-00456
Patent 11,036,856 B2

Before JAMES P. CALVE, THOMAS L. GIANNETTI, and
STEPHEN E. BELISLE, *Administrative Patent Judges*.

CALVE, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

Netskope, Inc. (“Petitioner”) filed a petition requesting *inter partes* review of claims 1–28 (the “challenged claims”) of U.S. Patent No. 11,036,856 B2 (“the ’856 patent”) (Ex. 1001). Paper 2 (“Pet.”), 1. Fortinet, Inc. (“Patent Owner”) timely filed a Preliminary Response. Paper 6. Applying the standard in 35 U.S.C. § 314(a), we instituted an *inter partes* review of all challenged claims on all grounds asserted in the Petition. Paper 10.

After we instituted trial, Patent Owner filed a Patent Owner Response. Paper 15 (“PO Resp.”). Petitioner filed a Reply to Patent Owner’s Response. Paper 18 (“Reply”). Patent Owner filed a Sur-reply to Petitioner’s Reply. Paper 24 (“Sur-reply”).

An oral hearing was held on May 31, 2024, and a copy of the transcript was entered in the record. Paper 27 (“Tr.”).

We have jurisdiction pursuant to 35 U.S.C. § 6. This decision is a Final Written Decision under 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73 as to the patentability of the claims on which we instituted trial. Petitioner bears the burden of proving unpatentability of the challenged claims. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). To prevail, Petitioner must prove unpatentability by a preponderance of the evidence. *See* 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d).

For the reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–28 of the ’856 patent are unpatentable.

A. Related Proceedings

The parties identify the following district court proceeding involving the '856 patent: *Netskope, Inc. v. Fortinet, Inc.*, No. 3:22-cv-01852-TLT (N.D. Cal.). Pet. 1; Paper 3 (Patent Owner's Mandatory Notices), 2.

B. Real Parties in Interest

Petitioner identifies Netskope, Inc. as the real party in interest. Pet. 1. Patent Owner identifies Fortinet, Inc. as the real party in interest. Paper 3, 2.

C. The '856 Patent

The '856 patent describes systems and methods for scanning and/or sandboxing files in cloud storage to protect users of an enterprise network from accessing malware-infected files. Ex. 1001, 1:20–23, 2:41–46.

A public cloud file store is natively mounted on a network security device with a first repository for storing an untrusted file until the network security device can apply security checks to it to determine whether the file is free of malicious content. Ex. 1001, 2:46–53. When the network security device determines that the file is clean, “the network security device makes the clean file accessible to the users by copying the clean file from the first repository to a second repository that is accessible to the users.” *Id.* at 2:53–57. The network security device copies only files that pass security checks to a sanitized storage area that is accessible to users. *Id.* at 3:27–36, 5:45–56. Network security devices provide security to private networks via network firewalling, antivirus intrusion protection, content filtering, data leak prevention, antispyware, and network access control. *Id.* at 5:4–15. Public cloud file stores can be provided by third-party cloud storage service providers such as Amazon Simple Storage Service (Amazon S3), Microsoft Azure, Google Cloud Platform, and IBM Cloud. *Id.* at 6:23–28.

Figure 1A of the '856 patent is reproduced below to illustrate this arrangement.

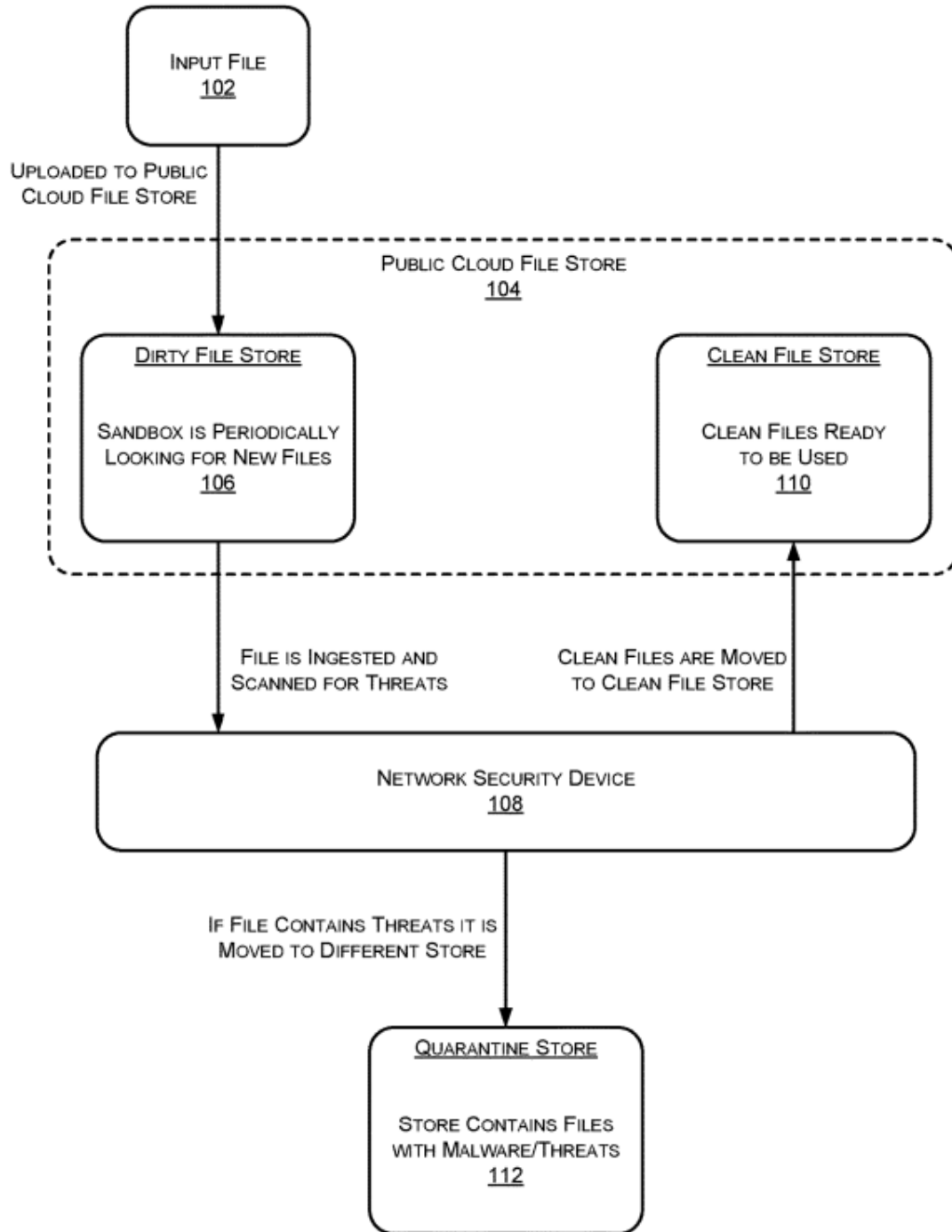


FIG. 1A

Figure 1A shows input file 102 loaded into dirty file store 106 that is natively mounted on network security device 108 to protect an enterprise network. Ex. 1001, 7:40–57. Figure 1A discloses that clean files are *moved* to clean file store 110. Input file 102 may be an email attachment, a file uploaded from an external web server, a website file, a file from another cloud service, or a file from enterprise network users. *Id.* at 7:59–8:5.

When input files 102 are stored in dirty file store 106, a notification service of public cloud file store 104 notifies network security device 108 via an Application Programming Interface (API) call from a notification service of the public cloud file store so that network security device 108 can perform security checks on the file to determine whether the new file is free of malicious content. Ex. 1001, 8:17–25, 6:46–55. Network security device 108 uses a sandbox/inspection engine to scan untrusted files uploaded into dirty file store 102, which is inaccessible to end users. *Id.* at 8:8–17.

If network security device 108 determines input file 102 is free of malware/malicious content, network security device 108 can “*transfer* file 102 from [a] first repository, i.e., dirty file store 106, to a second repository, e.g., clean file store 110, which is accessible to users.” Ex. 1001, 8:26–31 (emphasis added). “[N]etwork 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.” *Id.* at 8:53–57 (emphasis added). Network security device 108 can be a Unified Threat Management (UTM) appliance, sandbox appliance, firewall, content scanning engine, anti-virus engine, gateway device, and/or virtual machine (VM) controlled by a sandbox appliance. *Id.* at 8:31–36, 6:1–4. Figure 1A discloses that “Clean Files are *Moved* to Clean File Store” (emphasis added).

Clean file store 110 contains only clean files that are available to users of the enterprise network based on sharing rights granted to them. Ex. 1001, 8:58–60. Network security device 108 can remove malware that is detected from the untrusted file so the transfer to the clean file store 110 is made after freeing the file from malicious content. *Id.* at 9:7–12. Files associated with malicious content can be quarantined by storing files in quarantine store 112 that cannot be accessed by users, or files associated with malicious content can be deleted. *Id.* at 9:12–16. In another embodiment, clean file store 110 may be part of network security device 108 or part of external storage of an enterprise network, rather than a part of public cloud store 104 depicted in Figure 1A so users can access clean file store 110 seamlessly. *Id.* at 9:17–23, Fig. 1B (“Clean Files are Moved to Clean File Store”).

Figure 2 of the ’856 patent is reproduced below to illustrate secure data transfer system 200 comprising untrusted file processing module 202 and clean file transfer module 204. Ex. 1001, 9:28–35.

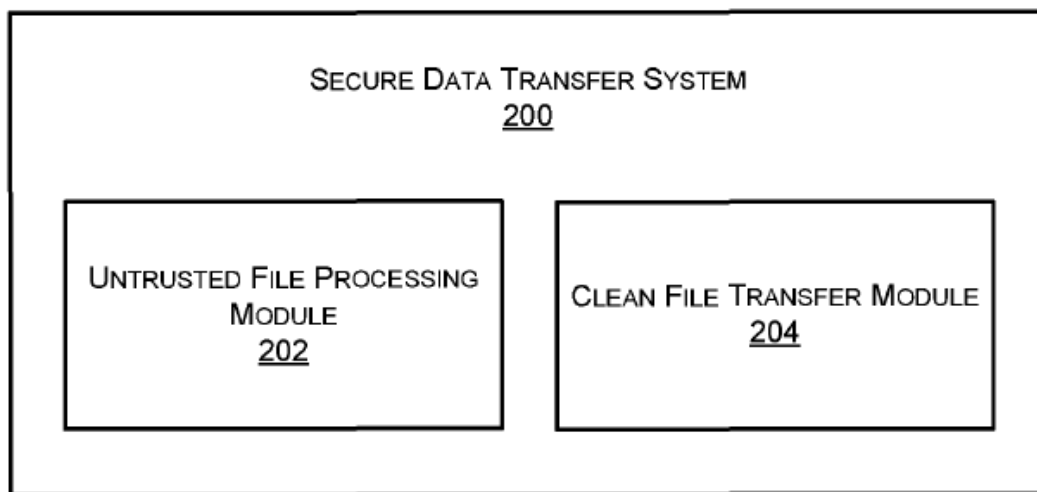


FIG. 2

Figure 2 depicts secure data transfer system 200 where untrusted file processing module 202 can access an untrusted file in a first repository in a public cloud file store natively mounted on a network security device that implements secure data transfer system 200. Ex. 1001, 9:35–41. When a new file is stored in the first repository, a notification is sent to untrusted file processing module 202 via an API call of the public cloud file store to alert untrusted file processing module 202 of the existence of an untrusted file so module 202 can apply security checks to the untrusted file. *Id.* at 9:54–63. Security checks may include (1) content scanning using any combination of file signature, file hash, file path, file attributes, file source, file pre-scan parameters, file extension, file content, and file name and/or (2) behavioral-based malware detection. *Id.* at 9:63–10:3. Untrusted file processing module 202 can remove any malware that is detected from the untrusted file and quarantine or delete the untrusted file when the results of the determination indicate the presence of malicious content. *Id.* at 10:4–16.

Clean file transfer module 204 makes a clean file accessible to users by “*copying or transferring* the clean file from a first repository (e.g., dirty file store 104) that is inaccessible to end users to a second repository (e.g., clean file store 110) that is accessible to end users” when it is determined to be clean. Ex. 1001, 10:17–23 (emphasis added). Clean files are files found or made free of malware or undesired attributes/behavior. *Id.* at 10:24–27. Clean file transfer module 204 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.” *Id.* at 10:28–33 (emphases added); *id.* at 6:5–10.

D. Challenged Claims

Petitioner challenges claims 1–28 of the '856 patent. Pet. 1. Claims 1, 13, and 21 are independent. Claims 2–12 depend from claim 1. Claims 14–20 depend from claim 13. Claims 22–28 depend from claim 21.

Claim 1 is representative and is reproduced below with Petitioner's annotations of the limitations.

1[pre] 1. A secure data transfer system comprising:
1[a] 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
1[b] one or more processors coupled to the non-transitory storage device and operable to execute the one or more routines, *1[c][i]* 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, *1[c][ii]* wherein the public cloud file store is natively mounted on a network security device that is protecting the enterprise network and *1[c][iii]* wherein the users do not have read access to the first repository of the public cloud file store; and
1[d] 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
1[e] 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.

E. Asserted Grounds of Unpatentability

Petitioner asserts that the challenged claims are unpatentable on the following three grounds (Pet. 3):

Ground	Challenged Claims	35 U.S.C. §	References
1	1–7, 9–18, 20–26, 28	103 ¹	Burdett ² , FortiSandbox ³
2	1, 2, 4, 5, 7–10, 12–14, 16, 18–22, 24, 26–28	103	Sharpe ⁴ , Seese ⁵ , Kamalapuram ⁶
3	3, 6, 11, 15, 17, 23, 25	103	Sharpe, Seese, Kamalapuram, Dods ⁷

Petitioner also relies on Declarations of Dr. Michael Franz. Ex. 1002; Ex. 1013. Patent Owner relies on a Declaration of Dr. John Black Jr. Ex. 2004.

¹ The Leahy-Smith America Invents Act (“AIA”) revised 35 U.S.C. § 103 effective March 16, 2013. Changes made to 35 U.S.C. § 103 in the AIA do not apply to any application for patent filed before March 16, 2013. Because the ’856 patent has an effective filing date after March 16, 2013, we refer to the AIA version of § 103.

² US 11,281,775 B2, issued Mar. 22, 2022 (Ex. 1004, “Burdett”).

³ FortiSandbox – Administration Guide, Version 2.3.2, dated Nov. 9, 2016 (Ex. 1005, “FortiSandbox”). See Ex. 1002 ¶ 66 for an online address.

⁴ US 9,811,662 B2, issued Nov. 7, 2017 (Ex. 1006, “Sharpe”).

⁵ US 2015/0100357 A1, published Apr. 9, 2015 (Ex. 1007, “Seese”).

⁶ US 2020/0050686 A1, published Feb. 13, 2020 (Ex. 1008, “Kamalapuram”).

⁷ US 10,382,468 B2, issued Aug. 13, 2019 (Ex. 1009, “Dods”).

II. DISCUSSION

A. Level of Ordinary Skill in the Art

Petitioner asserts that a skilled artisan “would have had at least a B.S. in computer science, computer engineering, or electrical engineering (or equivalent experience) and at least two years’ practical experience with computer networking and computer security.” Pet. 15. Patent Owner asserts a skilled artisan “would have had a Bachelor of Science degree in electrical engineering and/or computer science, and two years of work or research experience in the fields of network and data security, or a Master’s degree in electrical engineering and/or computer science and one year of work or research experience in related fields.” PO Resp. 14–15. Patent Owner asserts that its proposal is almost the same as Petitioner’s, and its positions would be the same under either party’s proposal. *See id.* at 15. The two formulations differ mainly in the levels of experience. We adopt Patent Owner’s proposal as more consistent with the ’856 patent and the prior art. Our decision and analysis would be the same under either party’s proposal.

B. Claim Construction

We interpret the claims “using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b).” 37 C.F.R. § 42.100(b). Under that standard, words of a claim are generally given their ordinary and customary meaning as understood by a person of ordinary skill in the art at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc). We construe the claims only to the extent necessary to reach our decision. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

The parties assert that claim terms should receive their plain and ordinary meaning and that no claim terms require construction. Pet. 16; PO Resp. 15. Having considered the record, we determine that no express claim construction of any claim term is necessary to reach our decision.

C. Principles of Law

A patent claim is unpatentable “if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains.” 35 U.S.C. § 103. “The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007). “[I]f a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.” *Id.* at 417.

The question of obviousness is resolved based on underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) when in evidence, objective evidence of non-obviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Neither party has presented any objective evidence of non-obviousness.

A party also must show that a skilled artisan would have a reasonable expectation of success in combining the teachings of prior art references to achieve the claimed invention. *Arctic Cat Inc. v. Bombardier Recreational Prods. Inc.*, 876 F.3d 1350, 1360–61 (Fed. Cir. 2017).

D. Ground 1: Obviousness Over Burdett and FortiSandbox

Petitioner asserts claims 1–7, 9–18, 20–26, and 28 are unpatentable under 35 U.S.C. § 103 over the combination of Burdett and FortiSandbox. Pet. 16–50.

1. Burdett

Burdett discloses an agentless scanner for cloud storage services, such as Amazon Web Service (AWS) S3, to protect files against malware and other exploits, as shown in Figure 3 reproduced below. Ex. 1004, 1:42–2:4.

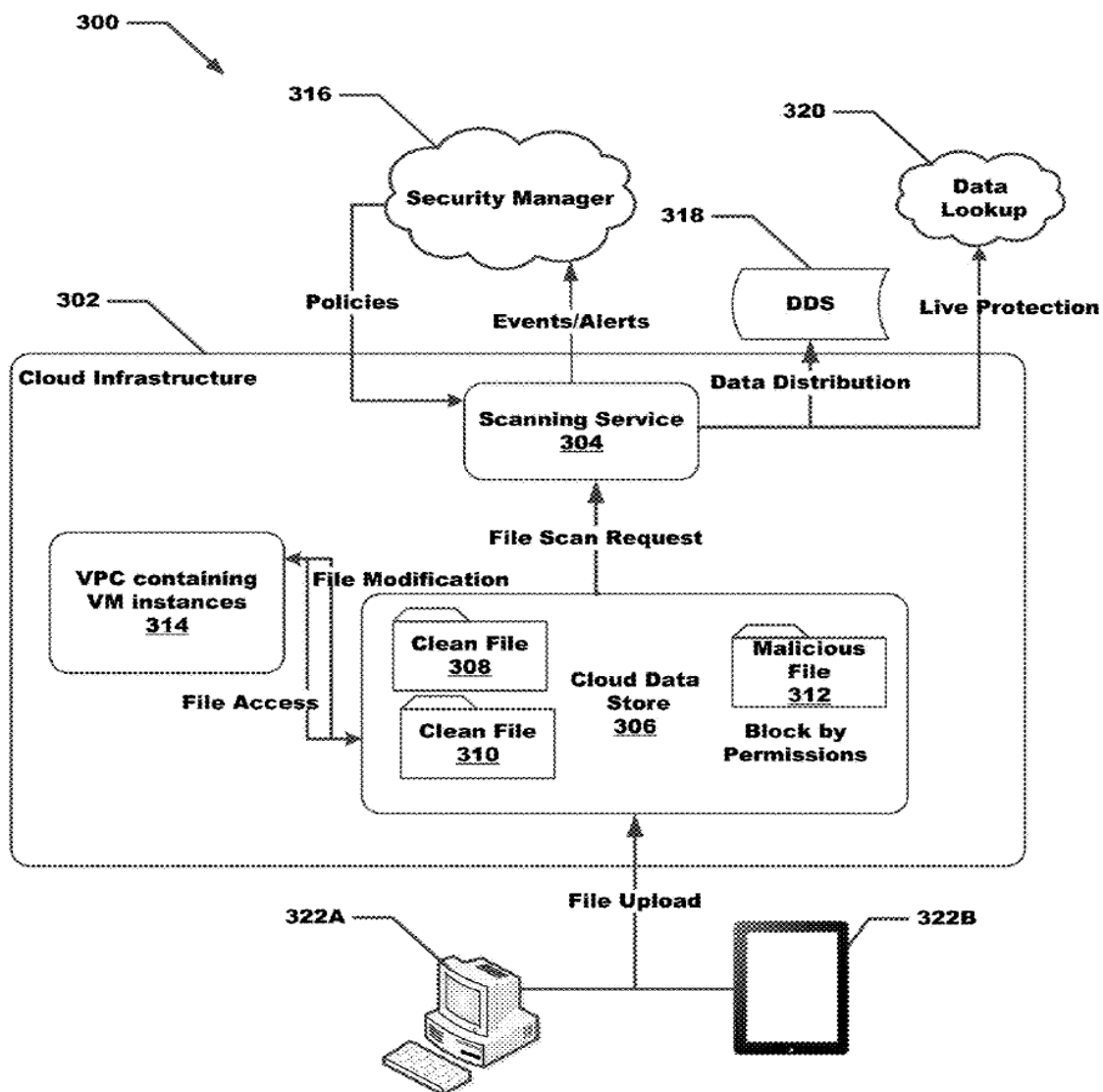


Figure 3 depicts system 300 that includes cloud infrastructure 302 with scanning service 304 and virtual machines running on virtual private clouds 314. Ex. 1004, 23:33–36. Cloud infrastructure 302 may be provided by AWS and AWS S3 buckets or other “cloud infrastructure services available from Microsoft Azure, CenturyLink Cloud, VMware, Rackspace, Joyent, and Google.” *Id.* at 23:43–56. Security manager 316 provides an interface to configure scanning service 304. *Id.* at 24:32–38.

Scanning service 304 is implemented in cloud infrastructure 302 to access cloud data store 306 (Ex. 1004, 23:33–24:10, 27:20–28:22) and is managed and configured by security manager 316 that accesses files to be scanned and controls file permissions (*id.* at 24:39–25:46). Applications may access clean files 308, 310 that lack malware but not access malicious file 312 that contains malware or malicious content. *Id.* at 26:49–51.

Scanning service 304 may be implemented as scanning applications on virtual machines in cloud infrastructure 302 and receive policies from security manager 316 and data updates from Data Distribution Service 318 such as code updates and malicious file definitions. Ex. 1004, 24:32–56. Scanning service 304 accesses files directly from cloud data store 306 and moves files or changes file names to control access. *Id.* at 25:18–28. The scanning service may replace a file with another file that is “clean.” *Id.* at 25:31–33. Scanning service 304 changes file permissions in cloud data store 306 to permit or deny access to files and provide data security with minimal installation and cost. *Id.* at 25:34–46. Scanning service 304 *registers with cloud infrastructure 302 to access files and receive notifications* by setting a role ID, key/password, authentication data, account details, resource rights, secure key store, API credentials, and privileges. *Id.* at 27:24–28:51.

2. *FortiSandbox Administration Guide*

FortiSandbox Administration Guide version 2.3.2 (“FortiSandbox”) discloses a device configured to sniff traffic from the network, scan files on a network share on a pre-defined schedule, quarantine malicious files, and receive files from FortiGate FortiWeb, FortiMail, and FortiClient. Ex. 1005, 8, 113. We reproduce instructions to natively mount a network share to a FortiSandbox device to scan files on the network share. *Id.* at 113–115.

To create a new network share:

1. Go to *Scan Input > Network Share*.
2. Click the + *Create New* button from the toolbar.
3. Configure the following options:

Enabled	Select to enable network share configuration. If network share is not enabled, its scheduled scan will not run.
Network Share Name	Enter the network share name.
Mount Type	Select the mount type from the drop-down list. The following options are available: • CIFS • NFSv2 • NFSv3 • NFSv4

The instructions describe how to create and mount a new network share to a FortiSandbox device by selecting a new network share name and selecting a mount type from a drop-down list. Ex. 1005, 114–115. Mount types used to mount the network share on a FortiSandbox network security device include CIFS, network file system version 2 (NFSv2), NFSv3, and NFSv4, which are native file systems protocols that enable the FortiSandbox system to communicate with the new network share in the file system’s native language. *Id.* at 115; *see* Pet. 18, 29.

3. *Motivation to combine*

a. *Petitioner's contentions*

Petitioner asserts that a skilled artisan would have been motivated to natively mount Burdett's public cloud file store on a FortiSandbox network security device to perform malware scanning because "[c]onfiguring 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." Pet. 19 (citing Ex. 1002 ¶¶ 69, 70). Petitioner asserts that Burdett's scanning service scans an enterprise's cloud file store for malware, and FortiSandbox deploys a FortiSandbox system in an enterprise network to scan a cloud file store so "an enterprise [can] preserve the privacy of its files in cloud storage while preventing enterprise users from accessing malicious files." *Id.*

Petitioner asserts that natively mounting Burdett's public cloud file store on a FortiSandbox network security device would improve Burdett's system and protect an enterprise network by (1) enabling Burdett's scanning service to access files in the cloud file store and natively communicate with the cloud file store to control access to the files by using the functionality of native cloud APIs such as a callback, (2) scanning files on the network share and optionally quarantining any malicious files, (3) scanning cloud files as bulk, scheduled, or on-demand scans, and using advanced security scans to improve scan throughput, (4) reacting quickly to changes in a cloud file store such as new file uploads or changes to files, (5) allowing the enterprise to control its scans instead of using a cloud provider's scanning services with different types of scans, scan times, and security, and (6) increasing privacy and controllability. Pet. 29–30; Ex. 1002 ¶¶ 88, 89; Ex. 1013 ¶ 37.

b. Patent Owner's arguments

Patent Owner argues that moving Burdett's scanning service 304 from cloud infrastructure 302 to the FortiSandbox device would be detrimental to Burdett's system because every file would have to be transmitted from cloud infrastructure 302 over a wide area network to the FortiSandbox device for scanning and this would cause delays due to the time used for file transfer, cause network congestion due to additional file transfers, pose security risks by transferring files over a wide area network, and require FortiSandbox to have access to files in cloud data store 306. PO Resp. 28–29 (citing Ex. 2004 ¶ 65). Patent Owner argues that there is no reason to move Burdett's scanning service 304 to the FortiSandbox device because it already controls access to files in the cloud file store, Burdett's security manager identifies new files to be scanned and provides notice via an API, and Dr. Franz did not allege that performing bulk scans on a remote FortiSandbox device provides any advantage over Burdett's "security manager" performing scans in the cloud infrastructure. PO Resp. 29–30 (citing Ex. 2004 ¶ 64).

c. Analysis

We determine that natively mounting Burdett's cloud data store 306 on a FortiSandbox device to implement Burdett's malware scanning services would improve network security. It would preserve the privacy of files in cloud file stores and protect the enterprise network from malware by using a FortiSandbox network security device at an enterprise network (rather than in a public cloud store) to scan files for malware. Files would be scanned on schedules and criteria optimized to the security of the enterprise rather than schedules or criteria of a third-party cloud-based service provider and doing bulk scans not taught in Burdett. Pet. 30; Ex. 1013 ¶ 37; Ex. 1002 ¶ 88.

We agree with Dr. Franz’s testimony that performing scans on a device located in an enterprise network would enhance controllability and privacy by allowing an enterprise to perform bulk scans on schedule or on demand and more advanced scans that a cloud service provide cannot do. Ex. 1013 ¶ 37; Tr. 21:20–23:22. An enterprise could scan files according to scanning schedules and criteria that most effectively improve its network security rather than using a cloud storage provider’s criteria and schedules. Indeed, Patent Owner asserts that scanning files in cloud storage on virtual machines is inefficient. PO Resp. 6 (citing Ex. 1001, 1:67–2:3); *see KSR*, 550 U.S. at 416 (“The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.”); *see DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F.3d 1356, 1368 (Fed. Cir. 2006) (an implicit motivation to combine exists when an “improvement” makes a product more efficient).

Burdett teaches that its scanning service 304 may be managed by security manager 316 implemented *outside* cloud infrastructure service 302. Ex. 1004, 24:1–3, 24:32–41. Burdett’s scanning service may copy files from the cloud data store to a local data store. *Id.* at 30:57–62; Reply 22. Burdett uses *local data storage* to perform security scans. Ex. 2004 ¶ 65.

We find that natively mounting a cloud data store on a FortiSandbox device for scanning files would give an enterprise greater control over the scanning of enterprise files for malware while storing the files in cloud data store 306. Ex. 1013 ¶ 37; Ex. 1002 ¶¶ 70, 88, 89. We agree with testimony of Dr. Franz that an enterprise scanner is easier to supervise, and it ensures that scans are performed and completed properly, and the encrypted network connections protect transmitted files. Ex. 1013 ¶ 38; *see* Tr. 23:23–24:10.

We determine that a skilled artisan weighing potential advantages and disadvantages would natively mount cloud data to a FortiSandbox device to increase control over scanning, meet security needs, improve efficiency, and preserve the privacy of cloud storage files. We are persuaded by Dr. Franz’s testimony that scanning files outside cloud infrastructure 302 would improve the enterprise’s control of scanning to use its own security scanning criteria on its own schedules to improve efficiencies and control the types of scans that are available, and when and how they are done. Ex. 1013 ¶¶ 37, 38; Ex. 1002 ¶¶ 88, 89; Tr. 21:20–24:10. Moreover, Sharpe, cited in Ground 2, teaches the knowledge in the art to place a network security device in close network proximity to cloud storage with a high bandwidth link to minimize latency. Ex. 1006, 98:26–32; Ex. 1013 ¶¶ 4, 37; Tr. 53:1–10. The combination does not have to provide an optimal result in every respect.⁸

d. Conclusion

We determine Petitioner has shown, by a preponderance of evidence, that a skilled artisan would have combined the teachings of Burdett and FortiSandbox as asserted with a reasonable expectation of success.

⁸ The Federal Circuit has recognized that an obviousness showing “does not require that a particular combination must be the preferred, or the most desirable, combination described in the prior art in order to provide motivation for the current invention.” *Novartis Pharms. Corp. v. West-Ward Pharms. Int’l Ltd.*, 923 F.3d 1051, 1059 (Fed. Cir. 2019) (quoting *In re Fulton*, 391 F.3d 1195, 1200 (Fed. Cir. 2004)). Here, Petitioner is required to show only that “‘there is something in the prior art as a whole to suggest the *desirability* . . . of making the combination,’ not whether there is something in the prior art as a whole to suggest that the combination is the *most desirable* combination available.” *Fulton*, 391 F.3d at 1200 (quoting *In re Beattie*, 974 F.2d 1309, 1311 (Fed. Cir. 1992)).

4. *Claim 1*

a. *1[pre]: A secure data transfer system comprising:*

(1) *Petitioner's contentions*

Petitioner asserts that Burdett discloses a secure data transfer system that scans files in cloud data store 306 using a scanning service. Pet. 20–21 (citing Ex. 1004, 1:42–53, 23:33–38, 24:19–25, 24:33–36, 25:18–19, 25:26–28, 25:56–67, 29:42–43, 31:8–14, Abstr., Fig. 3; Ex. 1002 ¶¶ 71–73).

(2) *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions regarding element 1[pre]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the record before us, we find Petitioner's reasoning and evidence persuasive that Burdett discloses a secure data system in Figure 3 as recited in element 1[pre], by a preponderance of the evidence.

b. *1[a]: 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*

(1) *Petitioner's contentions*

Petitioner contends that Burdett discloses a computer readable storage medium with routines operable to perform a scanning service that controls access by users to files in cloud data stores and prevent users from accessing malware-infected files. Pet. 22–25 (citing Ex. 1004, 2:14–16, 2:19–64, 5:29–31, 7:14–16, 9:29, 11:57–66, 14:18–24, 23:43–56, 24:22–25, 24:28–36, 25:26–28, 25:42–46, 25:55–67, 26:6–28, 26:44–58, 28:1–5, 29:31–36, 29:58–61, 32:10–67, 34:1–50, Fig. 3; Ex. 1002 ¶¶ 74–80).

(2) *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions regarding element 1[a]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Burdett discloses or suggests element 1[a].

- c. *1[b]: one or more processors coupled to the non-transitory storage device and operable to execute the one or more routines*

(1) *Petitioner's contentions*

Petitioner contends that Burdett discloses a processor that executes instructions on a computer-readable storage medium to perform routines. Pet. 25 (citing Ex. 1004, 2:22–53, 26:59–67, 32:10–15; Ex. 1002 ¶ 81).

(2) *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions regarding element 1[b]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Burdett discloses element 1[b].

- d. *1[c][i]: wherein 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*

(1) *Petitioner's contentions*

Petitioner asserts that Burdett has an untrusted file processing module and service to scan untrusted files in a cloud data store. Pet. 25–28 (citing Ex. 1004, 25:18–19, 25:56–61, 26:37–41, 26:59–67, 28:1–5, 28:10–13, 31:4–14, 31:24–34, 32:10–15, Fig. 3; Ex. 1001, 8:8–17; Ex. 1002 ¶¶ 82–84).

(2) *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions regarding element 1[c][i]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Burdett discloses or suggests element 1[c][i].

e. 1[c][ii]: wherein the public cloud file store is natively mounted on a network security device that is protecting the enterprise network

(1) *Petitioner's contentions*

Petitioner asserts that a FortiSandbox device mounts network shares by using CIFS and NFS mount types so that the FortiSandbox device can communicate with the file system in a native language to scan files on the network shares. Pet. 28–29 (citing Ex. 1005, 8, 10, 114–115; Ex. 1001, 11:7–10; Ex. 1002 ¶¶ 85–87). Petitioner contends that the '856 patent also describes mounting a data store to a network security device using NFS and copying clean files using CIFS. *Id.* at 29 (citing Ex. 1001, 11:7–10).

(2) *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions regarding element 1[c][ii]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that FortiSandbox discloses or suggests element 1[c][ii].

f. 1[c][iii]: wherein the users do not have read access to the first repository of the public cloud file store

(1) *Petitioner's contentions*

Petitioner contends that Burdett stores files in a cloud data store with default file permissions that prevent access by applications until the file is scanned and deemed clean as discussed for element [c][i] or stored in a repository that is inaccessible to applications. Pet. 31 (citing Ex. 1004, 24:22–25, 25:26–28, 25:57–64, 26:14–28, 26:44–58; Ex. 1002 ¶¶ 90, 91).

(2) *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions regarding element 1[c][iii]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Burdett discloses or suggests element 1[c][iii].

g. 1[d]: wherein the one or more routines include: an untrusted file processing module, which when executed by the one or more processors: . . . 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

(1) *Petitioner's contentions*

Petitioner contends that Burdett applies security checks to untrusted files and restricts or permits access to the files based on the scan results. Pet. 31–32 (citing Ex. 1004, 1:64–66, 8:1–12, 24:51–56, 25:12–13, 25:59–67, 29:42–52, 29:58–61, 31:4–14, 31:24–24; Ex. 1002 ¶¶ 92, 93).

(2) *Patent Owner arguments*

Patent Owner does not contest Petitioner's assertions regarding element 1[d]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Burdett discloses or suggests element 1[d].

h. 1[e]: 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.

(1) *Petitioner's contentions*

Petitioner asserts that Burdett made files accessible by changing file permissions or storage locations or moving files. Pet. 33 (citing Ex. 1004, 25:26–27, 25:64–67). Petitioner asserts it would have been obvious to use repository-level permissions to control access to files and to copy a clean file to a clean repository in a separate location that is accessible to users. *Id.* at 33–35 (citing Ex. 1004, 26:59–67, 31:4–14, 31:24–34, 32:10–15, Fig. 3; Ex. 1002 ¶¶ 94–97). Dr. Franz testifies that a skilled artisan would have found it obvious that “moving” files from one storage device to another reduces to copying the file to the new location and deleting the original. Ex. 1002 ¶ 96.

(2) *Patent Owner's arguments*

Patent Owner argues that the claims require “**copying** the clean file from the first repository to a second repository,” and Petitioner’s expert testifies that “***Burdett teaches moving not copying.***” PO Resp. 15–16. Patent Owner asserts that “copying” creates at least temporarily a second copy of information but “moving” changes the location of the information. *Id.* at 17 (citing Ex. 2004 ¶ 48). Patent Owner asserts that the ’856 patent does not use “moving,” “copying,” and “transferring” interchangeably. *Id.* at 18. Patent Owner argues that the prior art only describes moving files without copying. *Id.* at 20.

(3) *Analysis*

(a) *Moving and copying are equated*

The ’856 patent uses the terms moving and copying interchangeably in some contexts. Ex. 1001, 8:26–9:41, 10:17–40. Figures 1A and 1B state, “Clean Files are Moved to Clean File Store,” but the ’856 patent describes this moving as being performed by copying, transferring, and/or sharing of clean files. Ex. 1001, 7:37–9:27.

Dr. Black testifies that only Figure 1B copies files because the ’856 patent includes Figure 1B, where the “clean file store” is not part of the same “public cloud file store” as the original “dirty file store.” . . . Thus, Figure 1B shows an instance where files are physically moved from a first storage device to a different second storage device. In this context, “moving” files without “copying” would be contrived and a *POSITA* would instead implement such a move by “copying” files.

Ex. 2004 ¶ 58. His testimony is contrary to the ’856 patent’s description to move files by copying in annotated Figures 1A and 1B, reproduced below.

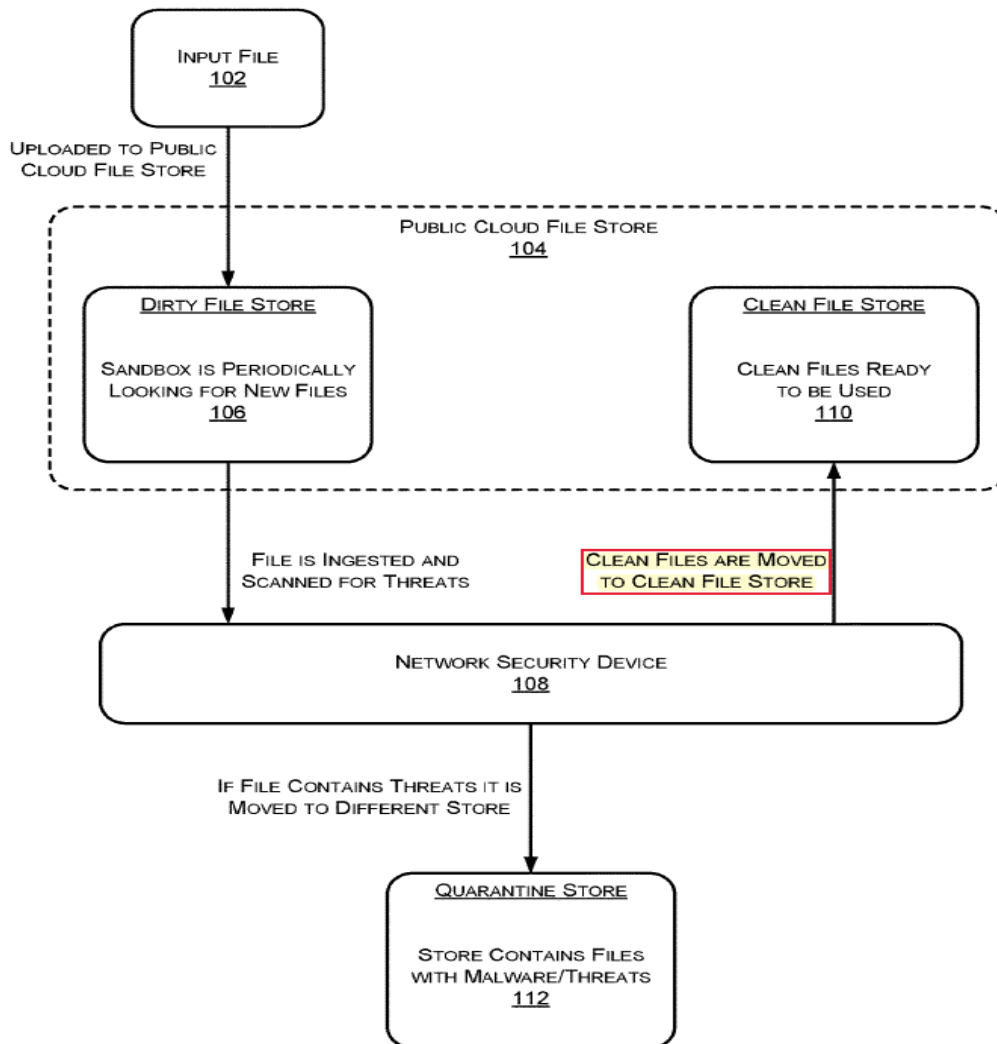


FIG. 1A

Figure 1A shows Dirty File Store 106 and Clean File Store 110 in Public Cloud File Store 104 and “Clean Files are Moved to Clean File Store” as annotated. The ’856 patent indicates that clean files are *moved* to clean file stores by *copying*, *transferring*, and *sharing* files. Ex. 1001, 7:37–9:7. We are not persuaded by Dr. Black’s testimony that Figure 1B shows a different type of moving because it discloses the same operation as Figure 1A, i.e., “Clean Files are Moved to Clean File Store,” which is described as copying, transferring, and sharing files as in annotated Figure 1B reproduced below.

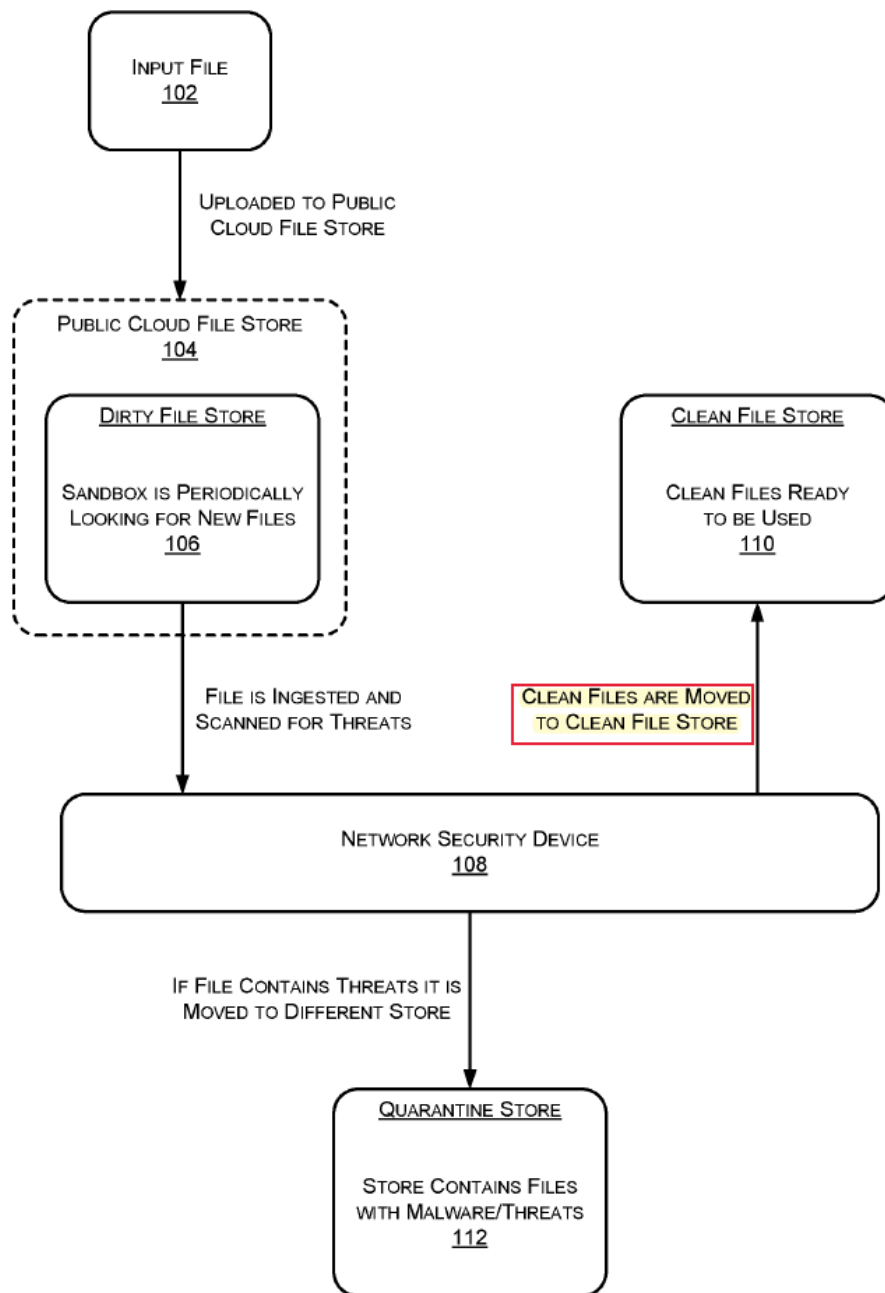


FIG. 1B

Annotated Figure 1B shows Dirty File Store 106 and Clean File Store 110 in different file stores, but “Clean Files are Moved to Clean File Store” as in Figure 1A. Ex. 1001, 9:16–27. Clean files are moved in Figures 1A and 1B. Moving can be done by copying or transferring files. *Id.*; *id.* at 8:53–9:6.

Whether dirty file store 106 and clean file store 110 are in the same public cloud file store 104 (Figure 1A) or different file stores (Figure 1B), clean files are moved by copying or transferring them. Ex. 1001, 7:37–9:41, 10:17–40; *id.* at 8:26–31 (clean files are transferred), 8:53–57 (clean files are copied and/or transferred), 8:67–9:11 (clean files are copied/transferred), 10:28–33 (clean file copied by sharing); *id.* at 9:35–41 (clean file is copied); 10:17–27 (copying or transferring clean file), 11:26–30 (transfer clean file).

(b) *Concepts overlap in the art*

Neither party proposed or sought a construction of “copying” or “moving.” The parties agree that moving files can be done by copying files as the ’856 patent itself discloses in Figures 1A and 1B as discussed above. Reply 12; PO Resp. 17; Ex. 2004 ¶ 60.⁹ Because claim 1 does not require a file to be retained in the untrusted file store, “copying the clean file” can be done by “moving.” The FortiSandbox Administrative Guide states “[w]hen a file is moved, to leave a copy in its original location . . . select the *Keep Original File At Current Location*.” Ex. 2003, 76. Users also can copy files without retaining a copy. *Id.* at 99 (“then files of the same path will only have one copy saved in the sanitized location”). Moving and copying a file involve essentially the same operation. Ex. 1013 ¶¶ 15, 16.

⁹ Their contentions are consistent with extrinsic evidence that both “moving” and “copying” files transfer files to another location so the difference between moving and copying files is whether the original file is deleted or retained. *Microsoft Computer Dictionary, Fifth Edition* 130 (Microsoft Press 2002) (Ex. 3001) (defining copying as duplicating information to another part of a document, file or memory location); *id.* at 349 (describing moving as also transferring data from one location to another); Tr. 18:1–19:20 (moving a file copies the bits and the original bits remain until you overwrite them).

(c) *Burdett renders copying obvious*

We agree with Petitioner that Burdett’s moving of files between file stores teaches or suggests to copy a clean file from a first repository to a second repository as claimed. Pet. 33–35; Reply 15–18. Burdett’s scanning service can (1) “move files,” (2) “change the name of files,” or (3) change a file’s location as a path in a file system to control access to files. Ex. 1004, 25:24–31. The scanning service may *replace* a file with a clean file, i.e., copy a file. *Id.* at 25:31–33. We agree with Dr. Franz that moving files requires files to be copied to another location to allow efficient processing by repository-level permissions. Ex. 1002 ¶¶ 94, 95; Tr. 20:1–21:6.

A skilled artisan would understand “move files” physically copies the files from one location to another. Pet. 33; Reply 12–15; Ex. 1002 ¶ 96; Tr. 18:1–20:14. Malicious files also can be moved. Ex. 1004, 26:55–58.

Burdett’s scanning service can “*move files* [or] change file names, etc. in order to control access.” Ex. 1004, 27:24–29 (emphasis added). To scan files, scanning service 304 may *copy a file* to a data store of the scanning service. Ex. 1004, 29:31–36. “The scanning service may copy the file from the cloud data store to another data store [that] may be a cloud data store [or] a local data store.” *Id.* at 30:57–62. It may *replace* a file with another file that is “clean.” *Id.* at 25:31–33. Access to files is prevented by *moving* files or by changing file names or permissions. *Id.* at 31:4–7, 25:24–33, 27:24–30, 26:55–58. Burdett thus teaches or suggests to move files by copying.

(4) *Conclusion*

Based on the parties’ contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Burdett discloses or suggests element 1[e].

i. Conclusion

Based on the current record, evidence, and contentions, we determine that Petitioner has established, by a preponderance of evidence, that claim 1 is unpatentable over the combination of Burdett and FortiSandbox.

5. Independent Claims 13 and 21

a. Petitioner's contentions

Petitioner provides detailed contentions that Burdett and FortiSandbox disclose or suggest every element of claim 13. Pet. 35–37 (citing Ex. 1004, 26:59–61, 28:42–43, 29:31–52, 29:58–61, 30:43–49, 30:54–56; Figs. 4A, 4B, 5A, 5B; Ex. 1002 ¶¶ 98–100 and contentions for similar subject matter in elements 1[c][i], 1[c][ii], 1[c][iii], 1[d], and 1[e]). Petitioner provides similar contentions for claim 21. *Id.* at 37–38 (citing Ex. 1004, 2:22–40, 28:33–31:53, 34:1–50; Ex. 1002 ¶ 105 and contentions for similar subject matter in elements 13[a][i], 1[c][ii], 1[c][iii], 1[d], and 1[e]).

b. Patent Owner's arguments

Patent Owner does not present separate arguments for claims 13 and 21 apart from what Patent Owner presented for claim 1. *See* PO Resp. 15–30; Sur-reply 9–22.

c. Analysis

We disagree with Patent Owner's arguments for the reasons discussed above for claim 1 where we address those arguments in detail.

d. Conclusion

Based on the current record, evidence, and contentions, we determine that Petitioner has established, by a preponderance of evidence, that claims 13 and 21 are unpatentable over the combination of Burdett and FortiSandbox.

6. *Dependent Claims 2–7, 9–12, 14–18, 20, 22–26, and 28*
a. *Petitioner’s contentions*

Petitioner asserts that FortiSandbox discloses a sandbox device, and Burdett teaches or suggests an intrusion detection system that provides host intrusion prevention through behavioral based protection against malicious malware code as recited in claims 2, 3, 14, 15, 22, and 23. Pet. 38–40 (citing Ex. 1004, 8:1–12; Ex. 1005, 8, 10; Ex. 1002 ¶¶ 111, 113).

Petitioner contends that Burdett and FortiSandbox disclose a network security device that is a virtual machine controlled by a sandbox appliance to determine whether an untrusted file is a clean file free of malicious content in claim 4. Pet. 40 (citing Ex. 1004, 1:64–66, 24:33–36, 24:51–56, 29:58–60, 31:4–14, 31:24–34; Ex. 1005, 8, 88; Ex. 1002 ¶¶ 114–116).

Petitioner contends that FortiSandbox mounts a network share folder to the FortiSandbox system by means of CIFS, NFSv2, NFSv3, and NFSv4, and it would have been obvious to copy the file to the second repository in Burdett using CIFS and/or NFS as recited in claims 5, 16, and 24. Pet. 41–42 (citing Ex. 1005, 83, 115; contentions for element 1[e]; Ex. 1002 ¶ 117).

Petitioner contends that Burdett discloses an untrusted file processing module that removes malware from the untrusted file that is detected by the security checks when the result of the determining is negative in claims 6, 17, and 25. Pet. 42. (citing Ex. 1004, 25:31–33; Ex. 1010; Ex. 1002 ¶ 118).

Petitioner asserts that Burdett and FortiSandbox teach or suggest that the untrusted file processing module quarantines or deletes the untrusted file when the result of the determination is negative as recited in claims 7, 18, and 26. Pet. 42–43 (citing Ex. 1004, 1:64–2:3, 7:23–26, 25:26–33, 26:44–58, 29:38–52, 31:39–44; Ex. 1005, 8, 76; Ex. 1002 ¶¶ 119–120).

Petitioner contends that forming a second repository in the public cloud file store as recited in claims 9, 20, and 28 would have been obvious in view of Burdett's disclosure of changing the storage location of a file to control access to it. Pet. 43–44 (citing Ex. 1004, 25:64–67, 27:24–29, 27:38–40, 28:13–21; Ex. 1002 ¶¶ 121, 122).

Petitioner contends that Burdett describes the public cloud file store is provided by a third-party cloud storage service provider as recited in claim 10, such as cloud data stores provided by Amazon Simple Storage Services (S3). Pet. 44 (citing Ex. 1004, 24:28–30, 28:3, 30:33–34; Ex. 1002 ¶ 123).

Petitioner asserts that Burdett discloses malware detection systems that determine whether an untrusted file is a clean file free of malicious content based on a file signature, file source, file extension, and file content, as recited in claim 11. Pet. 44–45 (citing Ex. 1004, 1:21–22, 8:13–17, 24:59–64, 31:26–30; Ex. 1002 ¶ 124).

Petitioner asserts that Burdett and FortiSandbox disclose or suggest the steps recited in claim 12. Pet. 45–50 (citing Ex. 1004, 1:64–66, 25:4–16, 24:51–56, 25:3–17, 25:25–28, 25:31–33, 25:64–67, 26:37–41, 29:31–38, 29:58–60, 30:59–62, 31:6–13, Fig. 3; Ex. 1002 ¶¶ 125–133).

b. Patent Owner's arguments

Patent Owner does not present any separate arguments that are distinct for any of claims 2–7, 9–12, 14–18, 20, 22–26, and 28 apart from their dependency from claims 1, 13, and 21. *See generally* PO Resp.; Sur-reply.

c. Conclusion

We determine that Petitioner has established, by a preponderance of evidence, that claims 2–7, 9–12, 14–18, 20, 22–26, and 28 are unpatentable over the combination of Burdett and FortiSandbox.

E. Ground 2: Obviousness Over Sharpe, Seese, and Kamalapuram

Petitioner asserts that claims 1, 2, 4, 5, 7–10, 12–14, 16, 18–22, 24, and 26–28 are unpatentable under 35 U.S.C. § 103 over the combination of Sharpe, Seese, and Kamalapuram. Pet. 50–79.

1. Sharpe

Sharpe describes cloud controller 4208 that accesses cloud storage system, 302 downloads files that are not marked as clean, and sends the files to anti-virus service 4214 for scans. Ex. 1006, 97:37–44. If a scan shows a file is clean, its metadata is updated. *Id.* at 97:56–58. If an infected file is found, cloud controller 4208 may remove, quarantine, and/or mark the file and its metadata. *Id.* at 97:56–62. We reproduce Sharpe’s Figure 42 below.

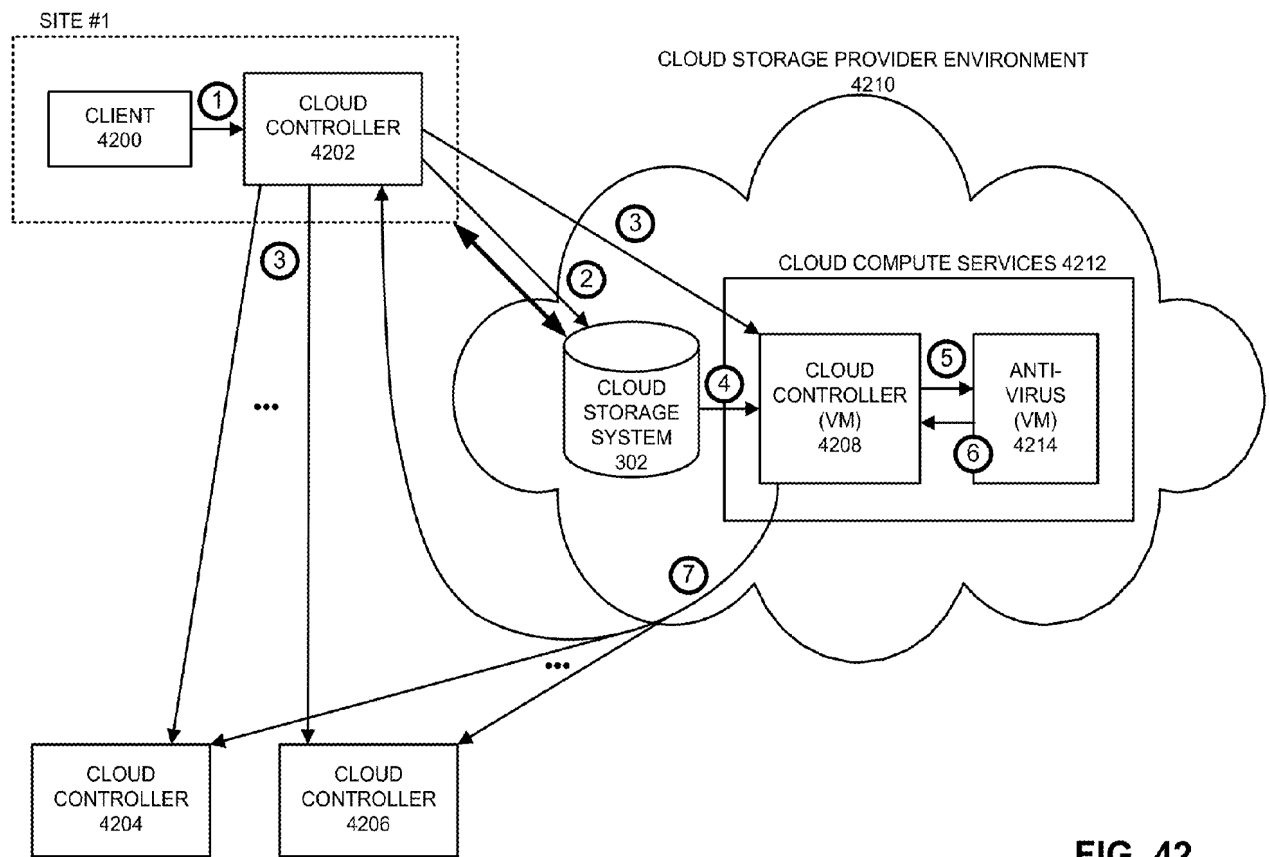


FIG. 42

Figure 42 shows cloud controller 4208 running anti-virus scans.

2. *Seese*

Seese's integrated storage system scans files on cloud service 104A on demand or as scheduled (e.g., daily, weekly, biweekly, and monthly). Ex. 1007 ¶¶ 63, 64. Data Loss Prevention (DLP) server 404 mounts a user share in cloud service 104A to execute discover scan tasks. *Id.* ¶¶ 63–67. DLP discover server 404 pulls files from a mounted user share and inspects the files against policies to generate an incidents report. *Id.* ¶ 68. We reproduce Figure 4 of Seese below to depict the system. Ex. 1007 ¶¶ 63–67.

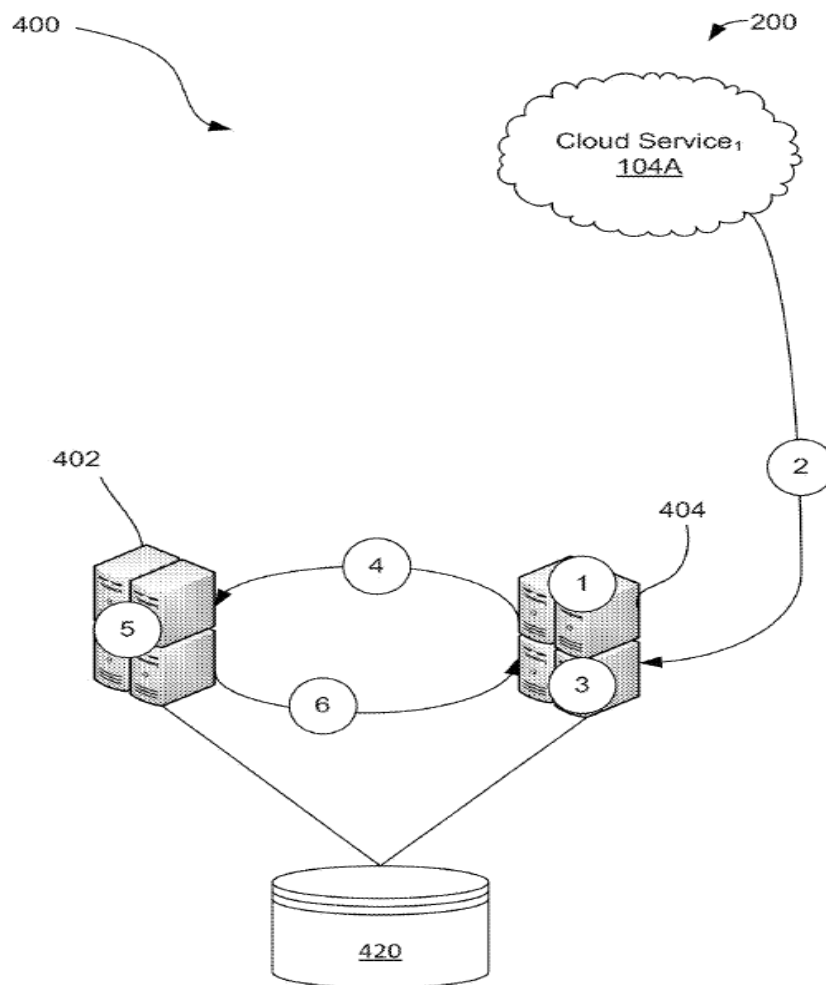


Figure 4 depicts integrated storage system 400 with cloud service 104A natively mounted to DLP server 404. Ex. 1007 ¶¶ 63–67.

3. *Kamalapuram*

Kamalapuram discloses a security analysis system for a network storage system that can be implemented as a cloud-only system for a host system client of an enterprise network or cloud storage system. Ex. 1008 ¶ 121. When the host system uploads a new file or changes an existing file in the cloud storage system, the security analysis system scans the file to determine whether it may be accessed by other hosts or users who cannot access the file until all scanning tools run and return data indicating the file is not compromised. *Id.* ¶¶ 121, 122. Files may be stored in an isolated area until scanned and moved to a general storage area after scanning. *Id.* ¶ 122.

4. *Motivation to combine*

a. *Petitioner's contentions*

Petitioner asserts that a skilled artisan would have been motivated to use Seese's network security device to perform Sharpe's malware scan of files in a first repository and copy clean files to a second repository as taught by Kamalapuram with a reasonable expectation of success because all three references scan shared file repositories for malware detection or data loss protection (DLP) policy compliance. Pet. 52–53 (citing Ex. 1006, 96:42–58; Ex. 1007 ¶¶ 67–68; Ex. 1008 ¶¶ 121–122; Ex. 1002 ¶¶ 138–139). Petitioner asserts that the combination would have improved the malware detection of Sharpe's system and enterprise security by performing Sharpe's malware scans of enterprise files stored in a cloud storage system on Seese's DLP server in the enterprise's network infrastructure to preserve the privacy of the enterprise's files and achieve Sharpe's goal of using an anti-virus service located at a secure site in close network proximity to a cloud storage system. *Id.* at 53 (citing Ex. 1006, 98:27–32; Ex. 1007 ¶ 63; Ex. 1002 ¶ 140).

b. Patent Owner's arguments

Patent Owner argues, “there is no rational basis (other than hindsight) for moving Sharpe’s malware scan from cloud storage environment 4210 onto Seese’ DLP server [that is] ‘deployed within an enterprise’s network infrastructure’ [because] [d]oing so would make Sharpe’s malware scan *worse* by needlessly requir[ing] transferring files from Sharpe’s cloud storage provider environment 4210 containing cloud storage system 302 to Seese’ DLP server for processing, resulting in delay, network congestion, increased security risk, and greater system management complexity.” PO Resp. 33–34. Patent Owner asserts that Petitioner’s proposed motivations do not actually improve the operation of Sharpe’s malware scan. *Id.* at 34.

Patent Owner argues that there is no motivation to move Sharpe’s malware scans from the cloud onto Seese’s DLP server because DLP and malware scanning are two different processes. PO Resp. 34. Patent Owner asserts that DLP discovery should be deployed on a server at the periphery of an enterprise network to prevent unauthorized transmissions of sensitive data and documents outside the network but a malware scan should be deployed in the same cloud storage provider environment as the files that are scanned to minimize file transfers and maximize efficiency. *Id.* at 34–35.

Patent Owner argues that natively mounting Seese’s public cloud file store onto Sharpe’s network security device that can access cloud file stores and communicate natively with cloud file stores is something that Sharpe’s malware scan already does. PO Resp. 35. Patent Owner asserts that moving Sharpe’s malware scan from Sharpe’s cloud storage provider environment 4210 onto Seese’ DLP server “serves no legitimate purpose, is detrimental to the overall system, and is driven entirely by improper hindsight.” *Id.*

c. *Analysis*

We determine that performing Sharpe’s malware scans of cloud file stores on Seese’s DLP server at a secure site in close network proximity to a cloud storage system would improve security as Sharpe expressly teaches

Note . . . 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 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 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 file[]system.*

Ex. 1006, 98:21–32 (emphasis added) (cited in Pet. 53 and Ex. 1002 ¶ 140).

We agree with Petitioner that Seese describes just such a secure site for anti-virus scans of a cloud file system. Reply 23 (“Sharpe . . . contains explicit motivation for the combination with Seese.”). Seese’s integrated storage system scans cloud files using DLP discover server 404 located in enterprise system 102. Ex. 1007 ¶ 64, Figs. 1, 4. We agree with Dr. Franz that using Seese’s DLP server to perform malware scans of cloud files as taught by Sharpe would enable an enterprise to preserve the privacy of its cloud files as Sharpe desires. Ex. 1002 ¶ 140 (citing Ex. 1006, 98:27–32).

We agree that it would have been obvious to use Seese’s DLP server to perform malware scans of files in cloud storage within the enterprise’s network to preserve the privacy of the files and to achieve Sharpe’s goal of using an anti-virus service at a secure site in close network proximity to a cloud storage system to minimize delays. Reply 23–24; Pet. 53, 61–64.

Using Seese's DLP server to scan files achieves Sharpe's goal of offloading anti-virus checks from cloud controllers that provide client file services to reduce the load on the controllers. Ex. 1006, 97:62–66. Natively mounting Sharpe's public cloud file stores on Seese's DLP server allows files to be scanned in the enterprise in native languages to improve privacy, security, communications, and efficiency by scheduling scans on demand or periodically. Ex. 1006, 97:66–98:5; Ex. 1007 ¶¶ 63–76; Pet. 52–53, 61–64.

Contrary to Patent Owner's arguments (PO Resp. 34–35), Seese and Sharpe scan files in cloud storage not at the periphery. Seese's DLP server scans cloud file shares daily, weekly, biweekly, or monthly. Ex. 1007 ¶ 63. DLP discover server 404 pulls files from a user share on cloud service 104A for inspection rather than inspecting files at the periphery as Patent Owner alleges. *Id.* ¶ 65. Sharpe also scans files in cloud storage system 302 by sending files to anti-virus service 4214 for scanning. Ex. 1006, 97:20–44. Data blocks for new files are accessed and transferred to anti-virus service 4212 for scanning. *Id.* at 97:48–53.

We also agree with Petitioner that a skilled artisan would have been motivated to move/copy a file from a repository where files are stored until they are scanned to a general storage area that is accessible to users after a scan indicates a file is free of malware as Kamalapuram teaches for one of the finite ways of doing so. Pet. 52–53, 67–68 (citing Ex. 1002 ¶ 172); Ex. 1008 ¶¶ 121, 122; Ex. 1006, 96:42–97:16.

d. Conclusion

We determine that Petitioner has established, by a preponderance of evidence, that a skilled artisan would have been motivated to combine the teachings of Seese, Sharpe, and Kamalapuram as asserted by Petitioner.

5. *Independent Claim 1*

a. *1[pre]*

(1) *Petitioner's contentions*

Petitioner asserts that Sharpe disclosed a secure data transfer system of computing devices that executed a cloud controller as a virtual machine 4208 or a dedicated physical device to access cloud storage system 302 and send files to anti-virus service 4214 for an anti-virus scan. Pet. 53–55 (citing Ex. 1006, 2:32–40, 96:54–66, 97:14–25, 97:20–24, 97:32–36, 97:56–58, 97:67–98:2, 98:28, 98:43–46, Fig. 42; Ex. 1002 ¶¶ 141–144).

(2) *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions regarding element 1[pre]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Sharpe discloses element 1[pre] to the extent the preamble is limiting.

b. *1[a]*

(1) *Petitioner's contentions*

Petitioner asserts that Sharpe scans public cloud file stores for viruses using routines embodied on a non-transitory computer-readable storage medium to prevent users of an enterprise network from accessing malware-infected files stored in the public cloud file stores such as cloud storage system 302, which is provided by an external vendor, and Seese also scans cloud file stores. Pet. 55–59 (citing Ex. 1006, 2:19–40, 6:42–7:3, 9:34–48, 96:54–66, 97:17–36, 98:1–8, 98:2–32, 100:60–62, 105:9–10, Fig. 42; Ex. 1007 ¶¶ 16, 64; Ex. 1002 ¶¶ 36, 79, 145–152).

(2) *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions regarding element 1[a]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that the combination of Sharpe and Seese discloses or suggests element 1[a].

c. 1[b]

(1) *Petitioner's contentions*

Petitioner contends that Sharpe discloses a processor(s) operable to execute routines as recited in element 1[b] as a cloud controller implemented as a virtual machine or dedicated physical system with a dedicated or shared processor that executes a software module or a piece of code. Pet. 59 (citing Ex. 1006, 6:62–7:3, 98:1–2, 98:5–8, 98:28–30, 105:9–13; Ex. 1002 ¶ 153).

(2) *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions regarding element 1[b]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Sharpe discloses or suggests element 1[b].

d. 1[c][i]

(1) *Petitioner's contentions*

Petitioner asserts that Sharpe's virus scanning executes on a processor as a software routine (an untrusted file processing module). Pet. 59 (citing Ex. 1006, 6:62–7:3, 98:1–2, 98:5–8, 98:28–30, 105:9–13; Ex. 1002 ¶ 154).

Petitioner asserts that Sharp's cloud controller accesses an untrusted file stored on cloud storage system 302 by retrieving untrusted files that did not have a "clean" metadata field, and a skilled artisan would have found it obvious that cloud storage system 302 included a first repository that stored untrusted files to prevent infection of other files and systems as was done routinely. Pet. 59–60 (citing Ex. 1006, 97:32–50, 97:40–51, Fig. 42; Ex. 1002 ¶¶ 155–157). Petitioner also contends that Kamalapuram implemented a security analysis system as a cloud-only system option and when a host system uploaded a file to the network storage system or changed an existing file, the file could be stored in an isolated area of the network storage system until it was scanned by the security analysis system. Pet. 61 (citing Ex. 1008 ¶¶ 58, 121, 122). Petitioner asserts it would have been obvious for Sharpe's cloud storage system to store files in a first repository used in Kamalapuram to isolate files prior to an anti-virus scan and ensure that infected files could not be accessed, and using an isolated file repository in this way would have been a combination of prior art elements according to known methods that would have yielded predictable results. *Id.* (citing Ex. 1006, 96:43–58; Ex. 1002 ¶ 158).

(2) *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions regarding element 1[c][i]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that the combination of Sharpe and Kamalapuram discloses or suggests element 1[c][i].

e. 1[c][ii]

(1) Petitioner's contentions

Petitioner contends that Sharpe and Seese natively mount a public cloud file store on a network security device as recited in element 1[c][ii]. Pet. 61. Petitioner contends that Sharpe's controller 3102 could mount a distributed file system and access its contents by server 3100 using an NFS file system (as the '856 patent system uses) to provide transparent access to data stored in the distributed file system. *Id.* at 61–62 (citing Ex. 1006, 25:38–42, 61:11–22, Fig. 31; Ex. 1001, 11:7–10; Ex. 1002 ¶¶ 159–161).

Petitioner contends that Seese mounts a public cloud file system to a network security device (data loss protection server) that scans a user share on the cloud service, and it would have been obvious to natively mount the user share to Seese's DLP server using well-known NFS and CIFS protocols described in Sharpe so the user share would be accessible to the operating system of the DLP server via native cloud APIs that detect directory changes in the user share and the DLP server can access and control access to the files. Pet. 62–64 (citing Ex. 1007 ¶¶ 18, 63, 64, 67, 68; Ex. 1006, Fig. 42; Ex. 1002 ¶¶ 162–164).

(2) Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions regarding element 1[c][ii]. *See generally* PO Resp.; Sur-reply.

(3) Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that the combination of Sharpe and Seese discloses or suggests element 1[c][ii].

f. 1[c][iii]

(1) Petitioner's contentions

Petitioner asserts that Sharpe prevents users from having read access to files in a cloud storage system until the files are scanned by the anti-virus service and a clean metadata field is marked. *Id.* (citing Ex. 1006, 96:64–66, 97:32–36). Petitioner asserts it would have been obvious to modify Sharpe to store files in a first repository that is not accessible until files are scanned and determined to be clean, as Kamalapuram teaches, to prevent access to untrusted files until they are scanned and approved for access. *Id.* at 64–65 (citing Ex. 1008 ¶ 122; Ex. 1006, 97:33–36; Ex. 1002 ¶¶ 165, 166).

(2) Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions regarding element 1[c][iii]. *See generally* PO Resp.; Sur-reply.

(3) Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that the combination of Sharpe and Kamalapuram discloses or suggests element 1[c][iii].

g. 1[d]

(1) Petitioner's contentions

Petitioner contends that Sharpe's cloud controller 4208 can transfer an untrusted file to anti-virus service 4214 to apply a security check (anti-virus scan) to determine whether the file is free of malicious content and to inform the cloud controller whether the file is clean or infected as recited in element 1[d]. Pet. 65–66 (citing Ex. 1006, 2:25–31, 2:56–61, 6:62–7:3, 96:54–58, 97:48–53, 98:1–2, 98:5–8, 98:28–30, 98:40–46, 105:9–13, Fig. 42).

Petitioner asserts that Seese discloses a network security device (DLP server) that scans files for compliance with a policy, and it would have been obvious to implement Sharpe's anti-virus scan service on Seese's network security device for the reasons discussed for element 1[c][ii] as a simple substitution of known elements with predictable results, particularly where network security devices that performed multiple security options were well-known. Pet. 66–67 (citing Ex. 1007 ¶¶ 67, 68; Ex. 1002 ¶¶ 167–169).

(2) *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions regarding element 1[d]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that the combination of Sharpe and Seese discloses or suggests element 1[d].

h. 1[e]

(1) *Petitioner's contentions*

Petitioner asserts that Sharpe and Kamalapuram both copy a clean file from a first repository to a second repository that is accessible to the users as recited in element 1[e]. Pet. 67. Petitioner asserts that Sharpe also discloses a virus-scanning operation implemented as software routines in a cloud controller executed as a virtual machine to scan a file and make any file that was determined to be clean available to client systems by modifying the file's metadata to mark the "clean" field, which allowed cloud controllers to serve the file to requesting clients. *Id.* (citing Ex. 1006, 2:32–40, 6:62–7:3, 58:28, 96:61–66, 97:23–24, 97:56–58, 98:1–2, 98:5–8, 98:28–30, 105:9–13; Ex. 1002 ¶ 171).

Petitioner contends that Kamalapuram stored a file in an isolated area of the network storage system (a first repository) while waiting to scan it and moved the file to a general storage area (a second repository) after the file was scanned and determined to be clean. Pet. 67–68 (citing Ex. 1008 ¶ 122). Petitioner asserts that it would have been obvious to copy a clean file into a separate repository to make it accessible as an alternative to changing the name or metadata of a clean file and a more efficient way to manage access by using repository-level permissions. *Id.* at 68 (citing Ex. 1002 ¶ 172). We agree with Dr. Franz’s testimony that a skilled artisan would know that “moving” a file from one physical device to another would entail creating a copy at the new location and later deleting the original. Ex. 1002 ¶ 172.

(2) *Patent Owner’s arguments*

Patent Owner argues that Kamalapuram does not disclose “copying” a file and instead describes “moving” files. PO Resp. 31 (quoting Pet. 67–68). Patent Owner asserts that Dr. Franz admits that Kamalapuram’s moving of a clean file might mean updating a directory entry or copying it to another disk and updating a directory entry. *Id.* at 31–32 (citing Ex. 2005 (Deposition of Dr. Franz), 68:8–10). Patent Owner argues that Kamalapuram only moves files in the same storage system so “it would be nonsensical to implement Kamalapuram’s ‘moving’ using any copying [when] the much more efficient solution would be to ‘move’ files by changing file system directory entries and thus *without* ‘copying.’” *Id.* at 32 (citing Pet. 75). Dr. Black testifies that Kamalapuram would not implement “moving” a clean file by “copying” the file when the first and second repositories are in the same storage system and the clear efficiency gains are from moving without copying. Ex. 2004 ¶ 71.

(3) *Analysis*

We find that Kamalapuram moves clean files from an isolated area of the network storage system while waiting to be scanned to a general storage area after the file was scanned. Ex. 1008 ¶ 122. We agree with Petitioner that it would have been obvious to move a clean file by copying it to a general storage area to make it accessible to users by using repository-level permissions as Dr. Franz testifies. Ex. 1002 ¶ 172; Pet. 67–68; Reply 20; *see* Ex. 1001, 7:37–9:27, Fig. 1A; *id.* at 9:35–41, 10:17–22, 11:26–30.

Dr. Franz testifies that moving a clean file by copying it to a second repository would allow a cloud storage system to manage access to clean files by using repository-level permissions that configure one repository to deny read access and a second repository with permissions that allow read access. Ex. 1002 ¶¶ 95, 172 (citing Ex. 1002 ¶ 95). Petitioner asserts that repository-level permissions are more efficient than file-level permissions that require the storage system to update the file permissions for each file and file move. *Id.* We are persuaded by his testimony, which Patent Owner and Dr. Black do not dispute. *See* PO Resp. 31–32; Ex. 2004 ¶ 71.

Petitioner also contends that it would have been obvious to locate the second repository of Kamalapuram on a network security device or external storage device similar to Seese’s “hybrid” model that retains critical data on an enterprise’s private cloud, and it would have been obvious to move clean files to such external storage by copying. Pet. 75–76. We agree because, as the parties agree, a clean file cannot be moved from a public cloud storage to an external storage location using a file directory change. It must be *copied* to that location. PO Resp. 20, 22–23, 32; Ex. 2004 ¶ 58; Ex. 1002 ¶ 96.

(4) *Conclusion*

Based on the parties' contentions and record evidence, we determine Petitioner has demonstrated, by a preponderance of the evidence, that the combination of Sharpe and Kamalapuram discloses or suggests element 1[e].

i. *Conclusion*

Based on the current record, evidence, and contentions, we determine that Petitioner has established by a preponderance of evidence that claim 1 is unpatentable over the combination of Sharpe, Seese, and Kamalapuram.

6. *Independent Claims 13 and 21*

a. *Petitioner's contentions*

Petitioner contends that Sharpe, Seese, and Kamalapuram disclose or suggest every element of claim 13. Pet. 68–70 (citing Ex. 1006, 2:26–52, 97:39–51, 98:33–46; Ex. 1008 ¶¶ 61, 121, 122, 126; Ex. 1002 ¶¶ 173–176; and contentions for similar subject matter in elements 1[c][ii], 1[c][iii], 1[d], and 1[e]). Petitioner asserts that Sharpe, Seese, and Kamalapuram disclose or suggest each element of claim 21. *Id.* at 70–71 (citing Ex. 1006, 6:42–61, 97:25, 98:21–32, 105:9–10; Ex. 1007 ¶¶ 18, 63, 67, 68; Ex. 1002 ¶¶ 181–182; and contentions for similar subject matter in elements 1[c][ii], 1[c][iii], 1[d], 1[e], and 13[a][i]).

b. *Patent Owner's arguments*

Patent Owner does not present separate arguments for claims 13 and 21 apart from what Patent Owner presented for claim 1 for Ground 2. *See* PO Resp. 31–36; Sur-reply 22–25.

c. *Analysis*

We disagree with Patent Owner's arguments for the reasons discussed above for claim 1 where we address those arguments in detail.

d. Conclusion

Based on the current record, evidence, and contentions, we determine that Petitioner has established, by a preponderance of evidence, that claims 13 and 21 are unpatentable over the combination of Sharpe, Seese, and Kamalapuram.

7. Dependent Claims 2, 4, 5, 7, 9, 10, 12, 14, 16, 18, 20, 22, 24, 26, and 28

a. Petitioner's contentions

Petitioner asserts that it would have been obvious to use Seese's DLP server as a network security device to execute Sharpe's anti-virus scanning based on Kamalapuram's configuration of servers as a firewall, gateway, and intrusion detection system for security analysis of files in a cloud file management system as recited in claims 2, 14, and 22 to protect against intrusions. Pet. 71–73 (citing Ex. 1008 ¶¶ 1, 14, 45, 76; contentions for elements 1[c][ii] and 1[d]; Ex. 1002 ¶¶ 188–192).

Petitioner asserts that Sharpe implemented an anti-virus service as a virtual machine to determine whether an untrusted file was free of malicious content, and Kamalapuram's security device executed a sandbox appliance in a virtual machine to scan a file for vulnerabilities as recited in claim 4. Pet. 73 (citing Ex. 1006, 2:26–31, 2:56–61, 96:54–58, 97:25, 98:40–46; Ex. 1008 ¶ 129). Petitioner contends it would have been obvious to configure Kamalapuram's sandbox virtual machine to execute Sharpe's anti-virus service virtual machine as a simple substitution that would have improved Sharpe's anti-virus service to mitigate system failures and prevent software vulnerabilities from spreading as Kamalapuram taught. *Id.* at 73–74 (citing Ex. 1008 ¶ 129; Ex. 1002 ¶¶ 193–195).

Petitioner asserts that Sharpe discloses NFS, CIFS, SAN, and iSCSI protocols for writing and reading data from a remote file system to support local storage, Seese discloses a network security device, and Kamalapuram discloses a second repository as recited in claims 5, 16, and 24, and it would have been obvious to implement such a network security device to copy files to one or more repositories using any of the protocols recited in claims 5, 16, and 24. Pet. 74–75 (citing Ex. 1006, 8:4–5, 9:8, 25:6–7, 25:38–42, 25:54–59; contentions for elements 1[c][ii] and 1[d]; Ex. 1002 ¶¶ 196–198).

Petitioner contends that Sharpe discloses a cloud controller that could quarantine a file that was found to be infected with malicious content as well as remove the infected file by deleting it as recited in claims 7, 18, and 26. Pet. 75 (citing Ex. 1006, 97:58–60; Ex. 1002 ¶ 199).

Petitioner contends that Kamalapuram discloses first and second repositories that are part of the same storage system, and it would have been obvious to form the repositories as part of a public cloud file store as recited in claims 9, 20, and 28. Pet. 76–77 (citing Ex. 1008 ¶¶ 58, 121, 122; contentions for element 1[e]; Ex. 1002 ¶ 201).

Petitioner contends that Sharpe discloses cloud storage provided by a third-party cloud storage service provider external to an enterprise as recited in claim 10. Pet. 77 (citing Ex. 1006, 9:35–36; 98:21–32; Ex. 1002 ¶ 202).

Petitioner asserts that Sharpe and Kamalapuram move files between repositories for virus scanning, and it would have been obvious to move files to a third repository for security checks and move clean files to a second repository as recited in claim 12. Pet. 77–79 (citing Ex. 1006, 2:26–31, 2:56–61, 96:54–58, 97:48–53, 98:40–46, Fig. 42; contentions for elements 1[c][i], 1[c][iii], and 1[e]; Ex. 1008 ¶ 122; Ex. 1010; Ex. 1002 ¶¶ 204–208).

b. Patent Owner's arguments

Patent Owner does not present any separate arguments for any of claims 2, 4, 5, 7, 9, 10, 12, 14, 16, 18, 20, 22, 24, 26, and 28 apart from their dependency from claims 1, 13, and 21. *See generally* PO Resp.; Sur-reply.

c. Conclusion

We determine that Petitioner has established by a preponderance of evidence that claims 2, 4, 5, 7, 9, 10, 12, 14, 16, 18, 20, 22, 24, 26, and 28 are unpatentable over the combination of Sharpe, Seese, and Kamalapuram.

8. Claims 8, 19, and 27

a. Petitioner's contentions

Petitioner asserts that Kamalapuram discloses a second repository in a “general storage area” of a network storage system and first repository in an “isolated area” of the same network storage system. Pet. 75 (citing Ex. 1008 ¶ 122; contentions for element 1[e]). Petitioner contends that it would have been obvious to locate a second repository on a network security device in the enterprise network to improve the security of files where Seese’s hybrid cloud storage model stored critical data in the enterprise’s private cloud separate from less-sensitive data that was stored on a public cloud storage provider. *Id.* at 75–76 (citing Ex. 1007 ¶ 6; Ex. 1002 ¶ 200); Reply 25.

b. Patent Owner's arguments

Patent Owner argues that claims 8, 19, and 27 recite a first repository that is part of a public cloud file store and a clean file is copied to a second repository that is part of a network security device or an external storage device of the enterprise network. PO Resp. 36. Patent Owner argues that none of the cited art discloses copying a clean file from a public cloud file store to outside that public cloud file store. *Id.* at 37 (citing Ex. 2004 ¶ 80).

Patent Owner argues that Seese describes mounting a public cloud file system on a network security device to scan the files to protect the enterprise against data loss, and implementing the proposed combination on a “hybrid cloud storage” of Seese does not provide a rationale for copying or moving the files from the public portion of the cloud storage to the private portion of the cloud storage. PO Resp. 38. Patent Owner asserts that the modification would not improve the security of files based on the importance of the data because data that is important enough to warrant storing in the enterprise network would not be stored in a first repository in a public cloud file store in the first instance and data that can be stored in a public cloud file store can remain there after it is confirmed clean with no security drawback. *Id.*

c. Analysis

We agree with Petitioner that it would have been obvious to locate a second repository on a network security device or external storage device in an enterprise network to improve file security based on an administrator’s assessment of the importance of the data. Seese teaches to use a “hybrid” cloud storage model to store critical data in the enterprise’s private cloud separate from less-sensitive data that is stored on and accessible from a public cloud storage provider to improve security as discussed *supra*. See Pet. 75–76; Ex. 1007 ¶ 6. Seese’s teachings of the advantages of using a hybrid cloud storage model to store critical data in an enterprise’s private cloud apart from less-sensitive data that can be stored on, and accessed at, a public cloud storage provider provides the motivation to move sensitive files from a public cloud store to an external enterprise network as proposed. *Cf.* Sur-reply 26. Seese stores critical data on an enterprise’s private cloud to improve security. Ex. 1007 ¶ 6.

We disagree with Patent Owner’s argument that a file with critical data would not be stored in a public cloud file store initially (PO Resp. 38) because enterprises use public cloud file stores to receive files from client systems at the public cloud file store in the first instance. Ex. 1007, 2:26–61, 97:17–36, Fig. 42; Ex. 1007 ¶¶ 63–69; Ex. 1008 ¶¶ 121, 122. Files are scanned after they are received in a public cloud file. If they are trustworthy and contain sensitive data, they would be moved to a second repository in the enterprise’s private cloud to protect the sensitive data. As a result, we disagree with Patent Owner’s arguments that “Petitioner’s rationale would actually counsel *against* ‘copying’ a ‘clean’ file from a ‘public cloud file store’ to outside that ‘public file store.’” PO Resp. 38–39. An enterprise would store files containing sensitive data in a private enterprise cloud where it would be accessible to enterprise users under conditions controlled directly by an enterprise to protect that data.

d. Conclusion

Based on the current record, evidence, and contentions, we determine that Petitioner has established by a preponderance of evidence that claims 8, 19, and 27 are unpatentable over the combination of Sharpe, Seese, and Kamalapuram.

F. Ground 3: Obviousness Over Sharpe, Seese, Kamalapuram, and Dods

Petitioner asserts that claims 3, 6, 11, 15, 17, 23, and 25 are unpatentable under 35 U.S.C. § 103 over the combination of Sharpe, Seese, Kamalapuram, and Dods. Pet. 79–81.

1. *Dods*

Dods discloses a security platform that uses behavior-based analysis to detect malware in files. Ex. 1009, 10:16–26.

2. *Motivation to combine*

a. *Petitioner’s contentions*

Petitioner contends that a skilled artisan would have been motivated to combine Dods’ teachings with Sharpe, Seese, and Kamalapuram to detect malware in files by using additional mechanisms of behavior-based analysis and a secure sandbox, to improve the overall malware detection capabilities of the combination, which lacks these mechanisms. Pet. 79–80.

b. *Patent Owner’s arguments*

Patent Owner argues that Petitioner identifies no motivation to combine Dods with the other cited prior art and does not identify the “additional mechanisms.” PO Resp. 40; Sur-reply 27.

c. *Analysis*

Petitioner relies on Dods to disclose a security platform that identifies a malicious payload using a secure sandbox and a behavior-based analysis of results of opening the secondary file. Pet. 79–80. We agree with Petitioner that it would have been obvious to use Dods’ sandbox and behavior-based analysis of the results of opening a file in the Sharpe-Seese-Kamalapuram combination to improve its malware detection ability similarly. *Id.*; Reply 27–28; *see KSR*, 550 U.S. at 417 (“[I]f a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.”).

d. Conclusion

We determine that Petitioner has established by a preponderance of evidence that it would have been obvious to combine the teachings of Dods with the Sharpe-Seese-Kamalapuram combination.

3. Claims 3, 6, 11, 15, 17, 23, and 25

a. Petitioner's contentions

Petitioner provides detailed contentions regarding how Sharpe, Seese, Kamalapuram, and Dods teach and suggest each element of claims 3, 6, 11, 15, 17, 23, and 25 and render those claims obvious. Petitioner supports its contention with testimony of Dr. Franz. Pet. 79–81 (citing Ex. 1002 ¶¶ 210–216).

b. Patent Owner's arguments

Patent Owner argues that Petitioner's generic assertion of unidentified improvements does not meet Petitioner's burden of proof. PO Resp. 27.

c. Analysis

We agree with Petitioner that using Dods' behavior-based scans in a sandbox environment to detect malicious payloads in the Sharpe-Seese-Kamalapuram combination would improve that combination similarly. Pet. 79–80; Reply 27–28.

d. Conclusion

Based on the current record, evidence, and contentions, we determine that Petitioner has established, by a preponderance of evidence, that claims 3, 6, 11, 15, 17, 23, and 25 are unpatentable over the combination of Sharpe, Seese, Kamalapuram, and Dods.

III. CONCLUSION

Petitioner has demonstrated by a preponderance of the evidence that claims 1–28 of the '856 patent are unpatentable.

Claims	35 U.S.C. §	References	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–7, 9–18, 20– 26, 28	103	Burdett, FortiSandbox	1–7, 9–18, 20– 26, 28	
1, 2, 4, 5, 7–10, 12–14, 16, 18– 22, 24, 26–28	103	Sharpe, Seese, Kamalapuram	1, 2, 4, 5, 7–10, 12–14, 16, 18– 22, 24, 26–28	
3, 6, 11, 15, 17, 23, 25	103	Sharpe, Seese, Kamalapuram, Dods	3, 6, 11, 15, 17, 23, 25	
Overall Outcome			1–28	

IV. ORDER

In consideration of the foregoing, it is:

ORDERED that claims 1–28 of the '856 patent have been shown to be unpatentable; and

FURTHER ORDERED that because this is a Final Written Decision, parties to this proceeding seeking judicial review of this Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.¹⁰

¹⁰ Should Patent Owner wish to amend the challenged claims in a reissue or reexamination proceeding, we draw Patent Owner's attention to the *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16654 (Apr. 22, 2019). If Patent Owner files a reissue application or request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of such related matters in updated mandatory notices. See 37 C.F.R. § 42.8(a)(3), (b)(2).

IPR2023-00456
Patent 11,036,856 B2

PETITIONER:

Thomas Millikan
Babak Tehranchi
Kristen Schunter
PERKINS COIE LLP
millikan-ptab@perkinscoie.com
tehranchi-ptab@perkinscoie.com
schunter-ptab@perkinscoie.com

PATENT OWNER:

James Glass
John McKee
Quincy Lu
Andrew Holmes
Ognjen Zivojnovic
QUINN EMANUEL URQUHART & SULLIVAN LLP
jimglass@quinnemanuel.com
johnmckee@quinnemanuel.com
quincylu@quinnemanuel.com
drewholmes@quinnemanuel.com
ogizivojnovic@quinnemanuel.com