

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,
Petitioner,

v.

FORTINET, INC.,
Patent Owner.

Case No. IPR2023-00456
U.S. Patent No. 11,036,856

PATENT OWNER RESPONSE
PURSUANT TO 35 U.S.C. § 316 AND 37 C.F.R. § 42.120

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. OVERVIEW OF THE '856 PATENT	4
III. OVERVIEW OF CERTAIN CITED ART	7
A. Ground 1 Cited Art.....	7
1. U.S. Patent No. 11,281,775 (“Burdett”) (Ex. 1004)	7
2. FortiSandbox (Ex. 1005)	10
B. Ground 2 Cited Art.....	10
1. U.S. Patent No. 9,811,662 (“Sharpe”) (Ex. 1006)	10
2. U.S. Patent Appl. Pub. No. 2015/0100357 (“Seese”) (Ex. 1007).....	12
3. U.S. Patent Appl. Pub. No. 2020/0050686 (“Kamalapuram”) (Ex. 1008)	13
C. Additional Ground 3 Cited Art	14
1. U.S. Patent No. 10,382,468 (“Dods”) (Ex. 1009)	14
IV. LEVEL OF ORDINARY SKILL IN THE ART.....	14
V. CLAIM CONSTRUCTION	15
VI. Response to Ground 1: Burdett and FortiSandbox.....	15
A. Petitioner Fails to Address the “Copying” Claim Limitation	15
1. Petitioner’s Cited Art Does Not Disclose the Claimed “Copying”	16

2.	Petitioner’s Cited Art Does Not Render Obvious the Claimed “Copying”	21
B.	Petitioner Failed to Show It Would Be Obvious to Combine Burdett with FortiSandbox	27
VII.	Response to Ground 2: Sharpe, Seese, and Kamalapuram	31
A.	Petitioner Fails to Address the “Copying” Claim Limitation	31
B.	Petitioner Failed to Show It Would Be Obvious to Combine Sharpe With Seese	33
C.	Petitioner Failed to Show Unpatentability of Dependent Claims 8, 19, and 27	36
VIII.	GROUND 3	39
IX.	CONCLUSION	40

EXHIBIT LIST

No.	Exhibit
2001	Declaration of John Black, Jr., Ph.D.
2002	<i>Curriculum vitae</i> of John Black, Jr., Ph.D.
2003	FortiSandbox 4.2.4 Administration Guide, <i>available at</i> https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/fba32b46-b7c0-11ed-8e6d-fa163e15d75b/FortiSandbox-4.2.4-Administration_Guide.pdf .
2004	Supplemental Declaration of John Black Jr., Ph.D.
2005	Transcript of the Testimony of Dr. Franz (November 29, 2023)

I. INTRODUCTION

The Board should uphold the validity of the claims of U.S. Patent No. 11,036,856 (the “’856 patent”). The deposition of Petitioner’s expert, Dr. Franz, confirmed the gaps in Petitioner’s invalidity theories first identified in Fortinet’s preliminary response and, in fact, negated the Board’s basis for instituting this IPR in the first instance.

First, Petitioner failed to show the cited art discloses or renders obvious the limitation “copying the clean file from the first repository to a second repository.” Notwithstanding the clear recitation of “copying,” Petitioner treats this limitation as if it was met by the cited art’s disclosure of “moving” files. As set forth below, experts for both Petitioner and Patent Owner agree that there is a distinction between “copying” and moving. Ex. 2005 at 38:20-22 (“[T]he difference between copying and moving is whether there still is a copy of that same file in the original dirty repository.”).

When the Board instituted this IPR, it did so on a less than fulsome record, finding that the cited art “discloses this [claimed] type of copying.” ID at 24. That finding has now been negated: when Petitioner’s own expert was asked “Does Burdett [in Ground 1] disclose the claimed copying?,” he testified that “Burdett does not.” Ex. 2005 at 44:4-7. Petitioner’s expert then went on to explain “Burdett teaches enough that a person of ordinary skill

would have found it obvious that one alternative to control access to a contaminated file was to **move** the file to a different location.” Ex. 2005 at 44:13-24.¹ But this only underscores Petitioner’s point: “moving” and “copying” are not the same, and Petitioner’s cited art discloses “moving,” not “copying.”

Moreover, it would be **nonsensical** to modify Petitioner’s cited art to “move” files by “copying” them. Petitioner’s cited art in both Grounds 1 and 2 only “moves” files within the **same** file system. Under those circumstances, there is an efficient solution for “moving” files, which is to modify file system directory entries. Doing so requires minimal processing regardless of file size. Critically, “moving” files by modifying file system directory entries does not entail any “copying.” Nonetheless, Petitioner asserts, without any explanation or analysis, that it would be obvious to modify these cited references to instead “move” files by “copying” them. Such a modification would be an absurd waste of processing, locking up computer resources by having them engage in the pointless copying of data, especially for larger files. The goal of Petitioner’s primary references is to improve efficiency. Ex. 1004 at 1:42-53 (“It is desired to provide protection ... in a manner that is **simple and efficient**

¹ All emphasis added unless stated otherwise.

and ***with minimal performance impact***’); Ex. 1006 at 8:16-18 (“These additional metadata structures can ... be used to ***quickly and efficiently*** construct snapshots that identify file metadata and file data that has changed due to recent write operations.”). It would be nonsensical to then modify the cited references to make them ***less*** efficient solely to arrive at the ’856 patent claims. Accordingly, Petitioner has also failed to show that the cited art renders obvious the “copying” claim limitations.

Second, Petitioner fails to present any cognizant rationale for combining the cited art. Petitioner’s combinations propose moving processing of files found in cloud infrastructure from a service running in that same cloud infrastructure to an alleged “network security device” deployed within an enterprise network. These proposed modifications are quintessential hindsight bias, since Petitioner does not identify any benefit from the modifications. Indeed, Petitioner fails to address the many ***disadvantages*** that would discourage a POSITA from making the proposed combination. For example, with Petitioner’s proposed modifications, every file to be processed would need to be transferred from the cloud infrastructure to the alleged network security device deployed in the enterprise network, whereas previously the relevant processing would be performed within the cloud infrastructure. Thus, Petitioner’s proposed modifications would only

lead to unnecessary file transfers that waste time, congest networks, and create security risks. Accordingly, Petitioner's proposed modifications are not only non-obvious, they are counterintuitive.

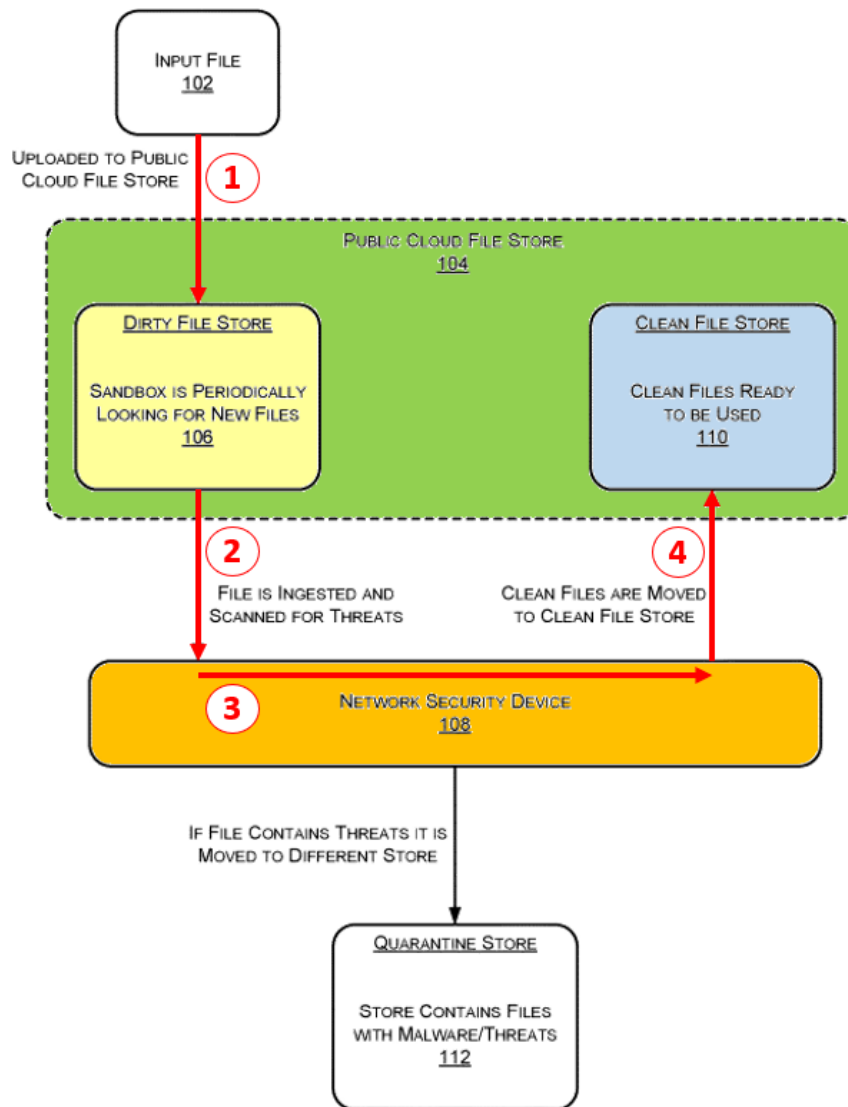
Moreover, Dr. Franz's deposition confirmed that the alleged motivations that Petitioner does present are illusory in nature. For example, Dr. Franz admitted that each base reference was already capable of accessing files and controlling access to files, even without Petitioner's proposed modifications. Ex. 2005 at 49:19-22, 50:2-5, 65:10-66:19. His obvious combinations also do not improve data file transfer or scanning speed. Accordingly, Petitioner failed to identify a rationale for the proposed combinations and thus cannot show the proposed combinations are obvious.

Third, Petitioner's arguments for various dependent claims require additional modifications to the cited art that lack any motivation other than being driven by hindsight bias.

Accordingly, the Board should reject Petitioner's invalidity grounds and uphold the validity of the '856 patent claims.

II. OVERVIEW OF THE '856 PATENT

The '856 patent has a priority date of September 16, 2018 and is titled "Natively Mounting Storage for Inspection and Sandboxing in the Cloud." Figure 1A (annotated) shows an exemplary embodiment:



The two key components in Figure 1A are the “network security device” (orange) that protects an “enterprise network” (not pictured) and checks files stored “public cloud file store” (green) for malicious content (e.g., viruses, malware, worms, Trojans, etc.). Within the “public cloud file store” there is a “dirty file store” (yellow)—also called a “first repository” in the claims—of files that users do not have read access to and a “clean file store”

(blue)—also called a “second repository” in the claims—of files accessible to the user.

New files that have not yet been checked are first uploaded to the “dirty file store” (step 1). From there, files are ingested (either in response to an alert or as part of a periodic scan) by the network security device (step 2). The network security device checks the files for malicious content (step 3). If a file is clean, it is copied to the “clean file store” and thereby made accessible to the user (step 4).

One additional feature of the ’856 patent is that the public cloud file store is “natively mounted” on the network security device. As the ’856 patent explains, “[c]urrently, scanning of a file residing on cloud storage requires passing the file through a security inspection virtual machine (VM)/image,” which is “inefficient.” ’856 patent at 1:67-2:3. “Natively mount[ing]” the “public cloud file store” allows a network security device to perform “desired security checks (e.g., AV scanning, file checking, sandboxing, etc.) while [the files are] residing in a segregated data storage area.” *Id.* at 3:27-36.

III. OVERVIEW OF CERTAIN CITED ART

The petition challenges the '856 patent's independent claims 1, 13, and 21 on two grounds: Ground 1 and Ground 2.²

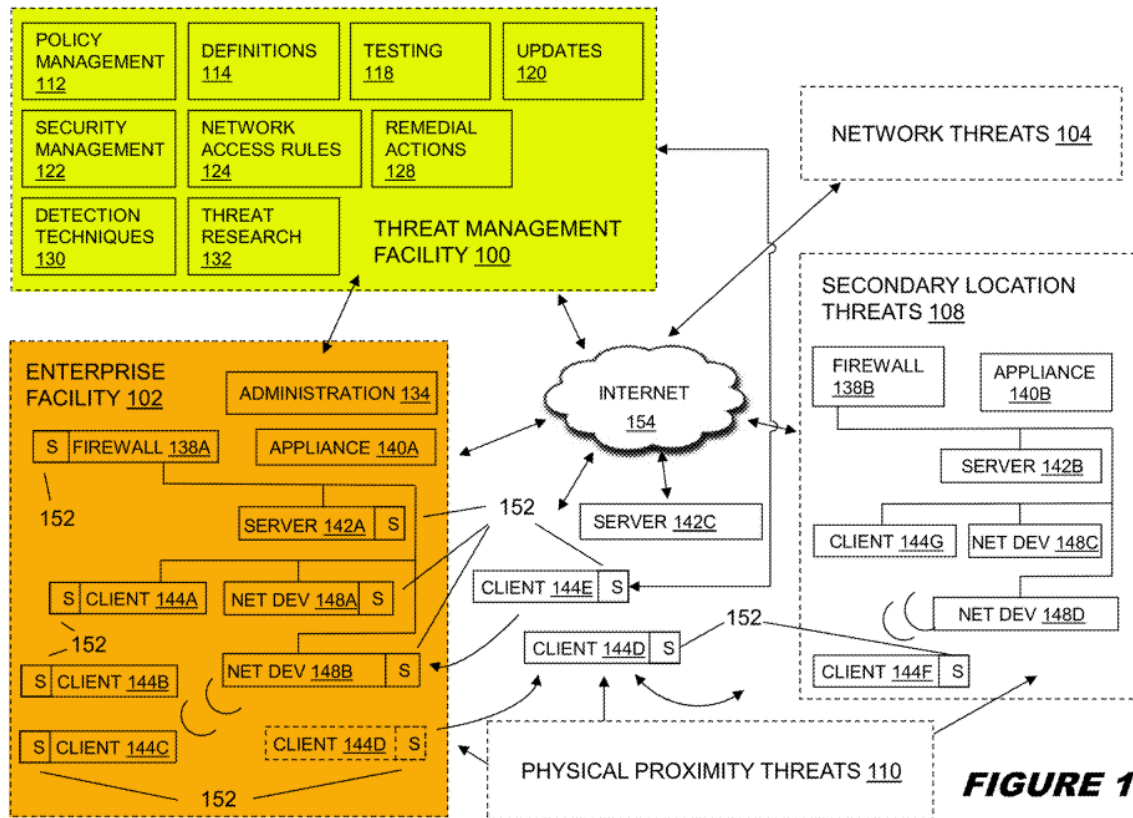
A. Ground 1 Cited Art

1. U.S. Patent No. 11,281,775 (“Burdett”) (Ex. 1004)

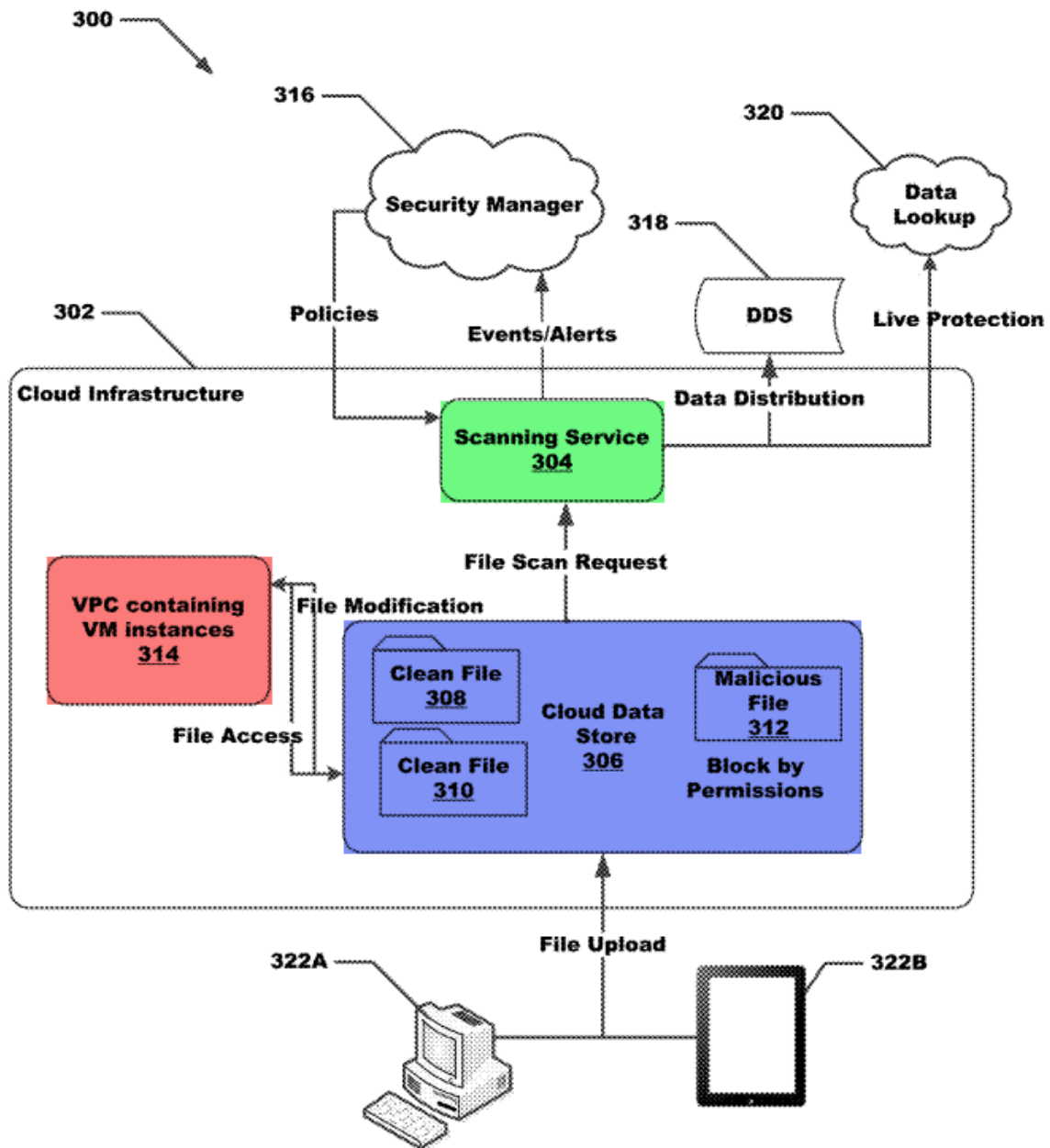
Burdett describes two separate embodiments (Figure 1 and Figure 3) that are relevant to Petitioner's Ground 1.

In the first embodiment, shown in Figure 1, a “threat management facility 100” (yellow) protects a traditional “enterprise facility 102” (orange) by, for example, “provid[ing] controlled access to the enterprise facility 102 networks.” Burdett at 11:57-58.

² The petition also asserted Ground 3 directed solely at dependent claims.



In contrast, in Figure 3, the relevant components all reside in a “cloud infrastructure 302,” where “scanning service 304” scans files in “cloud data store 306” to prevent “applications instantiated on virtual machines within the virtual private cloud [VPC] 314” from accessing malicious files. Burdett at 23:33-38, 26:44-49.



Absent from Burdett's description of Figure 3 is any reference to "threat management facility 100" or "enterprise facility 102" in Figure 1. Conversely, the description of Figure 1 never mentions "cloud infrastructure

302” or “VPC 314,” “cloud data store 306,” and “scanning service 304” found therein.

2. FortiSandbox (Ex. 1005)

FortiSandbox is an “Administration Guide” for one of Patent Owner’s own products, FortiSandbox Version 2.3.2. FortiSandbox is designed to “execute[] suspicious files in the VM [virtual machine] host module to determine if the file is High, Medium, or Low Risk based on behavior observed in the VM sandbox module.” FortiSandbox at 8. The files to be processed can be submitted on-demand, obtained by sniffing traffic passing on a network, received from another Fortinet appliance (e.g., FortiGate or FortiMail) or found on a remote network share. *Id.* at 88. When configuring FortiSandbox to scan files on a network share, the user specifies a “Mount Type,” “Server Name/IP,” and “Share Path,” and other variables. *Id.* at 114-15.

B. Ground 2 Cited Art

1. U.S. Patent No. 9,811,662 (“Sharpe”) (Ex. 1006)

Sharpe is a lengthy reference with numerous distinct embodiments and over forty figures. Petitioner’s allegations focus on Figure 42:

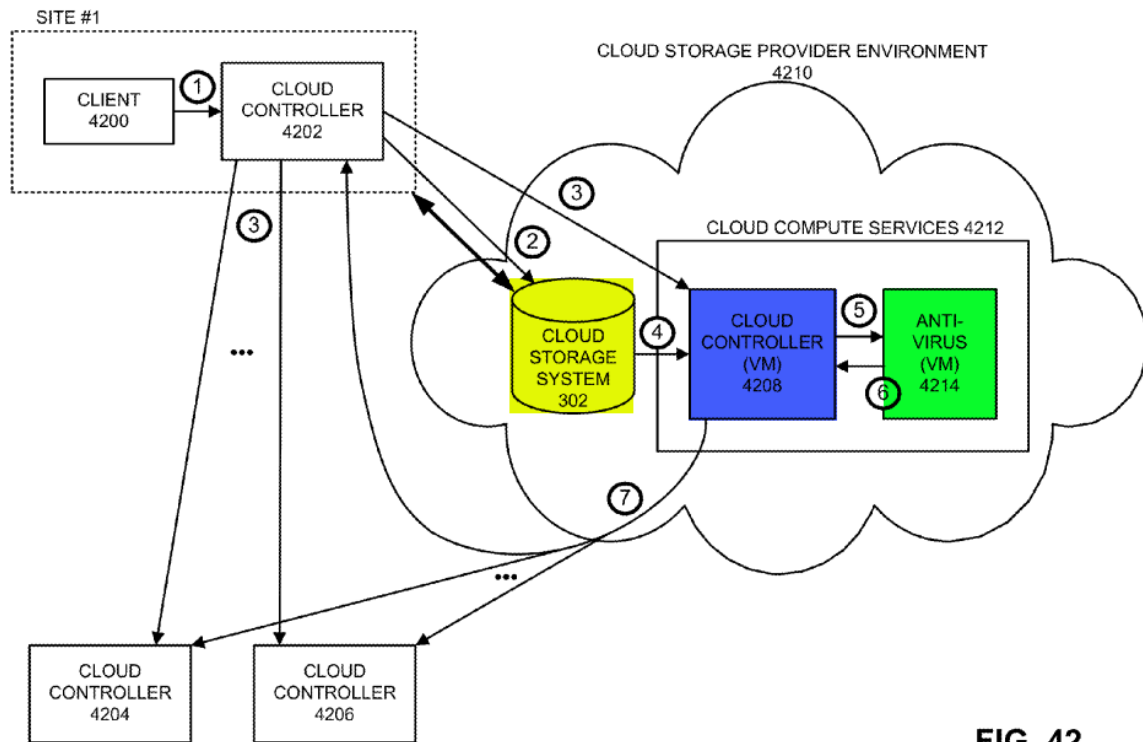
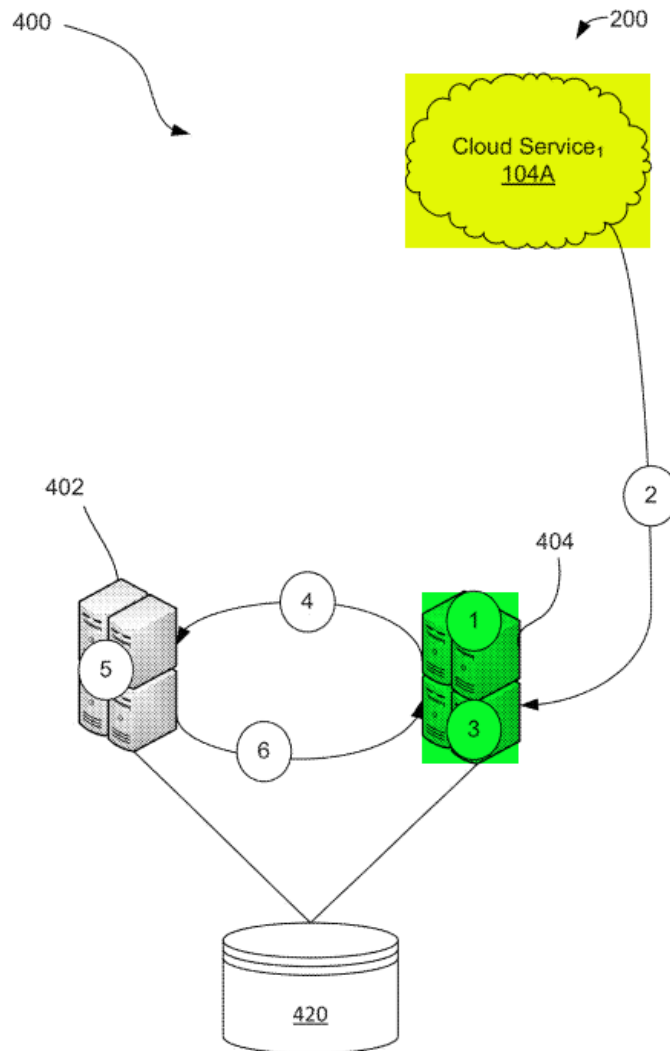


FIG. 42

In Sharpe, a client can upload a file to “cloud storage system 302” (yellow) via “cloud controller 4204.” When a new file is uploaded or an existing file is modified, “the file is not marked as clean,” and “other cloud controllers ... do not yet allow clients to actually access the new (or modified) file.” Sharpe at 97:27-36. The file is then scanned by “anti-virus service 4214” (green) via “cloud controller 4208” (blue). *Id.* at 97:37-53. If the scan indicates the file is clean, its metadata “is updated to indicate this clean status.” *Id.* at 97:56-58.

**2. U.S. Patent Appl. Pub. No. 2015/0100357 (“Seese”)
(Ex. 1007)**

Seese describes “scan[ning] of files stored on a cloud service.” Seese at [0064].



Specifically, “DLP [data loss prevention] discovery server 404” (green) executes a “discovery scan task” based on “DLP rules” for “identify[ing] confidential data. Such as Social security numbers, financial data (e.g., credit

card number, magnetic stripe data, and the like), username and password pairs, proprietary information, licensed data (e.g., copy righted works), or any other data that may compromise the enterprise if the data is misappropriated.” Seese at [0054], [0068]. To do so, the DLP discover server, “mounts” one “user share” at a time, “pulls files from the user share on the cloud service 104A” (yellow), and “inspects the files against configured policies and rules to generate an incidents report.” *Id.* at [0067]-[0068]. “[A]s incidents are detected by the DLP discover server 404[,] they are sent to an incident database 420 and are viewable from the enforce server 402 for incidents review and remediation as necessary.” *Id.* at [0070].

**3. U.S. Patent Appl. Pub. No. 2020/0050686
 (“Kamalapuram”) (Ex. 1008)**

Kamalapuram describes “a cloud only system” where uploaded files are first “scanned by a security analysis system.” Kamalapuram at [0121]. Initially, an uploaded file “may be stored in an isolated area of the network storage system,” and “[u]sers may be prevented from accessing the file, or the file may be limited to a view only mode until all scanning tools ... have been run.” *Id.* at [0122]. As part of that scan, “the network security analysis system” then “determine[s] whether the file may be accessed or downloaded

by other hosts or other users.” *Id.* at [0121]. Once the file has been scanned, it “may be moved to a general storage area.” *Id.* at [0122].

C. Additional Ground 3 Cited Art

1. U.S. Patent No. 10,382,468 (“Dods”) (Ex. 1009)

Dods describes a device for analyzing files in a secure “Sandbox” to identify potential malware. Specifically, Dods discloses opening a received file in a secure environment, determining that a secondary file may have been also accessed, and then analyzing the secondary file in the secure environment to identify malware. Dods at Abstract. The secondary file may be processed using “a static analysis (analyzing the secondary file without opening the secondary file), a signature-based analysis (comparing signature sequences of the secondary file with signature sequences in a database of malware signatures), a statistical-based analysis (using machine learning to determine whether the secondary file includes malware), a dynamic analysis (involving opening the secondary file), a behavior-based analysis (analyzing results of opening the secondary file), or the like.” Dods at 10:16-26.

IV. LEVEL OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the art (“POSITA”) relevant to the ’856 patent at the time of the invention 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.

Patent Owner's description of the level of ordinary skill in the art is almost the same as that of the Petitioner. *See* Pet. 15-16. The positions set forth in this preliminary response would be the same under either parties' proposal.

V. CLAIM CONSTRUCTION

In an *inter partes* review, claim terms receive their plain and ordinary meaning in light of the specification of the patent in which it appears, the same standard as used in district court. 37 C.F.R. § 42.100(b); *see Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005). Petitioner states that “no constructions are necessary.” Pet. 16. Patent Owner agrees that no claim terms presently require construction to resolve any current dispute between the parties. Patent Owner reserves the right to proffer a construction for a claim term at a later point if it becomes pertinent to any particular dispute.

VI. RESPONSE TO GROUND 1: BURDETT AND FORTISANDBOX

A. Petitioner Fails to Address the “Copying” Claim Limitation

All independent claims of the '856 patent require “*copying* the clean file from the first repository to a second repository.” The Board found at the

institution stage that “Burdett discloses [the claimed] type of copying.” ID at 24. This ruling, however, was based on an incomplete record; indeed, Petitioner’s expert has since expressly agreed in cross examination that ***Burdett does not disclose copying***. When asked “Does Burdett [in Ground 1] disclose the claimed copying?,” Petitioner’s expert testified that “Burdett does not.” Ex. 2005 at 44:4-7. Petitioner’s expert went on to explain that “Burdett teaches enough that a person of ordinary skill would have found it obvious that one alternative to control access to a contaminated file was to ***move*** the file to a different location,” therefore taking the position that ***Burdett teaches moving not copying***. Ex. 2005 at 44:13-24. Thus, there is no dispute that “moving” and “copying” files are different operations, and no dispute that Burdett only discloses “moving,” not “copying.” Because Petitioner also did not show that Burdett (alone or in combination with FortiSandbox) renders this limitation obvious, Petitioner’s Ground 1 fails.

1. Petitioner’s Cited Art Does Not Disclose the Claimed “Copying”

The relevant limitation of the ’856 patent independent claims requires “***copying*** the clean file from the first repository to a second repository.” See ’856 patent claims 1, 13, 21. This is in contrast to other limitations that require “***moving*** the untrusted file from the first repository to a third repository” for

checking. See '856 patent claim 12. Thus, based on the claims themselves, the terms “copying” and “moving” have ***different meanings*** and require that ***different actions*** be performed on files—copying vs. moving. Ex. 2004 ¶ 48; see also *Bd. of Regents of the Univ. of Tex. Sys. v. BENQ Am. Corp.*, 533 F.3d 1362, 1371 (Fed. Cir. 2008) (“Different claim terms are presumed to have different meanings.” (citation omitted)). The plain meaning of “copying” information requires creating at least temporarily a second copy of portions of that information. Ex. 2004 ¶ 48. In contrast, the plain meaning of “moving” merely requires changing the location of the information independent of any particular mechanism for doing so. *Id.* Indeed, even Petitioner’s expert, Dr. Franz, admitted that there was a difference between “moving” and “copying”: “the difference between copying and moving is whether there still is a copy of that same file in the original dirty repository.” Ex. 2005 at 38:20-22.

Thus, while “moving” ***can*** be implemented using “copying,” “moving” can also be implemented ***without*** any copying. For example, it is possible to change a file’s location by modifying the file system directory entries (thereby “moving” the file within the file system) without ever creating a second copy of even portions of that file (*i.e.*, without any “copying”). Ex. 2004 ¶ 49. Petitioner’s expert conceded this key distinction. Ex. 2005 at 48:2-4 (“Q. So high-level moving can be done with or without low-level copying. Is that your

testimony? A. Yes.”). For example, the “mv” command in POSIX systems uses a “rename” system call to modify file system directory entries, thereby “moving” the file to a new location within the file system without any “copying.” Ex. 2004 ¶ 49.

In its institution decision, the Board found that “the ’856 patent uses the terms ‘moving,’ ‘copying,’ and ‘transferring’ *interchangeably*” and that the cited art’s disclosure of “moving” a file thus also discloses the claimed “copying.” ID at 23-24 (emphasis in original). Respectfully, however, this argument is not supported in context of a more fulsome, post-institution record. The position was not raised in the Petition, was expressly refuted by Petitioner’s expert on cross examination, and is contrary to claim language (as noted above) that uses the two terms *differently*. Indeed, Petitioner’s expert, Dr. Franz, testified that it was **not** his testimony that “copying” is synonymous with “moving.” Ex. 2005 at 45:2-4 (“Q. Is it your position that the claimed language ‘copying’ is synonymous with ‘moving a file’? A. I never said that.”).

Nor does the intrinsic evidence cited in the institution decision mandate a different outcome. First, the institution decision cites to the ’856 patent’s disclosure that “copying” “can be performed by *sharing* the files.” ID at 22 (quoting ’856 patent at 6:5-10 and claim 5) (emphasis in original). Whether

“copying” can be implemented using a third process (“sharing”) does not mean the two terms are interchangeable, and is unrelated to whether “copying” and “moving” are interchangeable.³

Second, the institution decision states that the ’856 patent “ascribes no significance to copying or moving files.” ID at 23. Respectfully, as addressed below in more detail in connection with obviousness, there are significant differences between those two terms, at least as mandated by their separate use in different claims. Ex. 2004 ¶¶ 48-49, 52, 55-58.

Third, the institution decision cites the ’856 patent’s Figure 1A and 1B, which show that the “copying” step of the claims can also involve “moving” files. ID at 23. This is not a controversial proposition: both parties agree that “moving” *can* be implemented using “copying.” It is also undisputed that

³ Even if relevant, the statement that “copying” can be implemented by “sharing” does not show that these two, different terms are interchangeable. The process of “sharing” a file means making it accessible to others. Ex. 2004 ¶ 51. This in turn can be used to “copy” that file. *Id.* However, a first computer may, for example, “share” a file by making it accessible to a second computer via a shared network drive, but the second computer may never actually “copy” that file. *Id.*

“moving” can be implemented **without** “copying.” Ex. 2005 at 48:2-4 (“Q. So high-level moving can be done with or without low-level copying. Is that your testimony? A. Yes.”). As addressed below in connection with obviousness, the ’856 patent claims “copying” because it envisions scenarios (such as Figure 1B), where “moving” files without “copying” is not practical. Ex. 2004 ¶¶ 53, 58. In contrast, Petitioner’s cited art does not disclose any such scenario and **only** describes “moving” files **without** copying. *Id.* ¶ 57.

Upon finding that the claimed “copying” was interchangeable with “moving” files, the institution decision concluded that “Burdett disclose this type of copying, as Petition asserts.” ID at 24. Now that a more complete record has demonstrated that “copying” and “moving” are not synonymous and have different meanings, the Board should find that Burdett does **not** disclose the claimed “copying.” After all, even Petitioner’s expert, when asked “Does Burdett [in Ground 1] disclose the claimed copying?,” testified that “Burdett does not.” Ex. 2005 at 44:4-7; *see also* Pet. at 34 (arguing Burdett discloses “**mov[ing]** files” and that “[i]n light of Burdett’s disclosure, it would **also** have been **obvious** to **copy** a clean file,” rather than contending that Burdett discloses “copying” files).

2. Petitioner's Cited Art Does Not Render Obvious the Claimed "Copying"

Since neither Petitioner nor its expert ever alleged that Burdett discloses the claimed "copying," Petitioner instead argues that Burdett's "moving" renders obvious the claimed "copying." That is nonsensical. Burdett's "moving" is implemented by modifying file system directory entries, and thus without any "copying." Modifying Burdett to instead move files by "copying" them would only make Burdett's system *less* efficient, in direct contravention of Burdett's stated goals. Burdett at 1:42-53 ("It is desired to provide protection ... in a manner that is *simple and efficient* and *with minimal performance impact* ...").

In Burdett, both "clean files 308, 310" and "malicious file 312" are maintained in the same "cloud data store 306." Burdett at 26:29-30, 26:55-58. Burdett then describes "mov[ing]" files by "chang[ing] ... the location (*e.g.*, path in a file system) of a file." Burdett at 25:28-31. Since the file remains in the same "file system" in Burdett, "moving" the file can be efficiently implemented without performing any "copying" and instead by modifying file system directory entries. Ex. 2004 ¶ 57. Doing so requires only a minimal amount of processing, and the processing necessary to make the modification is also independent of the particular file being moved (and

thus does not increase with file size). *Id.* Burdett’s description of “changing” a file’s “path in a file system” confirms that Burdett indeed “move[s]” files by modifying the file system directory entries rather than performing any “copying,” as claimed. *Id.*

In contrast, modifying Burdett to “copy” files rather than just “chang[e]” a file’s “path in a file system” would actually make Burdett *less* efficient. Ex. 2004 ¶ 60. The amount of processing required to “copy” a real-word file is more than the amount of processing required to modify file system directory entries, which is akin to changing a pointer, and only increases with file size, since the larger the file, the more data there is to copy. *Id.* ¶¶ 49, 55, 60.

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.”

This is a significant distinction from Petitioner’s cited art combination in Ground 1, where scanned files originate and are subsequently stored back to the same “cloud data store 306.” Burdett at 26:29-30, 26:55-58. Tellingly, Petitioner does not even contend that its Ground 1 combination renders obvious dependent claims 8, 19, and 27, which require “copying” files from the “first repository” in the “public cloud file store” to a “second repository” that “is part of the network security device or part of an external storage device that forms part of the enterprise network” and thereby cover the embodiment of Figure 1B.⁴ Ex. 2004 ¶ 60. Thus, while the ’856 patent recognizes and claims the benefits of “copying” files rather than just “moving” them, those

⁴ As explained in Section VII.C below, Petitioner’s arguments for these dependent claims pursuant to Ground 2 also fail.

benefits are not apparent in other contexts (such as Petitioner’s cited art), where it is preferable to move files without any copying.

Petitioner provides no obviousness analysis to substantiate its conclusory assertion that, “[i]n light of Burdett’s disclosure, it would also have been obvious to copy a clean file to a second repository,” especially since modifying Burdett in this manner would make it ***less efficient***. Pet. at 34. Indeed, Petitioner does not even acknowledge any difference between the cited art’s “moving” and the claimed “copying” (as required under *Graham*), much less address motivation to combine or reasonable expectation of success. Ex. 2004 ¶ 59. Without any obviousness analysis, Petitioner cannot prevail. See *Unigene Labs., Inc. v. Apotex, Inc.*, 655 F.3d 1352, 1360 (Fed. Cir. 2011) (obviousness cannot be shown by “conclusory statements”; “there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness”); *Eli Lilly & Co. v. Teva Pharms. Int’l GmbH*, 8 F.4th 1331, 1348-49 (Fed. Cir. 2021) (“[I]t was, at all times, [Petitioner’s] burden to show that the claims would have been obvious, ***including that a skilled artisan would have had a reasonable expectation of success in achieving the claimed invention.***”).

The declaration of Petitioner’s expert, Dr. Franz, does not cure the lack of obviousness analysis in Petitioner’s petition. 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. This assertion is no replacement for the required obviousness analysis. First, the fact that “moving” **can** be implemented using “copying” is insufficient to show that using “copying” would be obvious. Second, Dr. Franz statement that it would be “obvious” to implement “moving” using “copying” “***in many circumstances***” implicitly admits that there are other “circumstances” where “copying” is **not** obvious. Petitioner’s cited art, Burdett, is one such circumstance. Accordingly, Dr. Franz provides no rationale for why it would be obvious to depart from Burdett’s teachings and instead implement Burdett’s “moving” using the claimed “copying,” when doing so would be **less** efficient than “moving” **without** “copying.” *Id.* ¶ 60.

Dr. Franz’s only other basis for contending that Burdett renders obvious the claimed “copying” is his view that different mechanisms for achieving “the end result” of having “the clean file [be] accessible to the end user” would be obvious. Ex. 2005 at 44:13-24. But leading to the same “end result” is not enough to render a claim obvious. *Ex Parte Colin et al.*, 2012 WL 5387625, at *2-3 (P.T.A.B. Oct. 31, 2012) (finding no “prima facie case of obviousness”

even though cited art “provides an alternative process that accomplishes the same end result” as the patent claims). There are countless mechanisms in the field of computer security for controlling access to files, many innovative in their own right, and it would be nonsensical if Burdett’s reference to “moving” files would somehow automatically render obvious every possible mechanism for making “the clean file [be] accessible to the end user.” See Ex. 2005 at 44:13-24; Ex. 2004 ¶ 61.

Accordingly, Petitioner failed to identify any rationale for modifying Burdett to “copy” a file, and any argument that Burdett renders obvious the claimed “copying” thus fails. See *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1367 (Fed. Cir. 2016) (“[T]he petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable. ... [I]t was [Petitioner’s] burden to explain to the Board how [the combination] rendered the challenged claims unpatentable.”). Moreover, having failed to proffer any rationale for modifying the cited art in its original petition, Petitioner cannot now belatedly come forward with a new rationale for modifying Burdett to arrive at the claimed copying. See *Henny Penny Corporation v. Frymaster LLC*, 983 F.3d 1324, 1330-31 (Fed. Cir. 2019) (“We agree with Frymaster that the Board did not abuse its discretion by holding HPC to the obviousness theory in its petition. ... [A]n IPR petitioner

may not raise in reply “an entirely new rationale” for why a claim would have been obvious.”). Accordingly, Petitioner cannot meet its burden of showing that Burdett (alone or in combination with FortiSandbox) render this limitation obvious.

B. Petitioner Failed to Show It Would Be Obvious to Combine Burdett with FortiSandbox

Petitioner relies on a combination of Burdett and FortiSandbox that allegedly renders obvious the claims of the '856 patent. Petitioner fails, however, to articulate any motivation for its proposed combination, which is counterintuitive, results in multiple disadvantages, is driven by hindsight bias, and thus non-obvious.

The needless complexity of Petitioner’s proposed combination alone demonstrates that Petitioner is driven by improper hindsight bias rather than any recognizable motivation to combine. First, Petitioner is pointing to Burdett’s enterprise facility 102 of Fig. 1 for the claimed “enterprise network” (Pet. at 22-23), and then adding a devices as taught by FortiSandbox to that network or threat management facility 100 (Pet. at 19, 30). Then, Petitioner is modifying the FortiSandbox device to add the capabilities of Burdett’s scanning service 304, thereby moving Burdett’s scanning service 304 from cloud infrastructure 302 to the FortiSandbox device. Pet. at 29-30. Finally,

Petitioner is further modifying Burdett's scanning service 304 to leverage FortiSandbox's native mounting to again give Burdett's scanning service 304 access to the files being scanned in cloud data store 306 in cloud infrastructure 302. Pet. at 30; *see also* Ex. 2004 ¶ 62 (additional overview of proposed combination). Burdett's original solution was much simpler: run scanning service 304 in the same cloud infrastructure 302 as the files it is scanning. Ex. 2004 ¶ 63.

Indeed, moving Burdett's scanning service 304 from its original location in cloud infrastructure 302 to the FortiSandbox device would be ***detrimental*** to the performance of Burdett's system. In Burdett, by hosting scanning service 304 in the same cloud infrastructure 302 that also contains cloud store 306 with the files being scanned, there is no need for any of those files to be transferred across a wide area network for scanning purposes. Ex. 2004 ¶ 65. In contrast, if Burdett's scanning service 304 were implemented on a FortiSandbox device in Burdett's enterprise facility 102 or threat management facility 100, then every file to be scanned would need to be transmitted from cloud infrastructure 302, over a wide area network, to the FortiSandbox for scanning purposes. *Id.* This unnecessary file transfer results in a host of detrimental repercussions:

- Delay in scanning due to time needed for file transfer

- Network congestion due to additional file transfers
- Security risks posed by transferring files across a wide area network
- Management complexities in ensuring FortiSandbox has access to files in cloud data store 306

Id.

None of Petitioner’s proffered motivations to combine justify moving Burdett’s scanning service 304 from the cloud infrastructure 302, as disclosed in Burdett, to a FortiSandbox device. Petitioner entirely fails to address this aspect of its proposed combination. For example, Petitioner argues that FortiSandbox’s teachings of native mounting “explain[] how to configure a device that could be deployed within an enterprise’s network infrastructure to scan files on a network share.” Pet. at 19. But this argument presupposes that Burdett’s scanning service 304 is running on the FortiSandbox device (“a device ... within an enterprise’s network infrastructure”) and does not supply any motivation to move Burdett’s scanning service 304 from its original location in cloud infrastructure 302 to the FortiSandbox device. Ex. 2004 ¶ 64.

Petitioner also contends that adding FortiSandbox’s native mounting to Burdett’s scanning service 304 would allow the scanning service to “access

files” and “controll[] file access.” Pet. at 30. As Dr. Franz admitted in his deposition, however, “Burdett’s scanning service, even without the teachings of FortiSandbox, was able to access files in the cloud file store” and “control access to files in the cloud file store.” Ex. 2005 at 49:19-22, 50:2-5; *see also* Ex. 2004 ¶ 64.

Petitioner also argues that this “would have enabled the network security device to perform scheduled or on-demand bulk scans within the cloud file store.” Pet. ta 30. But again, Burdett already disclosed a “security manager” that identifies new files that need to be scanned and provides notification of such files via an API (Burdett at 28:33-41, 29:31-41, 30:53-56), and Dr. Franz does not allege allowing a remote “network security device” perform a “bulk scan” leads to any advantage over the cloud infrastructure’s existing “security manager” performing that scan and providing the pertinent information to the “network security device” via the existing API. Ex. 2005 at 58:3-16; *see also* Ex. 2004 ¶ 64.

Accordingly, Petitioner has failed to show that it would be obvious to combine Burdett and FortiSandbox in the proposed manner to arrive at the ’856 patent claims. Petitioner has, therefore, not met its burden of showing that the ’856 patent claims are obvious under Ground 1.

VII. RESPONSE TO GROUND 2: SHARPE, SEESE, AND KAMALAPURAM

A. Petitioner Fails to Address the “Copying” Claim Limitation

All independent claims of the ’856 patent require “**copying** the clean file from the first repository to a second repository.” Petitioner acknowledges that “Sharpe did not explicitly describe that the ‘clean’ file would be copied to a second repository” (Pet. at 67) and relies on Kamalapuram for this limitation. But Petitioner’s theory in Ground 2 for this claim limitation suffers from the same defect as its theory in Ground 1: by Petitioner’s own admission, Kamalapuram does not disclose “copying” a file, as claimed, and instead describes “moving” files:

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].) Accordingly, Kamalapuram described **moving** the “clean” file from a first repository (an isolated area of the network storage system) to a second repository (a general area of the network storage system)

Pet. at 67-68.

As addressed in connection with Ground 1, the terms “copying” and “moving” refer to different actions. *See supra*, Section VI.A; Ex. 2004 ¶¶ 48-61, 67-69. Moreover, the Board’s finding that the cited art “satisfies this limitation” was based on an incomplete record and has since been contradicted

by Dr. Franz’s admission on cross-examination that Kamalapuram is silent on whether Kamalapuram’s “moving” entails any “copying,” as required by the claims. Ex. 2005 at 68:8-10 (admitting that “‘moving’ might mean updating a directory ... entry” or “[i]t might mean copying it to another disk and updating a directory entry”); Ex. 2004 ¶ 70.

Moreover, Petitioner’s Ground 2 combination fails to render obvious the claimed “copying” for the same reason as Petitioner’s Ground 1 combination. Petitioner admits that Kamalapuram, like Burdett, only describes “moving” files within “the same storage system.” Pet. at 75. Under these circumstances, it would be nonsensical to implement Kamalapuram’s “moving” using any copying—the much more efficient solution would be to “move” files by changing file system directory entries and thus **without** “copying.” Ex. 2004 ¶¶ 55-58, 69-71. Petitioner’s assertion of obviousness in Ground 2 is not supported by any rationale, nor is there any motivation to modify Kamalapuram to make it **less** efficient. *Id.* ¶¶ 70-71.

Accordingly, Petitioner has not met its burden to show that it would be obvious to modify Kamalapuram or any of the other Ground 2 art to arrive at the specific “copying” step required by all ’856 patent claims. *See Unigene*, 655 F.3d at 1360; *Harmonic*, 815 F.3d at 1367.

B. Petitioner Failed to Show It Would Be Obvious to Combine Sharpe With Seese

Similar to Ground 1, Petitioner’s Ground 2 combination is driven by hindsight bias, is detrimental to system performance, and thus far from obvious. Most significantly, Petitioner proposes moving Sharpe’s malware scan from Sharpe’s cloud storage provider environment 4210 to Seese’s DLP server, which is located outside the alleged “public cloud file store.” Pet. at 53; *see also* Pet. at 53 (“Seese’s DLP server was a physical device deployed within an enterprise’s network infrastructure”); Pet. at 63 (“Seese disclosed a data loss prevention (DLP) server as an example type of a network security device”). And because Petitioner is relying on Sharpe for the claimed “public cloud data store” (Pet. at 57), Petitioner then alleged that it would have been obvious to “natively mount” Sharpe’s “cloud storage system” onto Seese’s alleged “network security device” (Pet. at 63 (discussing “mount[ing] the user share to the DLP server described by Seese”)). *See also* Ex. 2004 ¶ 72.

Petitioner’s combination in Ground 2 suffers from the same basic defect as its combination in Ground 1: there is no rational basis (other than hindsight) for moving Sharpe’s malware scan from cloud storage provider environment 4210 onto Seese’ DLP server “deployed within an enterprise’s network infrastructure” (Pet. at 53). Ex. 2004 ¶ 73. Doing so would make Sharpe’s

malware scan **worse** by needlessly require transferring files from Sharpe's cloud storage provider environment 4210 containing cloud storage system 302 to Seese's DLP server for processing, resulting in delay, network congestion, increased security risk, and greater system management complexity. *Id.* ¶ 76. The more efficient solution, as already described in Sharpe and contrary to Petitioner's obviousness combination, would be just to run Sharpe's malware scans directly in the same cloud storage provider environment 4210 that already contains cloud storage system 302 and thus the files being scanned. *Id.* ¶¶ 73, 76.

Unsurprisingly, none of Petitioner's proposed motivations for combining the cited art in Ground 2 actually improve on the operation of Sharpe's malware scan alone. For example, Petitioner states "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." Pet. at 53. But even if adding Seese's DLP server to Sharpe's network would have helped preserve privacy, that is not a motivation to then move Sharpe's malware scans from the cloud onto that server. Ex. 2004 ¶ 74. DLP and malware scanning are two different processes, and there is no need for them to be deployed on the same server. *Id.* Indeed, it makes sense for DLP discovery software to be

deployed on a server at the periphery of an enterprise network to monitor data and documents being transmitted outside that network, since preventing unauthorized transmission of sensitive data and documents is a core aspect of DLP. *Id.* In contrast, it makes sense for the malware scan to be deployed in the same cloud storage provider environment as the files being scanned so as minimize file transfers and maximize efficiency. *Id.*

Petitioner also writes “[i]t 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.**” Pet. at 64. But as Dr. Franz confirmed in his deposition, Sharpe’s malware scan (even without the teachings of Seese) was able to “access files in the cloud file store” and “control[] access to the files.” Ex. 2005 at 66:9-19; *see also* Ex. 2004 ¶ 75.

Thus, Petitioner’s proposed changes to Sharpe, and especially Petitioner’s proposal to move 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. Ex. 2004 ¶ 76. Accordingly, Petitioner failed to

articulate a valid rationale for its combination of art cited in Ground 2 and its obviousness theory fails.

C. Petitioner Failed to Show Unpatentability of Dependent Claims 8, 19, and 27

Petitioner only challenges dependent claims 8, 19, and 27 in the context of Ground 2 (these claims are not challenged in Grounds 1 and 3). But even under Ground 2, Petitioner’s invalidity argument for claims 8, 19, and 27 fails.

Claims 8, 19, and 27 require that “a first repository” be part of “a public cloud file store” (see claims 1, 13, 21, from which they depend) and that “clean file[s]” then be copied to “a second repository” that is “part of the network security device or part of an external storage device that forms part of the enterprise network” (see claims 8, 19, and 27). Ex. 2004 ¶ 78. In Petitioner’s obviousness combination, this “network security device” allegedly corresponds to Seese’s “DLP server” (Pet. at 63), which is “deployed within an enterprise’s network infrastructure” (Pet. at 53) and thus outside the alleged “public cloud store.” Ex. 2004 ¶ 78. Similarly, the claimed “external storage device that forms part of the enterprise network” is according to Petitioner also outside the claimed “public cloud file store,” since Petitioner contends that the term “public cloud file store” by definition “refers

to a file store maintained on shared infrastructure, *as opposed to an enterprise's private infrastructure.*" Pet. at 24; Ex. 2004 ¶ 78.

Thus, to prevail, Petitioner would need to show its combination of cited art renders obvious taking a file from a "public cloud file store" and (after determining the file is clean) copying the file to storage outside that "public cloud file store." Ex. 2004 ¶ 79. Petitioner fails to make any such showing.

First, none of Petitioner's cited art discloses this limitation. Ex. 2004 ¶ 80. In Sharpe, all files, both before and after scanning, are stored in the same "cloud storage system 302," and access is controlled via metadata. Pet. 51 ("If the file was deemed clean, the cloud controller would update the metadata, if infected, the file could be removed, quarantined, or marked."); *see also* Pet. at 59, 68; Sharpe at Fig. 42. Petitioner does not rely on Seese for any aspect of the "copying" limitation; thus, Seese necessarily does not teach copying (or even moving) files from a public cloud file store to outside that public cloud file store. Pet. at 67 ("Sharpe and Kamalapuram disclosed [the 'copying'] limitation [1[e]]."). And Kamalapuram, as Petitioner admits, "taught or suggested that the first and second repositories were in the same storage system." Pet. at 75. Thus, none of Petitioner's cited art discloses copying (or even moving) a "clean" file from a "public cloud file store" to outside that "public cloud file store." Ex. 2004 ¶ 80.

Second, Petitioner presents no rationale for departing from the teachings of its own cited art. At best, Petitioner cites the disclosure in Seese of “hybrid cloud storage,” ***but that is not the type of cloud storage system relied on by Petitioner in its obviousness combination.*** Pet. at 62-63 (arguing Seese “not only described mounting a ***public*** cloud file system in the context of scanning the files to protect an enterprise against data loss, but also described mounting the ***public*** files on a network security device”). Moreover, merely implementing Petitioner’s proposed combination in the context of “hybrid cloud storage” is not a rationale for then “copying” (or even moving) files from the “public” portion of that cloud storage to the “private” portion of that cloud storage. Ex. 2004 ¶ 81. Finally, Petitioner’s argument that the proposed modification would somehow “improve[] security of files” based on “the importance of the data” does not hold up to logic. Pet. at 76. If a file is sufficiently “importan[t]” to warrant storing within the “enterprise network,” then it would not have been stored to a “first repository” in a “public cloud file store” in the first instance. Ex. 2004 ¶ 81. Conversely, if it is permissible to store a file in a “public cloud file store” initially, then there is no drawback to allowing the file to remain there after it is confirmed cleaned. *Id.* Thus, consistent with Petitioner’s own cited art, Petitioner’s rationale

would actually counsel ***against*** “copying” a “clean” file from a “public cloud file store” to outside that “public file store.”

Third, the totality of the Petition demonstrates that Petitioner’s proposal to modify the Ground 2 art to copy files from a “public cloud file store” to outside that “public file store” is based on hindsight bias. For purposes of dependent claims 8, 19, and 27, Petitioner’s Ground 1 and Ground 2 art is substantively identical. Ex. 2004 ¶ 82. In Ground 1, similar to Ground 2, the alleged “clean files” remain within the same “cloud data store 306.” Burdett at 26:29-30, 26:55-58. Petitioner does not contend the Ground 1 art renders obvious dependent claims 8, 19, and 27. Yet when confronted with substantively the same disclosure in Ground 2, where “Kamalapuram taught or suggested that the first and second repositories were in the same storage system” (Pet. at 75), Petitioner contends that substantively the same disclosure renders obvious dependent claims 8, 19, and 27. There is no basis for treating Petitioner’s Ground 1 art differently from its Ground 2 art. Ex. 2004 ¶ 82. Neither combination of cited art discloses or renders obvious the ’856 patent’s claims 8, 19, and 27.

VIII. GROUND 3

Petitioner’s Ground 3 cited art allegedly discloses the additional limitations of dependent claims 3, 6, 11, 15, 17, 23, and 25 of the ’856 patent,

but does not purport to cure the deficiencies of Ground 2 with respect to the independent claims. Thus, Ground 3 fails for the same reasons as Ground 2.

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.

IX. CONCLUSION

For the foregoing reasons, Patent Owner respectfully requests that the Board affirm that validity of the challenged '856 patent claims.

Date: December 12, 2023

By: /s/ James Glass
James M. Glass (Reg. No. 46,729)
QUINN EMANUEL URQUHART &
SULLIVAN LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
Email: jimglass@quinnemanuel.com
Phone: 212-849-7142
Fax: 212-849-7100

Counsel for Patent Owner
Fortinet, Inc.

CERTIFICATE OF LENGTH (37 C.F.R. §§ 42.24)

The undersigned hereby certifies that, according to the word-processing system used to prepare the foregoing document, this document has 7,795 words and thus complies with the applicable word limit.

Date: December 12, 2023

By: /s/ James Glass
James M. Glass (Reg. No. 46,729)
QUINN EMANUEL URQUHART &
SULLIVAN LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
Email: jimglass@quinnemanuel.com
Phone: 212-849-7142
Fax: 212-849-7100

*Counsel for Patent Owner
Fortinet, Inc.*

CERTIFICATE OF SERVICE (37 C.F.R. §§ 42.6(E), 42.105(A))

The undersigned hereby certifies that the foregoing document was served in its entirety on December 12, 2023 upon the following parties via Electronic Mail:

Thomas N. Millikan (millikan-ptab@perkinscoie.com)
Babak Tehrani (tehranchi-ptab@perkinscoie.com)
Andrew N. Klein (klein-ptab@perkinscoie.com)
Wei Yuan (yuan-ptab@perkinscoie.com)
Netskope-FortinetIPRTeam@perkinscoie.com

Date: December 12, 2023

By: /s/ James Glass
James M. Glass (Reg. No. 46,729)
QUINN EMANUEL URQUHART &
SULLIVAN LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
Email: jimglass@quinnemanuel.com
Phone: 212-849-7142
Fax: 212-849-7100

*Counsel for Patent Owner
Fortinet, Inc.*