

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'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. OVERVIEW OF THE '856 PATENT	3
III. OVERVIEW OF CERTAIN CITED ART	6
A. Ground 1 Cited Art.....	6
1. U.S. Patent No. 11,281,775 (“Burdett”) (Ex. 1004)	6
2. FortiSandbox (Ex. 1005)	9
B. Ground 2 Cited Art.....	9
1. U.S. Patent No. 9,811,662 (“Sharpe”) (Ex. 1006).	9
2. U.S. Patent Appl. Pub. No. 2015/0100357 (“Seese”) (Ex. 1007)	11
3. U.S. Patent Appl. Pub. No. 2020/0050686 (“Kamalapuram”) (Ex. 1008)	12
IV. LEVEL OF ORDINARY SKILL IN THE ART	13
V. CLAIM CONSTRUCTION	13
VI. Response to Ground 1: Burdett and FortiSandbox.....	14
A. Petitioner Fails to Address the “Copying” Claim Limitation	14
B. Petitioner Failed to Show Burdett and FortiSandbox Disclose or Render Obvious “Natively Mount[ing]” a “Public Cloud File Store” on a “Network Security Device”	18
1. No alleged prior art reference discloses “natively mount[ing]” a “public cloud file store” on a “network security device”	19

2.	Petitioner failed to show it would be obvious to combine Burdett with FortiSandbox.....	23
C.	Petitioner Improperly Combines Different Embodiments of Burdett Without Performing Any Obviousness Analysis.....	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 Alleged Prior Art Disclose or Render Obvious “Natively Mount[ing]” a “Public Cloud File Store” on a “Network Security Device”	33
1.	No alleged prior art reference discloses “natively mount[ing]” a “public cloud file store” on a “network security device”.....	34
2.	Petitioner failed to show it would be obvious to combine the alleged prior art	37
VIII.	GROUND 3	40
IX.	CONCLUSION	41

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. INTRODUCTION

The Board should deny institution of *inter partes* review of U.S. Patent No. 11,036,856 (the “’856 patent”) because Petitioner’s invalidity grounds re-write or ignore claim limitations and oversimplify the alleged prior art.

First, Petitioner failed to conduct any obviousness analysis for the limitation “copying the clean file from the first repository to a second repository.” Notwithstanding the clear recitation of “copying,” Petitioner treats the claims as if they required “moving” files. Petitioner’s cited art, according to Petitioner’s own characterization, only discloses “moving” files from one location to another. “Moving” and “copying” are two different actions, as confirmed by the fact that the ’856 patent claims use both verbs in different limitations. Petitioner completely ignores this difference and provides no obviousness analysis to show that the cited art’s “moving” somehow renders obvious the claimed “copying.” In fact, Petitioner does not even acknowledge that there is any difference between these two verbs, thereby failing to perform one of the most basic steps in any obviousness analysis: “ascertain[ing]” the “differences between the prior art and the claims at issue.” *See Graham v. John Deere Co.*, 383 U.S. 1, 17 (1996).

Second, Petitioner ignores the word “public” in the limitation “the public cloud file store is natively mounted on a network security device.”

Petitioner admits that this limitation is not taught by either of its primary references (Burdett in Ground 1; Sharpe in Ground 2) but contends it is disclosed in secondary references (FortiSandbox in Ground 1; Seese in Ground 2). Petitioner fails to demonstrate, however, that either of its secondary references discloses or renders obvious “natively mount[ing]” a “**public** cloud file store” as opposed to, e.g., a private cloud file store. “natively mount[ing]” a “public cloud file store” on an entity’s “network security device” presents additional compatibility and privacy challenges that are not applicable when an entity “natively mount[s]” its private cloud file store on its own “network security device.” Thus, Petitioner’s secondary references do not cure the defects in Petitioner’s primary references.

Third, for Ground 1, Petitioner’s theory improperly combines two different embodiments from Burdett without conducting the necessary obviousness analysis. For the “enterprise network” limitation, Petitioner cites Burdett’s Figure 1, which depicts a traditional facilities-based infrastructure. In contrast, for the “public cloud file store” limitation, Petitioner cites to Burdett’s Figure 3, which depicts a cloud-based infrastructure. None of the elements in Burdett’s Figure 1 are repeated in its Figure 3, and vice versa, and more generally there is no cited evidence Burdett’s Figures 1 and 3 are part of the same embodiment. Petitioner ignores this aspect of Burdett, however,

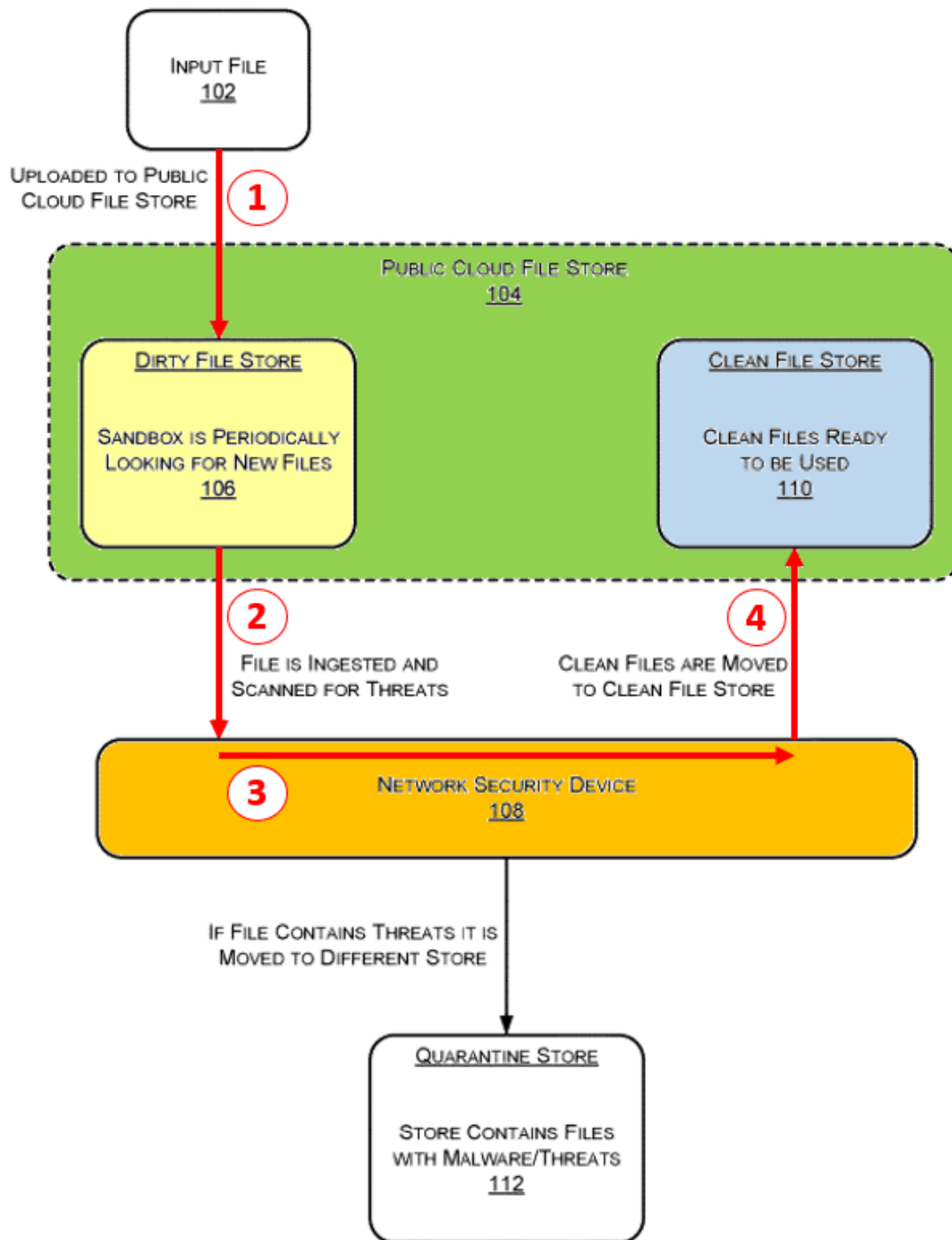
fails to analyze whether it would be obvious to combine these two embodiments from Burdett, instead treating them (incorrectly) as if they were part of the same embodiment.

For all these reasons, as well as others discussed below, Petitioner fails to meet its burden and the Board should deny institution of *inter partes* review.

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 2.¹

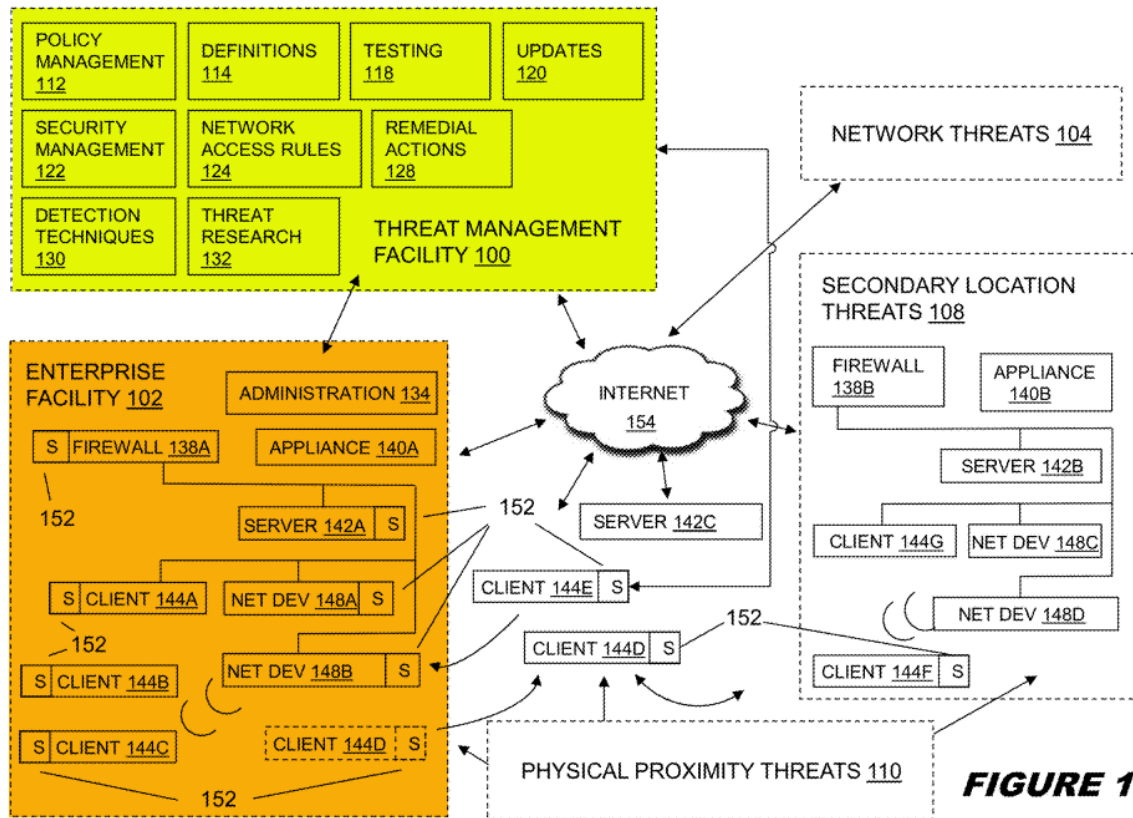
A. Ground 1 Cited Art

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

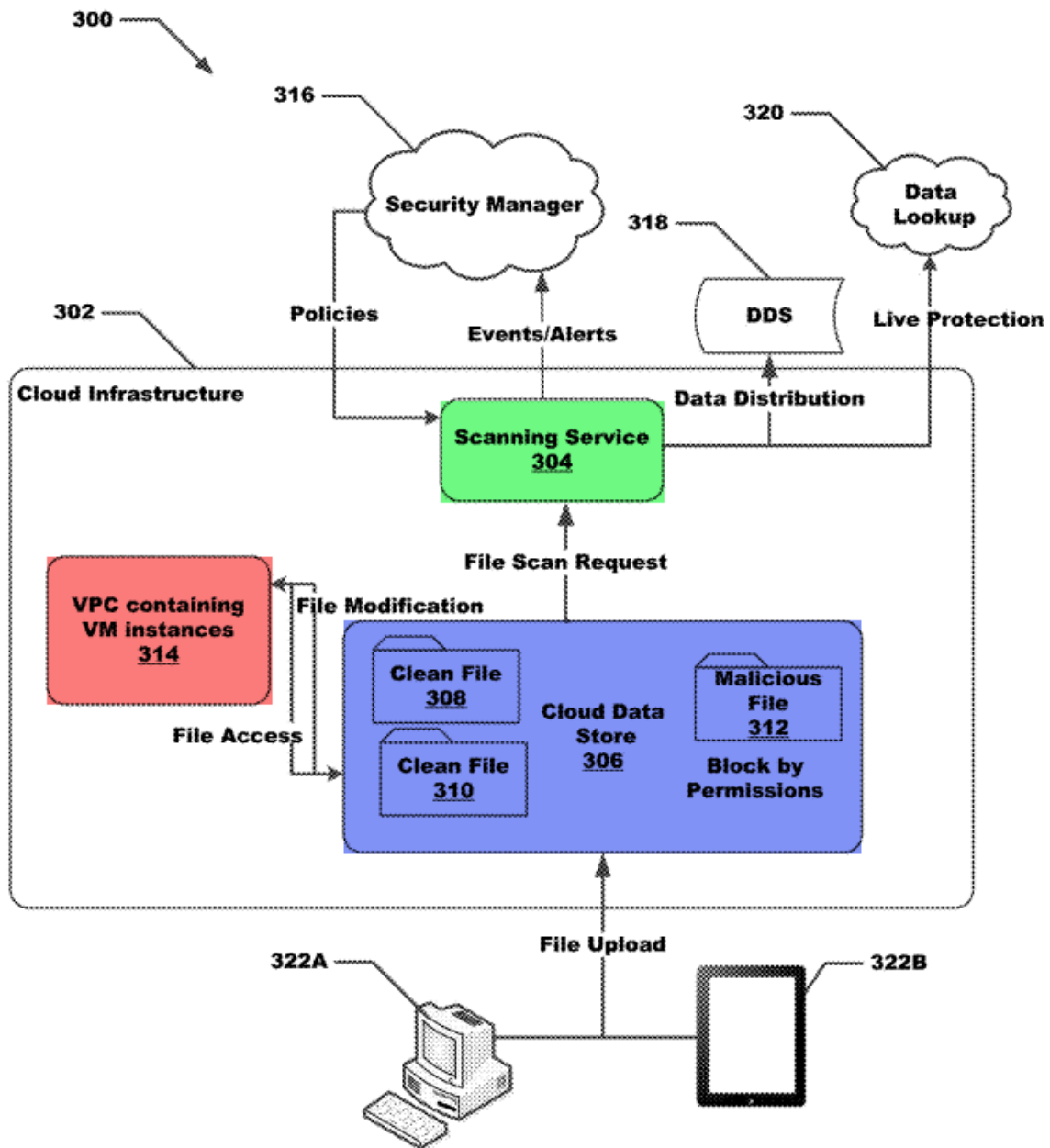
Burdett describes two separate embodiments (Figure 1 and Figure 3) that are relevant to Petitioner's Ground 1.

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.

¹ 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:

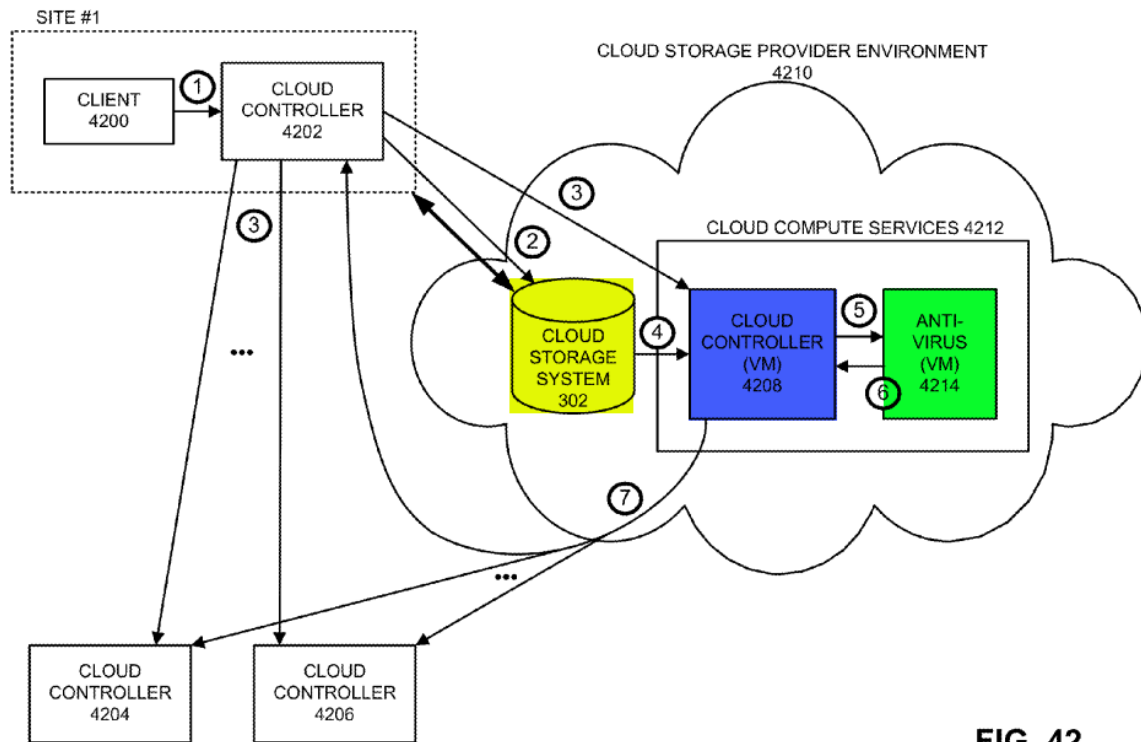
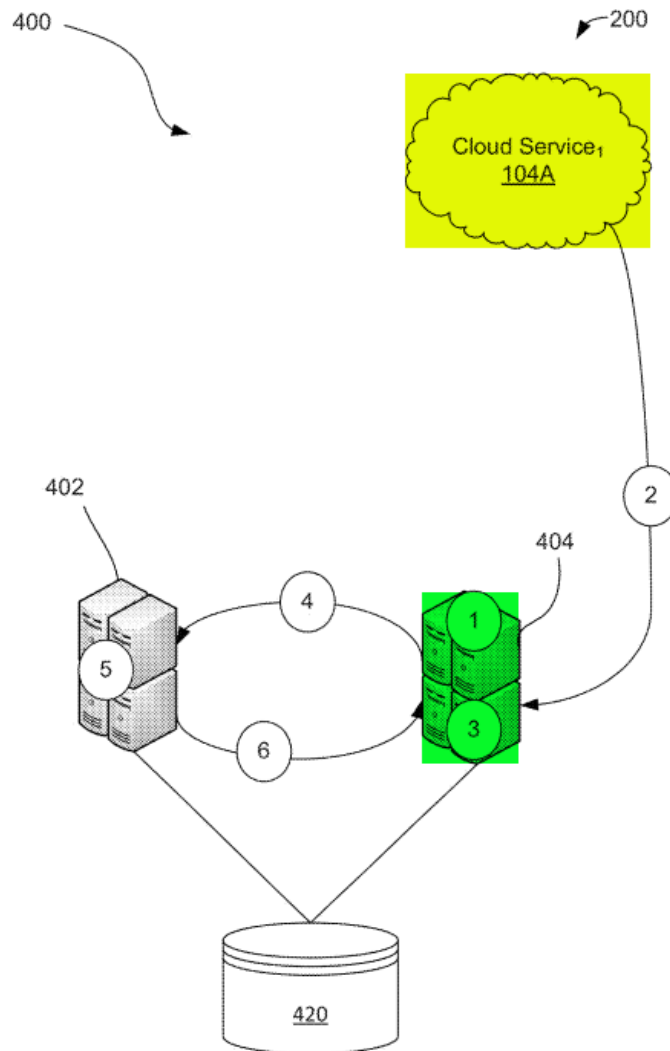


FIG. 42

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].

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.” Petitioner ignores the claim language as written and alleges that Burdett’s “*mov[ing]*” of a file somehow meets the “copying” limitation without providing any analysis to justify Petitioner’s departure from the clear language of the claims.

The relevant limitation of the ’856 patent independent claims uses clear language to require “*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. The terms “copying” and “moving” have different meanings and require that different actions be performed on files—copying vs. moving. Ex. 2001 (“Black Decl.”) ¶ 46; 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 second copy of portions of that information. Black Decl. ¶ 46. In contrast, the plain meaning of “moving” merely requires changing the location of the information independent of any particular mechanism for doing so. *Id.*

That a file has been “moved” does not alone disclose or render obvious “copying” the file, since it is possible to change a file’s location by modifying the file system structure (thereby “moving” the file within that structure) without ever creating a second copy of even portions of that file (i.e., without any “copying”). Black Decl. ¶ 47. For example, the “mv” command in POSIX systems uses a “rename” system call to modify the file directory entries, thereby “moving” the file to a new location with the file system without any “copying.” *Id.*

Indeed, there are in some instances good reasons to “move” a file without performing any “copying.” Black Decl. ¶ 48. For example, “moving” a file by modifying the file system structure generally requires only a constant amount of processing, since the processing necessary to make the modification is independent of the particular file being moved (and thus also independent of the file’s size). *Id.* In contrast, the amount of processing required to “copy” a file generally increases linearly with file size, since the larger the file, the more data there is to copy. *Id.* Accordingly, there are good

reasons in some instances to “move” a file, as described in Petitioner’s cited art, without performing any “copying,” as required by the ’856 patent claims.

Petitioner ignores this distinction between “copying” and “moving” files. Petitioner states that Burdett describes “changing the storage location of the file” based on Burdett’s disclosure that “the scanning service may move files ... in order to control access.” Pet. at 33 (quoting Burdett at 25:26-27). Petitioner then concludes that, “[g]uided by Burdett, a POSITA would have found it obvious that one alternative to control access to a contaminated file was to **move** the file to a different location.” Pet. at 33. But Burdett’s teaching of “mov[ing]” files does not include any “copying,” as claimed. Black Decl. ¶¶ 49-50. Rather, Burdett explains it “move[s]” 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 the reference to “changing” a file’s “path in a file system” further confirms that Burdett “move[s]” files by modifying the file system’s directory entries rather than performing any “copying,” as claimed. *Id.* ¶ 50.

Since Burdett teaches “moving” rather than “copying” files, it was Petitioner’s burden to show that Burdett’s “moving” somehow renders obvious the claimed “copying.” Petitioner fails to meet that burden. Other

than the 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 ” (Pet. at 34), Petitioner provides no analysis or explanation of how or why Burdett’s teaching of “mov[ing]” files or any part of that process meets the claim limitation requiring “copying” files or renders that limitation obvious. See Black Decl. ¶ 51. 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. 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”).²

² Petitioner’s expert, Dr. Franz, generally just repeats Petitioner’s argument, and any additional arguments in Dr. Franz’s declaration should not be considered. See *Cisco Sys., Inc. v. C-Cation Techs., LLC*, IPR2014-00454, Paper 12, at 9-10 (PTAB August 29, 2014) (designated informative) (“Th[e] practice of citing the Declaration to support conclusory statements that are not otherwise supported in the Petition ... amounts to incorporation by reference. ... [W]e will not consider arguments that are not made in the Petition, but are instead incorporated by reference to the cited paragraphs ... of [the expert’s] Declaration.”).

Since Petitioner failed to conduct the necessary obviousness analysis, no further showing by Patent Owner is necessary to warrant denying the petition. *See Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1367 (Fed. Cir. 2016) (“In an IPR, the 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 prior art combination] rendered the challenged claims unpatentable.”). Having ignored the claim language as written—specifically, the clear requirement of “*copying*” files—Petitioner cannot meet its burden of proof on this limitation.

B. Petitioner Failed to Show Burdett and FortiSandbox Disclose or Render Obvious “Natively Mount[ing]” a “Public Cloud File Store” on a “Network Security Device”

All independent claims of the ’856 patent require a “public cloud file store [that] is natively mounted on a network security device.” According to Petitioner, this “‘public cloud file store’ being ‘natively mounted on a network security device’ was ‘the very limitation Applicant argued was missing in McErlean to obtain allowance.’ Pet. at 13-14. Yet tellingly, Petitioner’s cited references fare no better than the art considered during prosecution, since Petitioner’s art also fails to disclose or render obvious that same limitation.

In particular, Petitioner acknowledges that a “public cloud file store” is a specific type of “cloud file store” but then glosses over the distinction

between “public” and other types of cloud file stores, such as a private cloud file store. This is fatal to Petitioner’s Ground 1. Petitioner relies on FortiSandbox for this limitation, but Petitioner’s contention is unsupported by any evidence or analysis showing FortiSandbox works with a “**public** cloud file store.” Petitioner’s Ground 1 fails for that reason alone. Even if the petition is interpreted as relying on a combination of Burdett and FortiSandbox for the “natively mount[ing]” a “public file store” limitation, Petitioner fails to explain why a POSITA would have a reasonable expectation of success or be motivated to apply FortiSandbox’s teachings regarding generic “cloud file store[s]” to Burdett’s alleged “public cloud file store.”

1. No alleged prior art reference discloses “natively mount[ing]” a “public cloud file store” on a “network security device”

Petitioner states “Burdett did not explicitly describe mounting the public file store on a network security device, but FortiSandbox did.” Pet. at 28; *see also* Franz Decl. ¶ 85 (“Burdett did not explicitly describe natively mounting the public file store, but FortiSandbox disclosed this operation.”). Thus, Petitioner’s theory is that FortiSandbox allegedly discloses “natively mount[ing]” the claimed “public cloud file store.” Petitioner’s theory is unsupported by any evidence or analysis, and on that basis should be rejected.

Every word in the claim language should be given meaning, and in the case of the '856 patent claims, the word “public” distinguishes a “public cloud file store” from other types of “cloud file store[s]” such as a private cloud file store. See Black Decl. ¶ 53; *see also Akzo Nobel Coatings, Inc. v. Dow Chem. Co.*, 811 F.3d 1334, 1339-40 (Fed. Cir. 2016) (construing “pressurized collection vessel” to give meaning to the word “collection”). Even Petitioner agrees that the term “public cloud file store” has a specific meaning, arguing that “a ‘public cloud file store’ generally refers to a file store maintained on shared infrastructure, as opposed to an enterprise’s private network.” Pet. at 24.³ Thus, there is no dispute that not every “cloud file store” is necessarily a “**public** cloud file store.”

In the case of FortiSandbox, other than an unsupported assertion that “FortiSandbox disclosed this operation” (Franz Decl. ¶ 85), Petitioner presents no evidence or analysis that FortiSandbox’s “network share” corresponds to a “**public** cloud file store.” Black Decl. ¶ 54. FortiSandbox describes “five methods for importing files” that are then scanned for known

³ The PTAB need not resolve the accuracy of Petitioner’s proffered construction to reject its petition, and for that reason Patent Owner reserves the right to present an alternative construction if this IPR is instituted. For purposes of evaluating the Petition, it is suffice to note that the parties agree that the term “public” must be given meaning.

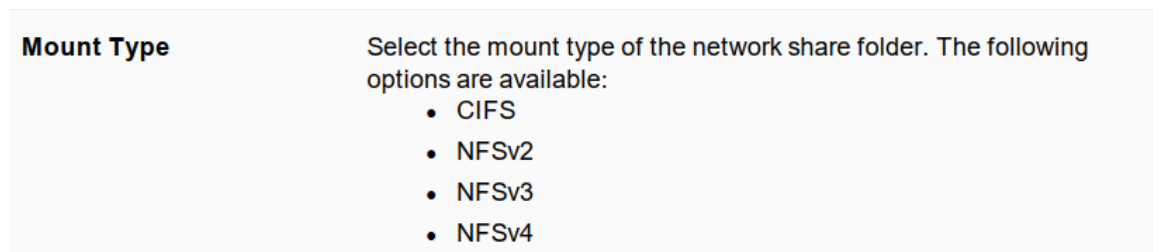
threats, including “network share.” FortiSandbox at 88. “Network share allows you to scan files located on a remote file share as scheduled, and quarantine bad files.” *Id.* To use this feature, the user specifies a “Server Name/IP,” a “Share Path,” and a “Mount Type.” *Id.* at 115. Absent from Petitioner’s analysis is any basis for alleging that FortiSandbox’s “remote file share” corresponds to a “public cloud file store” such that mounting a “file share” discloses “natively mount[ing]” a “**public** cloud file store,” as claimed.

The only analysis by Petitioner is that “FortiSandbox’s use of mount types including CIFS and NFS protocols” mirrors the ’856 patent’s use of “NFS” and “CIFS.” Pet. at 29 (quoting ’856 patent at 11:7-10).⁴ However, even if the ’856 patent were to disclose that use of “NFS” and “CIFS” were part of the technology used to “natively mount[]” a “public cloud file store,” use of those protocols alone is not sufficient to disclose this claim limitation. Black Decl. ¶¶ 55, 60. For example, the ’856 patent identifies specific software “for mounting an Amazon Web Services (AWS) Simple Storage Service (S3) bucket” as opposed to relying solely on generic protocols such

⁴ Petitioner’s expert merely repeats arguments from the Petition and does not provide any additional analysis. Franz Decl. ¶¶ 85-89. At most, Dr. Franz asserts that “CIFS and NFS” were “protocols used to access files across a network, and in particular to access files from cloud storage” but also fails to address FortiSandbox’s lack of disclosure on using these protocols to natively mount a “**public** cloud file store.” See *id.* ¶ 86.

as NFS and CIFS. ’856 patent at 5:28-32. Thus, the mere overlapping references to NFS and CIFS are insufficient to show that FortiSandbox discloses “natively mount[ing]” a “public cloud file store.”

Subsequent developments in Patent Owner’s FortiSandbox product line further confirm that the FortiSandbox reference cited by Petitioner does not, without more, disclose “natively mount[ing]” a “public cloud file store.” Black Decl. ¶¶ 56-58. Petitioner’s FortiSandbox reference corresponds to FortiSandbox version 2.3.2 released (according to Petitioner) in 2016. FortiSandbox at 1; Pet. at 18 n.5. The only available “mount type[s]” in FortiSandbox version 2.3.2 were “CIFS” and “NFSv2” to “v4”:



By FortiSandbox version 4.2.4, released in 2023—after the ’856 patent’s priority date—FortiSandbox included “mount type[s]” expressly corresponding to “public cloud file store[s],” such as Amazon Web Services (“AWS”) and Microsoft Azure:

Mount Type	Select the mount type. The following options are available: • CIFS (SMB v1.0, v2.0, v2.1, v3.0). • NFSv2, NFSv3, NFSv4. • AWS S3, AWS S3 BJ, AWS S3 NX. See AWS S3 Settings on page 100. • Azure File Share. See Azure File System on page 101. • Azure Blob Storage. See Azure Blob Storage on page 101. For domain-based DFS namespaces, ensure the domain name can be resolved with the system Primary DNS server.
-------------------	---

Ex. 2003 at 74.

The addition of express support for “public cloud file store[s]” as “mount type[s]” in FortiSandbox version 4.2.4 shows that the FortiSandbox reference for version 2.3.2 (without more) does not itself disclose the claim limitation of “natively mount[ing]” a “public cloud file store,” as claimed.

Accordingly, Petitioner’s invalidity theory is that FortiSandbox discloses “natively mount[ing]” a “public cloud file store,” but Petitioner has not actually shown that FortiSandbox discloses this limitation. Thus, Petitioner’s theory fails.

2. Petitioner failed to show it would be obvious to combine Burdett with FortiSandbox

Petitioner’s invalidity theory is that FortiSandbox alone discloses the “natively mount[ing]” a “public cloud file store” on a “network security device” limitation. Pet. at 28 (“Burdett did not explicitly describe mounting the public file store on a network security device, *but FortiSandbox did.*”); Franz Decl. ¶ 85 (“Burdett did not explicitly describe natively mounting the public file store, but *FortiSandbox disclosed this operation.*”). Because it

does not, Petitioner's invalidity theory fails. But even if Petitioner's theory were interpreted as relying on a combination of both Burdett and FortiSandbox for this limitation, Petitioner has not met its burden of showing that it would be obvious to apply FortiSandbox's alleged teaching of "natively mount[ing]" to Burdett's alleged teaching of a "public cloud file store."

First, Petitioner has not met its burden of showing a reasonable expectation of success for any such hypothetical combination. *See 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 extent of Petitioner's "reasonable expectation of success" analysis is a single sentence asserting that "[a] POSITA would have been motivated to combine Burdett and FortiSandbox with a reasonable expectation of success." Pet. at 19; *see also* Franz Decl. ¶ 70 (repeating same sentence verbatim). A bald assertion the legal standard is met is insufficient to meet Petitioner's burden, especially since "natively mount[ing]" a "public cloud file store" on a "network security device" raises compatibility and privacy challenges not present when interfacing with a private cloud file store maintained by the same entity as the claimed "network security device." Black Decl. ¶ 60.

Second, Petitioner has not met its burden of identifying any motivation for applying FortiSandbox’s alleged “native[] mount[ing]” to Burdett’s alleged “public cloud file store.” See *Hulu, LLC v. Sound View Innovations, LLC*, IPR2018-00582, Paper 34, at 16 (PTAB Aug. 5, 2019) (designated informative) (finding claims non-obvious where “Petitioner’s proffered reasoning to combine the references is inadequate”). Petitioner argues combining Burdett and FortiSandbox “would have enabled the network security device to access files in the cloud file store and to natively communicate with the cloud file store to perform actions such as controlling file access” and “would have enabled the network security device to perform scheduled or on-demand bulk scans within the cloud file store.” Pet. at 30. But Burdett’s scanning service already disclosed “controlling file access” **without** natively mounting its alleged “public cloud file store,” and the ability of Burdett’s scanning service to “perform scheduled or on-demand bulk scans” is already providing by giving it “permissions to enable it to access files” without any “natively mount[ing].” Burdett at 25:27-28 (“[T]he scanning service may move files or change the name of files in order to control access.”); Burdett at 27:38-40; Black Decl. ¶ 61. Because the alleged base prior art reference already had the capabilities cited by Petitioner as alleged

motivation to combine, Petitioner has not met its burden of showing it would be obvious to combine these references.

Separately, Petitioner argues that “[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. at 19. But this alleged benefit goes to the scanning capabilities of FortiSandbox and does not constitute motivation for adding FortiSandbox’s alleged “native[] mount[ing]” to Burdett. Black Decl. ¶ 62. Thus, Petitioner’s purported motivation to combine is insufficient to meet its burden of showing it would be obvious to combine these references.

Third, Petitioner’s failure to adequately address reasonable expectation of success and motivation to combine is especially glaring in light of evidence that technology for natively mounting a generic network share (such as NFS and CIFS) is not, without more, sufficient for natively mounting a “public cloud file share.” Specifically, approximately seven years passed between FortiSandbox version 2.4.2 cited by Petitioner, which supported NFS and CIFS protocols, and FortiSandbox version 4.2.4, which had express “mount type[s]” for a “public cloud file share.” *Compare* FortiSandbox at 83 *with* Ex. 2003 at 74; *see also* Black Decl. ¶ 63. If it were obvious to modify

FortiSandbox to permit for the native mounting of a “public cloud file share,” Patent Owner would have done so years earlier.

Accordingly, even if the Petition were interpreted to allege it were obvious to combine FortiSandbox and Burdett to arrive at the “natively mount[ing]” a “public cloud file store” limitation, Petitioner has failed to meet its burden on any such hypothetical obviousness theory.

C. Petitioner Improperly Combines Different Embodiments of Burdett Without Performing Any Obviousness Analysis

All independent claims require “an enterprise network,” a “public cloud file store,” and “prevent[ing]” or “protect[ing]” users of the “enterprise network” from accessing files in the “public cloud file store.” To arrive at these limitations, Petitioner attempts to combine Burdett’s Figure 1 (allegedly showing an “enterprise network”) with Burdett’s Figure 3 (allegedly showing a “public cloud file store”). Entirely absent from Petition, however, is any analysis showing Burdett’s Figures 1 and 3 describe the same embodiment (they do not) or showing that it would be obvious to combine those embodiments.

Independent claim 1 requires “prevent[ing] users of an enterprise network from accessing malware infected files that are stored within public cloud file stores.” For the recitation of “enterprise network,” Petitioner cites

Burdett at column 5:29-31, 7:14-16, and 14:18-21 (Pet. at 22-23) and specifically quotes discussion of “threat management facility 100 ... provid[ing] threat protection to the enterprise facility 102, where the enterprise facility 102 may include a plurality of network components” (Burdett at 14:18-21).

In contrast, for the “mechanism to prevent distribution of malware files *within a cloud repository*,” Petitioner cites Burdett at column 25:26-28, 25:55-67, 26:44-58, 29:31-36, 29:58-61 (Pet. at 23 (emphasis added)). This discussion in Burdett corresponds to Figure 3 and specifically “scanning service 304” that restricts “applications in the [virtual private cloud or VPC] 314” from accessing files in “cloud data store 306.” Burdett at 25:47-55.

Petitioner then assumes—without demonstrating—that the discussion of “prevent[ing] users ... from accessing malware infected files” in connection with Figure 3 applies to Burdett’s “enterprise network” of Figure 1. Pet. at 23; *see also* Black Decl. ¶¶ 65-66. There is no support for Petitioner’s assumption. Figure 1 depicts a traditional (i.e., not cloud-based) “networked computer-based infrastructure” (Burdett at 6:35-40), whereas Figure 3 depicts a separate “cloud infrastructure 302” (Burdett at 23:33-34).

None of Petitioner’s cited portions of Burdett⁵ state that the “scanning service 304” of Figure 3 can be used to restrict access to files by the “networked components” of “enterprise facility 102” in Figure 1. Similarly, Petitioner has not shown that the “networked components” of Burdett’s “enterprise facility 102” in Figure 1 can be implemented as “applications running in the VPC 314” of Figure 3. *See* Black Decl. ¶ 67.

Since Petitioner is relying on Burdett’s teachings pertaining to two separate embodiments, Petitioner was required to conduct the proper obviousness analysis to demonstrate it would have been obvious to combine Burdett’s embodiment of Figure 1 with its embodiment of Figure 3. *See Microsoft Corp. v. Biscott, Inc.*, 878 F.3d 1052, 1064 (Fed. Cir. 2017) (“Microsoft did not separately address whether Kenoyer rendered the limitations of claim 6 obvious based on the teachings located in different parts of the specification, so Microsoft failed to prove obviousness for claims 36 and 37.”). Petitioner failed to do so here, presenting no proposed modification

⁵ Specifically, Petitioner cites Burdett at column 9:29, 11:57-66, 14:19-24, 24:22-25, and 26:14-28. Pet. at 23. These cited portions describe either Burdett’s Figure 1 or Burdett’s Figure 3, but Petitioner does not contend that any of these cited portions tie Burdett’s Figure 1 and Figure 3 into a single embodiment. Petitioner also cites the declaration of its expert, Dr. Franz, but Dr. Franz merely repeats almost verbatim the discussion in the Petition. Franz Decl. ¶¶ 76-77.

to either Burdett's Figure 1 or Figure 3 embodiment, no discussion of reasonable expectation of success, and no motivation to combine. See Black Decl. ¶ 68.

Petitioner also does not rely on FortiSandbox for either the "enterprise network" limitation or the "public cloud file store" limitation. See Black Decl. ¶ 69. Specifically, for the limitation requiring "a network security device that is protecting the enterprise network," Petitioner argues that "at least some of the operations conducted by Burdett's scanning service would have been performed by a device, like a FortiSandbox device." Pet. at 29-30. But Petitioner's obviousness combination does not purport to change that this "scanning service" (now implemented as a FortiSandbox) restricts access by "applications in the VPC 314" to files in "cloud data store 306" (see Burdett at 25:47-55), rather than the "enterprise facility 102" cited by Petitioner for the "enterprise network" limitation. Thus, Petitioner's combination with FortiSandbox cannot cure the fact that Petitioner is combining different embodiments in Burdett without conducting the necessary obviousness analysis.

Petitioner's arguments for independent claims 13 and 21 fare no better. Claim 13 requires "protecting an enterprise network," but the words "enterprise network" do not even appear in Petitioner's discussion of any

claim limitation, which predominantly cites back to Petitioner’s analysis of claim 1. Pet. at 35-37. Claim 21 similarly requires that “users of an enterprise network [be] protected by the network security device,” but Petitioner’s discussion for this limitation merely cites back to Petitioner’s analysis for claim 1. Pet. at 37. Petitioner’s theories for claims 13 and 21 thus are analogous to Petitioner’s theories for claim 1. See Black Decl. ¶ 70.

Accordingly, for all three independent claims, Petitioner combines two different embodiments from Burdett (Figure 1 and Figure 3) without performing the necessary obviousness analysis. Petitioner’s Ground 1 based on Burdett thus fails.

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 (emphasis added); *See* Black Decl. ¶¶ 72-73.

As discussed in more detail in connection with Ground 1, the terms “copying” and “moving” refer to different actions, and there are reasons why a POSITA would be motivated to “move” files rather than “copy” them. *See supra*, Section VI.A; Black Decl. ¶¶ 46-48. Petitioner makes no attempt to address this distinction. After admitting that Kamalapuram discloses “moving” a file (rather than “copying,” as claimed), Petitioner then concludes “a POSITA would have been guided by the teachings of Kamalapuram, and would have found it obvious, to copy the clean file into a separate repository to make it accessible to the users.” Pet. at 68. Entirely absent is any analysis showing that Kamalapuram’s “moving” of files somehow renders obvious the claimed “copying.” As in Ground 1, Petitioner never even acknowledges the difference between Kamalapuram’s “moving” and the claimed “copying” (as

required under *Graham*) and also fails to address motivation to combine and reasonable expectation of success. See Black Decl. ¶ 74. Petitioner’s assertion of obvious, devoid of any supporting analysis, is insufficient to meet Petitioner’s burden of proof. See *Unigene*, 655 F.3d at 1360 (finding “conclusory statements” not enough to show obviousness); *Harmonic*, 815 F.3d at 1367 (Fed. Cir. 2016) (burden is always on Petitioner to “show with particularity” why challenged claims are allegedly obvious)..⁶

Thus, having failed to address the claim language as written—relying on disclosure of “moving” files even though the claims clearly require “copying” files—Petitioner cannot prevail on Ground 2.

B. Petitioner Failed to Show Alleged Prior Art Disclose or Render Obvious “Natively Mount[ing]” a “Public Cloud File Store” on a “Network Security Device”

All independent claims of the ’856 patent require that a “public cloud file store is natively mounted on a network security device that is protecting the enterprise network.” As already addressed in connection with Ground 1, not every “cloud file store” is necessarily a “*public* cloud file store,” and

⁶ Petitioner also cannot rely on any additional arguments in Dr. Franz’s declaration not found in the petition. See *Cisco*, IPR2014-00454, Paper 12, at 9-10 (refusing to “consider arguments that are not made in the Petition, but are instead incorporated by reference to the cited paragraphs ... of [the expert’s] Declaration.”).

“natively mount[ing]” a “public cloud file store” on a “network security device” raises privacy and compatibility challenges not present when an entity “natively mount[s]” its private cloud file store to its own “network security device.” See Black Decl. ¶¶ 53, 60. Notwithstanding this distinction, Petitioner fails to analyze whether the alleged prior art cited for this limitation natively mounts a “public cloud file store” on a “network security device,” as claimed, or some other system component or a private cloud file store. Petitioner also does not show that it would be obvious to combine multiple references to arrive at this claim limitation. Thus, Petitioner has failed to perform the analysis necessary to show that the “natively mount[ing]” a “public cloud file store” on a “network security device” limitation is disclosed or rendered obvious.

1. No alleged prior art reference discloses “natively mount[ing]” a “public cloud file store” on a “network security device”

Petitioner admits that “Sharpe did not describe mounting the distributed filesystem to a network security device, and did not discuss mounting the filesystem in the context of scanning the files.” Pet. at 62. In addition, Petitioner also has not shown that Sharpe discloses natively mounting any “public cloud file store” for any purpose. Petitioner contends that Sharpe’s “cloud storage system 302” is the claimed “public cloud file store” (Pet. at 57-

59), but Petitioner has not shown that the alleged “native[] mount[ing]” in Sharpe’s Figure 31 is for “cloud storage system 302” (highlighted in green below) and rather a different system component, cache 3112 in storage pool 3108 (highlighted in red below). Black Decl. ¶ 76.

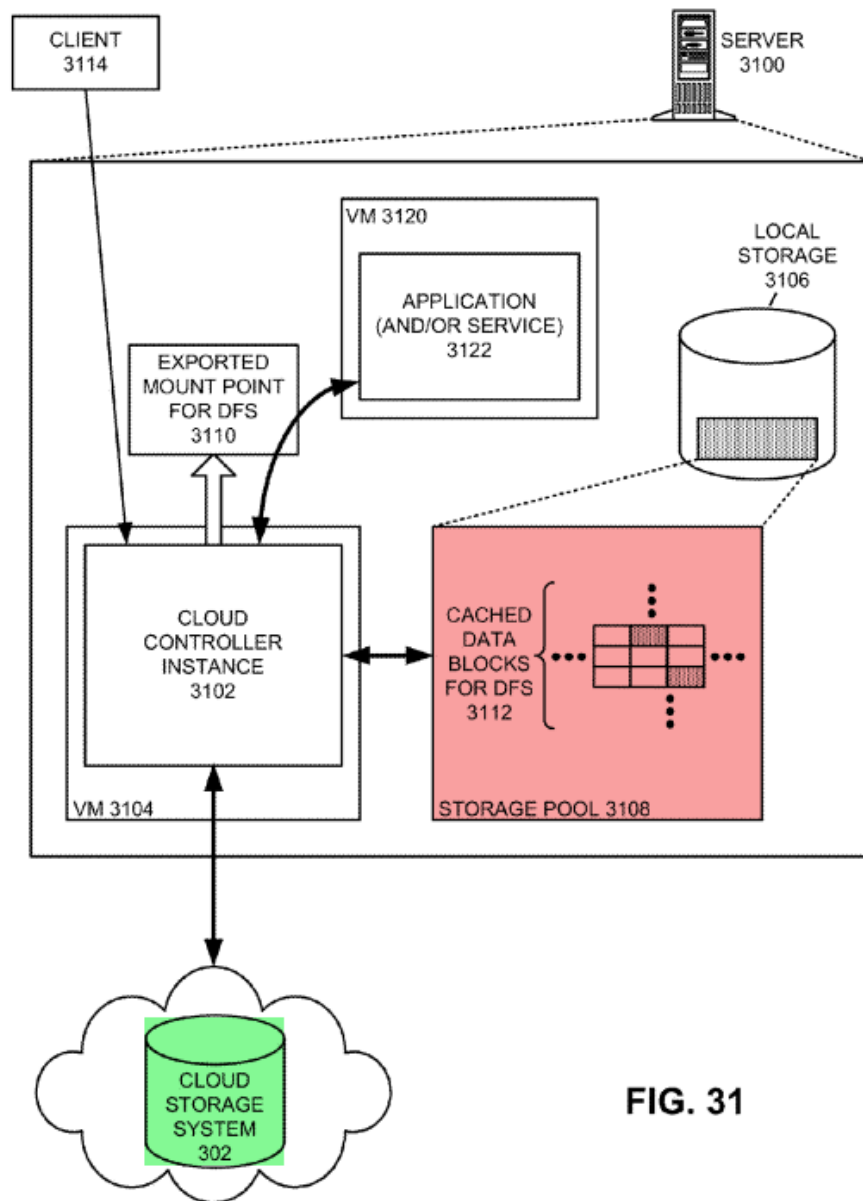


FIG. 31

Specifically, while Sharpe’s “cloud controller instance 3102 supports an additional interface that enables full, transparent access to the data stored in the distributed file system,” this is implemented by “cloud controller instance 3102 ensur[ing] that file blocks requested ... are loaded from cloud storage system 302 and cached 3112 in storage pool 3108.” Sharpe at 61:20-26. Thus, in Sharpe, the alleged “native mount[ing]” is for local storage pool 3108, and Petitioner provides no analysis showing how doing so corresponds to “natively mount[ing]” Sharpe’s cloud storage system 302. Black Decl. ¶ 77.

According to Petitioner, “Seese ... describe[s] mounting a public cloud file system in the context of scanning the files to protect an enterprise against data loss” and also” mounting the public files on a network security device.” Pet. at 62-63. Petitioner provides no analysis or evidence to show, however, that Seese’s “cloud service” is indeed a “**public** cloud file store” as opposed to (for example) a private cloud. Black Decl. ¶ 78. Seese itself acknowledges in its “Background” section that “[t]here are three traditional types of cloud storage systems”: “public cloud storage,” “private cloud storage,” and “hybrid cloud storage.” Seese at [0004]-[0006]. Petitioner cites Seese’s paragraphs [0063]-[0068] as allegedly disclosing “natively mount[ing]” a “user share on the cloud service 104A” (Seese at [0068]), but never addresses whether

Seese’s “cloud service 104A” corresponds to “public cloud storage” or “private cloud storage.” Indeed, Petitioner’s analysis for the claimed “public cloud file store” never analyzes whether that limitation is met by Seese. *See* Pet. at 57-59.

Petitioner thus has not shown that either Seese or Sharpe discloses “natively mount[ing]” a “public cloud file store” on a “network security device.” Petitioner’s expert merely repeats Petitioner’s arguments almost verbatim and provides no additional relevant analysis. Franz Decl. ¶¶ 159-64. Finally, Petitioner does not contend that Kamalapuram is relevant to this limitation, and Kamalapuram thus also cannot cure the deficiencies in Petitioner’s analysis.

Accordingly, Petitioner has not met its burden of showing that the alleged prior art discloses or renders obvious “natively mount[ing]” a “public cloud file store” on a “network security device,” as claimed.

2. Petitioner failed to show it would be obvious to combine the alleged prior art

Petitioner’s invalidity theory is that Seese alone discloses the “natively mount[ing]” a “public cloud file store” on a “network security device” limitation. Pet. at 62-63 (arguing that Sharpe “descibe[s] mounting a public cloud file system in the context of scanning the files to protect an enterprise

against data loss” and “mounting the public files on a network security device”). Because it does not, Petitioner’s invalidity theory fails. But even if Petitioner’s theory were interpreted as relying on a combination of both Sharpe and Seese for this limitation, Petitioner has not met its burden of showing that it would be obvious to apply Seese’s alleged teaching of “natively mount[ing] on a network security device” to Sharpe’s alleged teaching of a “public cloud file store.”

First, Petitioner contends that “Sharpe ... provided a motivation or suggestion to a POSITA for performing [the operation of mounting the distributed filesystem to a network security device], making it obvious to combine Sharpe with Seese.” Pet. at 62. But as explained above, Petitioner has not shown that Sharpe’s “native[] mount[ing]” even applies to a “public cloud file store,” even though Petitioner contends that Sharpe discloses such a “public could file store.” Sharpe cannot supply a “motivation or suggestion” to apply Seese’s alleged “native[] mount[ing]” on a “network security device” to Sharpe’s alleged “public cloud file store” when Sharpe allegedly already had “native[] mount[ing]” and a “network security device,” yet chose not to combine those features in the claimed manner. Black Decl. ¶ 80.

Second, Petitioner entirely fails to address “reasonable expectation of success.” The petition contains a single clause within a conclusory statement

that pays lip service to “reasonable expectation of success” (Pet. at 52) but presents no analysis on that subject. This is especially problematic because “natively mount[ing]” a “public cloud file store” on a “network security device” raises privacy and compatibility challenges not present when an entity “natively mount[s]” its private cloud file store on its own “network security device.” See Black Decl. ¶ 60. Petitioner’s expert repeats that same sentence verbatim and adds no analysis addressing differences between “natively mount[ing]” a “public cloud file store” as opposed to, e.g., a private cloud file store. Franz Decl. ¶ 138. For that reason alone, Petitioner fails to meet its burden of showing obviousness. Black Decl. ¶ 81.

Third, Petitioner proffers no defensible reason for why a POSITA would be motivated to combine Sharpe and Seese to arrive at this claim limitation. Petitioner argues that Sharpe and Seese are directed to similar prior art fields (malware detection and policy compliance) (Pet. at 53), but that at most shows they are analogous art and does not supply a motivation to combine them. Petitioner also argues that “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 Petitioner never explains why “natively mount[ing]” a “public cloud file share” on a “network security

device” furthers those alleged “goals.” Black Decl. ¶ 82. Finally Petitioner argues that “mount[ing] a public cloud file store, as taught by Seese and suggested by Sharpe, on a network security device as taught by Seese” would have “enable[d] 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 Sharpe’s “cloud controllers” were already capable of “acces[ing] files in the cloud file store” and “controlling access to the files” without incorporating the teachings of Seese. Sharpe at 97:39-62 (“[C]loud controller 4208 may be configured ... to immediately access cloud storage system 302” and, “if the file was found to be infected,” to “quarantine the file”); *see also* Black Decl. ¶ 82. Thus, none of Petitioner’s alleged motivations to combine pass muster, and Petitioner thus fails to show that it would be obvious to combine Sharpe and Seese to arrive at the claimed “natively mount[ing]” a “public cloud file store” on a “network security device.”

VIII. GROUND 3

Petitioner’s Ground 3 addresses limitations of dependent claims 3, 6, 11, 15, 17, 23, and 25 of the ’856 patent missing from the references combined in Ground 2, but does not purport to cure the deficiencies of Ground 2 with

regard to the limitations of the independent claims. Thus, Ground 3 fails for the same reasons as Ground 2.

IX. CONCLUSION

For the foregoing reasons, Patent Owner respectfully requests that the Petition be denied.

Date: June 20, 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 7,407 words and thus complies with the applicable word limit.

Date: June 20, 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 June 20, 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: June 20, 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.*