Trials@uspto.gov
571-272-7822

Paper 41
May 18, 2020

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

IPR2018-01760
Patent 9,413,722 B1

Before BRIAN J. McNAMARA, J. JOHN LEE, and
JOHN P. PINKERTON, *Administrative Patent Judges*.

LEE, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining Some Challenged Claims Unpatentable
Denying Petitioner's Motion to Exclude
Denying Patent Owner's Motion to Exclude
35 U.S.C. § 318(a)

INTRODUCTION

Cisco Systems, Inc. ("Petitioner") filed a Petition (Paper 1, "Pet.") requesting an *inter partes* review of claims 1–25 ("the challenged claims") of U.S. Patent No. 9,413,722 B1 (Ex. 1001, "the '722 Patent").[1] An *inter partes* review of all challenged claims was instituted on May 20, 2019. Paper 9 ("Inst. Dec."). After institution, Centripetal Networks, Inc. ("Patent Owner") filed a Patent Owner Response (Paper 14, "PO Resp."), Petitioner filed a Reply (Paper 20, "Pet. Reply"), and Patent Owner filed a Sur-reply (Paper 26, "PO Sur-reply"). The parties also filed motions to exclude evidence, which are addressed below. An oral hearing was held on February 20, 2020. Paper 40 ("Tr.").

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a). As explained below, Petitioner has shown by a preponderance of the evidence that all challenged claims of the '722 Patent are unpatentable.

A. Related Cases

The parties identify as related to the present case: *Centripetal Networks, Inc. v. Cisco Systems, Inc.*, Case No. 2:18-cv-00094-MSD-LRL (E.D. Va); and *Centripetal Networks, Inc. v. Keysight Techs., Inc.*, Case No. 2:17-cv-00383-HCM-LRL (E.D. Va). Pet. 8; Paper 3, 1.

---

[1] On its face, the '722 Patent indicates the earliest effective filing date is April 17, 2015. Ex. 1001, code (63). Consequently, for all purposes relevant to this Decision, we apply statutes as they stand after the Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011).

B. The '722 Patent

The '722 Patent relates to "rule-based network-threat detection." Ex. 1001, 1:45–46. The Specification describes a process in which a packet-filtering device receives data packets and determines whether each packet corresponds to criteria specified by a packet-filtering rule. *Id.* at 1:49–52. The packet-filtering rule criteria may correspond to one or more "network-threat indicators." *Id.* at 1:52–53. A network-threat indicator may be, for example, "network addresses, ports, fully qualified domain names (FQDNs), uniform resource locators (URLs), uniform resource identifiers (URIs), or the like" that are associated with network threats (e.g., malware). *Id.* at 3:18–33. The packet-filtering rule also specifies an "operator" to be applied by the packet-filtering device when the rule is triggered, the operator being configured to cause the device to either prevent or allow the packet to continue toward its destination. *Id.* at 1:53–58.

The device also generates a log entry comprising information from the packet-filtering rule identifying the network-threat indicator(s) and whether the packet was prevented or allowed to continue. *Id.* at 1:58–63. In addition, the Specification describes that the packet-filtering device communicates this information as well to a user device, which presents the information in an interface through which the user can cause the packet-filtering device to reconfigure the operator specified by the packet-filtering rule such that future packets would be prevented from continuing. *Id.* at 1:64–2:10. Figure 7 is a flow chart illustrating an embodiment of the disclosed method, and is reproduced below.

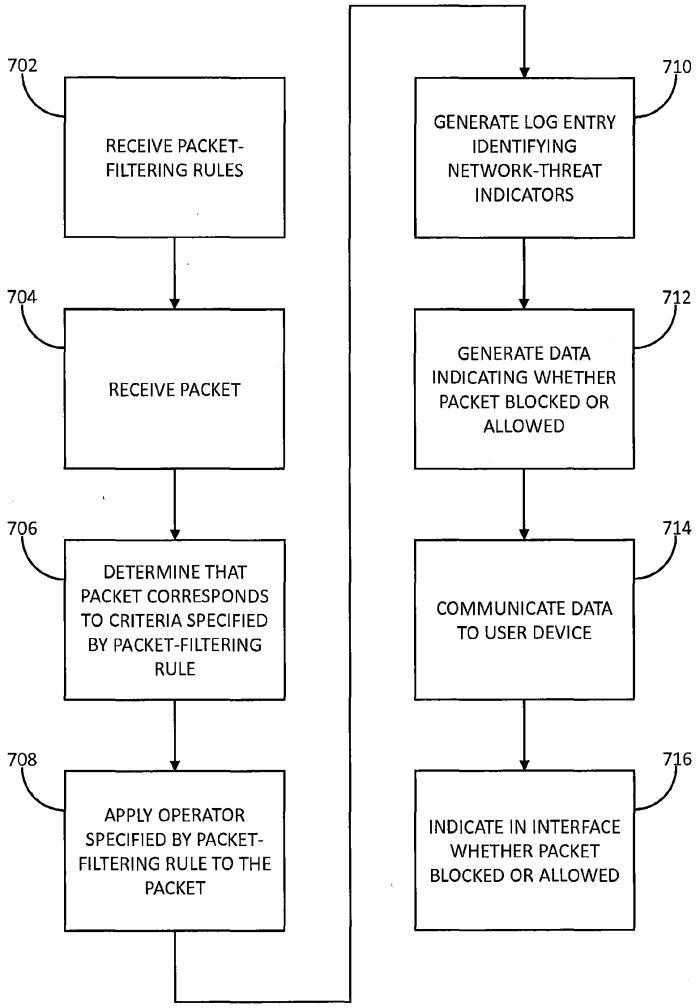


FIG. 7

Id. at Fig. 7. The above figure depicts an illustrative method for rule-based network-threat detection. *Id.* at 15:52–54; *see id.* at 15:54–16:34 (describing in detail each step depicted in Figure 7).

C. Challenged Claims

Petitioner challenges all of the claims of the ’722 Patent. Claim 1, the only independent claim, is illustrative and is reproduced below (letters in brackets added for ease of reference):

1. A method comprising:

[a] receiving, by a packet-filtering device, a plurality of packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators;

[b] receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;

[c] responsive to a determination by the packet-filtering device that the first packet satisfies one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more network-threat indicators of the plurality of network-threat indicators:

> [d] applying, by the packet-filtering device and to the first packet, an operator specified by the packet-filtering rule and configured to cause the packet-filtering device to allow the first packet to continue toward a destination of the first packet;
>
> [e] communicating, by the packet-filtering device, information from the packet-filtering rule that identifies the one or more network-threat indicators, and data indicative that the first packet was allowed to continue toward the destination of the first packet;
>
> [f] causing, by the packet-filtering device and in an interface, display of the information in at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators;
>
> [g] receiving, by the packet-filtering device, an instruction generated in response to a user invoking an element in the at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators; and
>
> responsive to receiving the instruction:

> [h] modifying, by the packet-filtering device, at least one operator specified by the packet-filtering rule to reconfigure the packet-filtering device to prevent packets corresponding to the one or more criteria from continuing toward their respective destinations; and
>
> [i] responsive to a determination by the packet-filtering device that the second packet corresponds to the one or more criteria:
>
> > [j] preventing, by the packet-filtering device, the second packet from continuing toward a destination of the second packet;
> >
> > [k] communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and
> >
> > [l] causing, by the packet-filtering device and in the interface, display of the data indicative that the second packet was prevented from continuing toward the destination of the second packet.

D. Instituted Ground of Unpatentability and Asserted Prior Art

Trial was instituted on the sole ground of unpatentability asserted in the Petition:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–25	103	Sourcefire[2]

[2] Sourcefire 3D System User Guide, Version 4.10 (Ex. 1004, "Sourcefire").

Inst. Dec. 27; *see* Pet. 24. The parties dispute whether Sourcefire qualifies as prior art under 35 U.S.C. § 102(a)(1), specifically whether it was publicly accessible in (or before) April of 2011. *See* Pet. 24; PO Resp. 2–11; Pet. Reply 2–7; PO Sur-reply 2–10.

Petitioner relies on the Declaration of John Leone (Ex. 1005) and the Declaration of Jacob H. Baugher III (Ex. 1042), which present testimony to support Petitioner's assertions regarding public accessibility. In addition, Petitioner further relies on the Declaration of Dr. Stuart Staniford (Ex. 1003), its proffered expert witness. Similarly, Patent Owner relies on a declaration by its proffered expert witness, Dr. Alessandro Orso (Ex. 2002).

ANALYSIS

A. Level of Ordinary Skill in the Art

Petitioner asserts that a person of ordinary skill in the art would have had a bachelor's degree in computer science, computer engineering or an equivalent, as well as four years of industry experience. Pet. 15 (citing Ex. 1003 ¶¶ 21–24 (Dr. Staniford's testimony)). In addition, Petitioner asserts that a person of ordinary skill would have had "a working knowledge of packet-switched networking, firewalls, security policies, communication protocols and layers, user interfaces, and the use of customized rules to address cyber-attacks." *Id*.

In its Response, Patent Owner does not dispute Petitioner's definition of the level of skill in the art.[3] Based on the complete trial record, we find

[3] Dr. Orso testified to a slightly different description of the level of skill in the art (Ex. 2002 ¶ 36), but Patent Owner did not argue during trial that Dr. Orso's description should be adopted instead of Petitioner's description and waived any such argument as a result. *See In re NuVasive, Inc.*, 842

Dr. Staniford's testimony credible and persuasive (Ex. 1003 ¶¶ 21–24), and we adopt Petitioner's definition as a result.

B. Claim Construction

For petitions filed before November 13, 2018, as here, claim terms in an unexpired patent are given their broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b) (2018); *see Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016). In the Decision on Institution, we preliminarily construed the term "network-threat indicator" as an "indicator that represents the identity of a resource associated with a network threat." Inst. Dec. 8. During trial, neither party disputed this preliminary construction. *See* PO Resp. 25; Pet. Reply 7–8; Tr. 10:22–11:9. We do not discern any evidence in the full record after trial indicating that this construction is incorrect or should be modified. Moreover, the Specification supports this construction, indicating that "network addresses, ports, fully qualified domain names (FQDNs), uniform resource locators (URLs), uniform resource identifiers (URIs), or the like" are examples of "network-threat indicators." Ex. 1001, 3:18–26. Thus, we apply this construction in this Decision.

At the oral hearing, Patent Owner belatedly argued that the Specification indicates the above examples are insufficient by themselves to constitute "network-threat indicators" because the Specification further mentions "other information associated with the network threats," such as

---

F.3d 1376, 1380–81 (Fed. Cir. 2016). Moreover, Dr. Orso testified that his opinions would be unchanged under Petitioner's description of the level of ordinary skill. Ex. 2002 ¶ 36.

threat type and geographic location. *See* Tr. 45:9–25, 62:10–64:23, 80:15–82:2. As an initial matter, Patent Owner did not make this argument in its claim construction positions advanced during trial and, thus, it is untimely. *See* PO Resp. 25–28; PO Sur-reply 10–12; *NuVasive*, 842 F.3d at 1380–81.

Even were we to consider this argument, we disagree and decline to modify our construction to require such "other information." The Specification describes that "[n]etwork-threat-intelligence providers" disseminate "network-threat-intelligence reports" that include "network-threat indicators (e.g., network addresses, ports, fully qualified domain names (FQDNs), uniform resource locators (URLs), uniform resource identifiers (URIs), or the like) associated with the network threats, *as well as other information* associated with the network threats." Ex. 1001, 3:18–33 (emphasis added). In other words, the "other information" is included in network-threat-intelligence reports *along with* network-threat indicators, *not* as part of them, which also is evidenced by how the "other information" is *not* included in the parenthetical listing the examples of such indicators. In fact, Patent Owner itself admits that the '722 Patent "makes clear that the network-threat indicator is the identity of the resource associated with the threat *and not the threat itself or other information associated with the threat*." PO Sur-reply 12–13 (quoting Ex. 1001, 3:18–33) (emphasis added).

We note that the parties disagree further about whether our construction of "network-threat indicator" encompasses certain specific examples potentially relevant to the prior art, particularly ports. *See* PO Resp. 27–28; Pet. Reply 10; PO Sur-Reply 11–12. As this dispute concerns the application of our construction rather than the construction itself, we

address it to the extent necessary to determine the patentability of the challenged claims in our obviousness analysis below.

No other claim terms in the ’077 Patent require express construction for purposes of this Decision. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (holding that only claim terms in controversy require express construction, and only to the extent necessary to resolve the controversy).

C. Alleged Unpatentability Under § 103

Petitioner’s sole asserted ground of unpatentability as to all challenged claims is obviousness in view of Sourcefire. Pet. 24. A claim is unpatentable under § 103 if the differences between the claimed subject matter and the prior art are “such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) objective evidence of nonobviousness, i.e., secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

Additionally, the obviousness inquiry typically requires an analysis of “whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (requiring “articulated reasoning with some rational underpinning to support the legal conclusion of obviousness”)); *see In re Warsaw Orthopedic, Inc.*, 832 F.3d 1327, 1333

(Fed. Cir. 2016) (citing *DyStar Textilfarben GmbH & Co. Deutschland KG v. C. H. Patrick Co.*, 464 F.3d 1356, 1360 (Fed. Cir. 2006)).

1. Overview of Sourcefire

Sourcefire is a user guide for the Sourcefire 3D System, a system that provides "real-time network intelligence for real-time network defense." Ex. 1004, 32.[4] The system operates via "3D Sensors" that can each run the Sourcefire "Intrusion Prevention System" (IPS), which allows monitoring of networks for attacks by examining packets for malicious activity. *Id.* at 33–34. Users can create custom "intrusion rules" to examine packets for attacks and manage the rules across all the 3D Sensors in the system through a centralized "Defense Center." *Id*. at 34, 254.

Intrusion rules can be "pass" rules, "alert" rules, or "drop" rules. *Id.* at 761. If a pass rule is met, the network traffic in question is ignored (and allowed to continue). *Id*. Conversely, if a drop rule is met, the packet is dropped and an "event" is generated. *Id*. Rules can be written based on "keywords" and their "arguments," i.e., the possible values of the keyword. *Id.* at 762–763.

The Sourcefire 3D System also features "preprocessors" that can facilitate processing of network traffic by identifying and decoding certain types of traffic, such as HTTP (hypertext transfer protocol) and SSL (secure sockets layer) traffic. *Id.* at 513–514. The SSL preprocessor, for example, can be used to identify encrypted traffic that IPS cannot analyze, thereby

[4] All citations to Sourcefire refer to the document's original pagination.

enabling IPS to ignore (pass) the encrypted packets and avoid wasting resources trying to inspect them. *Id.* at 596.

2. Public Accessibility of Sourcefire

Petitioner asserts that Sourcefire qualifies as prior art under § 102(a)(1). Pet. 24. Patent Owner asserts that Sourcefire does not qualify as applicable prior art because it is not a printed publication. *See* PO Resp. 2–11 (citing 35 U.S.C. § 311(b)); PO Sur-reply 2–10. In determining whether a prior art reference constitutes a printed publication, "the touchstone is public accessibility." *In re Bayer*, 568 F.2d 1357, 1359 (CCPA 1978); *see Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1348 (Fed. Cir. 2016). "A given reference is 'publicly accessible' upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence, can locate it." *SRI Int'l, Inc. v. Internet Sec. Sys., Inc.*, 511 F.3d 1186, 1194 (Fed. Cir. 2008) (quoting *Bruckelmyer v. Ground Heaters, Inc.*, 445 F.3d 1374, 1378 (Fed. Cir. 2006)).

Petitioner contends that Sourcefire was publicly available because (1) it was actually disseminated to hundreds of customers who purchased Sourcefire 3D System products, and (2) it was available on Sourcefire's support website. *See* Pet. 24; Pet. Reply 2. As explained below, we conclude that Petitioner has shown sufficiently that Sourcefire was publicly available due to its actual dissemination to customers.

According to Petitioner, Sourcefire was enclosed on a CD-ROM disk that was "included with each [Sourcefire] 3D System appliance sold, and offered for sale, from April 2011 through at least March 2013 – no less than

two years before the '722 Patent." Pet. Reply 3. Specifically, Petitioner asserts there were "586 sales of the [Sourcefire] 3D System that included [the Sourcefire reference]" during this time period. *Id.* Petitioner relies on the testimony of John Leone and Jacob H. Baugher III, two former employees of Sourcefire's manufacturer. *Id.* (citing Ex. 1005 (Leone Declaration); Ex. 1042 (Baugher Declaration)). Mr. Leone testified that Sourcefire was included with every Sourcefire 3D System product in that timeframe, and that "approximately 586 customers purchased the Sourcefire 3D System from April 2011 through March 2013 and had access to the Sourcefire 3D System User Guide." Ex. 1005 ¶¶ 11, 19. Mr. Baugher provided corroborating testimony in which he explained how Sourcefire sales records were kept and that, based on those records, "there were approximately 586 customers that purchased the Sourcefire 3D System from April 2011 through March 2013." Ex. 1042 ¶¶ 5–8. He further testified that "[t]hese 586 customers include entities having large network security teams," including Microsoft, Symantec, and various other technology companies, as well as governmental organizations such as the U.S. Department of Defense, the U.S. Department of Homeland Security, and the North Atlantic Treaty Organization (NATO). *Id.* ¶ 9.

Additionally, Petitioner cites a press release about the relevant Sourcefire 3D System published in BusinessWire in April 2011 (Ex. 1034), a product review for the Sourcefire 3D System published by ITPro in January 2007 (Ex. 2009), and a product review for the system published by SC Media in May 2006 (Ex. 2010), as evidence establishing that the Sourcefire 3D System (including its accompanying user manual, the Sourcefire reference) was publicly marketed and sold to customers. Pet.

Reply 4. Patent Owner argues that these facts and Petitioner's evidence are insufficient to establish public accessibility under controlling case law. *See* PO Sur-reply 3–10.

Petitioner relies on *Mass. Inst. of Tech. v. AB Fortia*, 774 F.2d 1104 (Fed. Cir. 1985) ("*MIT*"). Pet. Reply 3. In *MIT*, a paper was orally presented at a scientific conference attended by "50 to 500 cell culturists." 774 F.2d at 1108. Copies of the paper "were distributed on request, without any restrictions, to as many as six persons." *Id.* at 1108–09. The Federal Circuit held that these facts were sufficient to establish public accessibility. *Id.* at 1109; *see also In re Klopfenstein*, 380 F.3d 1345, 1349 (Fed. Cir. 2004) ("The key to the court's finding [in *MIT*] was that actual copies of the presentation were distributed."). Petitioner also cites *Garrett Corporation v. United States*, 422 F.2d 874, 878 (Ct. Cl. 1970). Pet. Reply 3. In *Garrett*, the court held that a government report was a "printed publication" under § 102(b) because approximately 80 copies were disseminated, including to six commercial companies. 422 F.2d at 878. The court held that "distribution to commercial companies without restriction on use clearly" established that the report is a printed publication. *Id*.

Patent Owner relies on *Medtronic, Inc. v. Barry*, 891 F.3d 1368 (Fed. Cir. 2018). PO Sur-reply 4–5. In *Medtronic*, the prior art at issue was disseminated to attendees of three conferences. 891 F.3d at 1379. The Federal Circuit distinguished *Medtronic* from past cases involving references stored in repositories (e.g., libraries)—rather than considerations like indexing and cataloguing, the relevant inquiry was whether the *distribution* of the reference to certain groups of people was sufficient for public accessibility. *Id.* at 1379–80. Issues underlying that inquiry include,

for example, "whether there is an expectation of confidentiality between the distributor and the recipients of the materials," as well as "[t]he expertise of the target audience." *Id.* at 1381–82. Although agreeing with the Board that "[d]istributing materials to a group of experts" is not enough for public accessibility "simply by virtue of the relative expertise of the recipients," the Federal Circuit held that the Board in that case had not sufficiently considered all of the recipients of the distributed materials, or whether all the recipients were expected to hold the distributed materials in confidence. *Id.* at 1382–83.

Based on the above facts and case law, we conclude that Sourcefire was publicly accessible. The evidence of record indicates that the Sourcefire 3D System was publicly marketed and sold, and that the Sourcefire reference was actually distributed to over 500 customers of the Sourcefire 3D System. Ex. 1005 ¶¶ 11, 19; Ex. 1042 ¶¶ 5–9. This vastly exceeds the distribution to six people in *MIT* and distribution of 80 copies in *Garrett*. Record evidence also supports Petitioner's contention that the customers who received Sourcefire included entities interested in network security products, including persons of ordinary skill in the art. *See* Ex. 1042 ¶ 9; *see also* Ex. 1004, 1, 32–33 (identifying Sourcefire as a "User Guide" and indicating Sourcefire provides information for network administrators); Ex. 1005 ¶ 5 (indicating Sourcefire was drafted in consultation with, and reviewed by, engineers who designed the Sourcefire system). Moreover, similar to *MIT* and as discussed in *Medtronic*, the record indicates that the recipients of Sourcefire were not subject to confidentiality requirements restricting use or further distribution. *See* Ex. 1004, 2 (Sourcefire copyright page stating, "You may use . . . and otherwise copy and distribute

[Sourcefire] solely for non-commercial use").[5] Although Patent Owner asserts that *MIT* and *Klopfenstein* are distinguishable because they involved "the free distribution of academic documents to conference and meeting attendees" (PO Sur-reply 7), case law indicates that distribution to commercial entities also may be sufficient. *See Garrett*, 422 F.2d at 878; Pet. Reply 3.[6]

Patent Owner argues that Mr. Leone's testimony regarding the number of customers who purchased relevant Sourcefire products (and, thus, received the Sourcefire reference) is not credible. *See* PO Resp. 6–7; PO Sur-reply 8. According to Patent Owner, insufficient explanation was provided as to "how many 'documentation disks' were provided with the product and whether the documentation disks were indexed in any

---

[5] Patent Owner asserts that "Mr. Baugher reveals that each sale of a Sourcefire product was subject to licensing restrictions," arguing that such restrictions preclude public accessibility. PO Sur-reply 9–10 (citing Ex. 2017, 47:6–18). Mr. Baugher, however, does not mention any "licensing restrictions," instead indicating only that a "signed sales order" or a "purchase order" was required. Ex. 2017, 47:6–21. He also mentions that customers would "click through an agreement to agree to our terms and conditions," but Patent Owner does not identify any evidence about those terms and conditions or otherwise explain how they show restrictions on the dissemination of Sourcefire.

[6] Both decisions by Board panels relied on by Patent Owner (PO Sur-reply 5–6) are distinguishable on their facts, including because both involved references that were subject to restrictions prohibiting their reproduction or further dissemination. *See ASM IP Holding B.V., v. Kokusai Elec. Corp.*, IPR2019-00369, Paper 8, at 18 (PTAB June 27, 2019); *VMAC Global Techs. Inc., v. Vanair Mfg, Inc.*, IPR2018-00670, Paper 9, at 13–14 (PTAB Aug. 10, 2018). In *ASM*, the panel further noted that there was no evidence of actual dissemination to interested artisans. *See ASM*, Paper 8, at 17.

meaningful way," and Mr. Leone's role does not indicate sufficient personal knowledge about sales or customers. *See* PO Resp. 6–7; PO Sur-reply 8.

The relevant question, however, is not whether Sourcefire was publicly accessible on a certain number or format of "documentation disks," but rather whether Sourcefire was adequately disseminated. Regarding Mr. Leone's credibility, we find his testimony to be credible and persuasive, particularly as supported by the testimony of Mr. Baugher, who also confirmed the number of customers who purchased the Sourcefire system. *See* Ex. 1042 ¶¶ 5–8. We note that Patent Owner declined to depose Mr. Leone to determine the extent of his personal knowledge or the manner in which he informed himself of the facts necessary for his testimony. *See* Pet. Reply 3–4. Patent Owner also is not seeking to exclude any aspect of Mr. Leone's testimony for any reason, including for lack of personal knowledge under Rule 602. *See* Paper 28 (Patent Owner's motion to exclude); Fed. R. Evid. 602.

Patent Owner also challenges Mr. Baugher's testimony, asserting that Mr. Baugher's methodology for determining the relevant customers was flawed. *See* PO Sur-reply 8–9. We are not persuaded, however, because Patent Owner's assertions are not consistent with Mr. Baugher's testimony. For example, according to Patent Owner, Mr. Baugher's "method of analysis relied entirely on a SKU (stock keeping unit) scheme in which certain SKUs contained the '3D' prefix in its value," which allegedly undermines his testimony because he could not "verify that he specifically analyzed sales record having a product description naming Sourcefire 3D **Sensor** products, i.e., specific products named in Mr. Leone's declaration as . . . containing

the Sourcefire reference." *Id.* (citing Ex. 2017, 53:5–25 (emphasis added by Patent Owner)).

Mr. Baugher testified, however, that the records he relied on included both SKU descriptions and product descriptions. *See* Ex. 2017, 52:24–53:4; *see also id.* at 51:4–52:23 (indicating the records were identified based on "product family" rather than "SKU alone," and that each SKU was accompanied by "a description of the product . . . which would also identify it as a 3D product type"). Additionally, Mr. Leone's Declaration named "3D Sensor" products as only one *example* of products that included the Sourcefire reference, i.e., "each Sourcefire 3D System appliance (*e.g.*, 3D Sensor, Defense Center)." Ex. 1005 ¶ 11. Thus, whether Mr. Baugher could recall that "3D Sensor" products specifically were included is of limited relevance given his explanation that the records were identified based on the Sourcefire 3D System *product family*. *See* Ex. 2017, 51:4–53:4.

Patent Owner also argues that, even if sales of Sourcefire products (including the Sourcefire reference) were established, such dissemination is insufficient, and that Petitioner must additionally demonstrate that a person of ordinary skill would have been able to locate Sourcefire through reasonable diligence. PO Resp. 2–3, 7–8; PO Sur-reply 4–6, 7–8 (citing *Acceleration Bay, LLC v. Activision Blizzard, Inc.*, 908 F.3d 765, 772 (Fed. Cir. 2018)). The Federal Circuit has indicated that public accessibility is established by showing that the reference was "disseminated *or otherwise* made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it." *Acceleration Bay*, 908 F.3d at 772 (quoting *Jazz Pharm., Inc. v. Amneal Pharm., LLC*, 895 F.3d 1347, 1355–56 (Fed. Cir. 2018)) (emphasis added).

Here, Petitioner has shown that Sourcefire was "disseminated" to interested artisans; thus, it is unnecessary to additionally show that it was also "otherwise" made available to them. *See Klopfenstein*, 380 F.3d at 1349 ("The key to the court's finding [in *MIT*] was that actual copies of the presentation were distributed."). We note the Federal Circuit has held that if the latter is shown (i.e., accessibility through reasonable diligence), it is unnecessary to show actual access or dissemination. *See*, *e.g.*, *Jazz Pharm.*, 895 F.3d at 1356 ("If accessibility is proved, there is no requirement to show that particular members of the public actually received the information.").

Consequently, we are unpersuaded that Sourcefire was not publicly accessible due to various issues surrounding whether the Sourcefire website made the reference adequately accessible, given the evidence of actual dissemination through sales and commercial distribution. *See* PO Resp. 3–5; PO Sur-reply 2–3. Nor are we persuaded by Patent Owner's contention that the cost of the Sourcefire 3D System was too high and, thus, a skilled artisan would not have been able to access Sourcefire. *See* PO Resp. 8–9; PO Sur-reply 6–7. The cost did not prevent over 500 customers from actually obtaining Sourcefire by purchasing Sourcefire 3D System products. Moreover, there is no evidence in the record indicating that sales of the relevant Sourcefire products were restricted or limited to only certain customers, or that the cost[7] of acquiring a Sourcefire 3D System product was prohibitively high to the relevant artisans.

---

[7] The record includes evidence of a range of prices for various configurations of Sourcefire 3D System products, from $1,385 to £25,000. Ex. 2009, 1; Ex. 2010, 1. Based on Mr. Leone's testimony, Sourcefire would have been distributed with the purchase of any of these products.

Additionally, Patent Owner cites *In re Bayer*, 568 F.2d 1357 (CCPA 1978), arguing the prior art in *Bayer* (a thesis) was held not to have been publicly accessible despite actual distribution to faculty on a graduate committee reviewing the thesis. PO Sur-reply 5. In *Bayer*, the relevant issue was whether the appellant's "uncatalogued, unshelved thesis, by virtue of its accessibility to the graduate committee," constituted a printed publication. 568 F.2d at 1359. The Federal Circuit has clarified *Bayer*, explaining that the thesis was held not publicly accessible because "a work is not publicly accessible if the only people who know how to find it are the ones who created it," such as the faculty on the graduate committee reviewing and advising on student theses. *See Samsung Elecs. Co. v. Infobridge Pte. Ltd.*, 929 F.3d 1363, 1371–72 (Fed. Cir. 2019). Thus, *Bayer* is inapposite here, where Sourcefire was distributed to over 500 customers.

In summary, we find that a preponderance of the evidence establishes that Sourcefire was distributed commercially through sales of the Sourcefire 3D System to over 500 customers, including interested persons of ordinary skill, and that those customers were not subject to any restriction or expectation of confidentiality with regard to its use or further distribution. Therefore, we conclude that Sourcefire was publicly accessible, and that it constitutes prior art under § 102(a)(1).

3. Independent Claim 1

Petitioner contends claim 1 of the '722 Patent would have been obvious in view of Sourcefire. As explained in more detail below, we find

---

Ex. 1005 ¶ 11 (testifying that Sourcefire was "included with each Sourcefire 3D System appliance (*e.g.*, 3D Sensor, Defense Center) sold to a customer").

that Petitioner has shown by a preponderance of the evidence that Sourcefire teaches each limitation of claim 1.

a. Limitation 1[a]

Limitation 1[a] of claim 1 recites, "receiving, by a packet-filtering device, a plurality of packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators."

Petitioner identifies Sourcefire's 3D Sensor with IPS as the recited "packet-filtering device," and the rules received by the 3D Sensor via, for example, intrusion policies imported from a centralized Defense Center as the recited "packet-filtering rules." Pet. 36–39 (citing *inter alia* Ex. 1004, 34, 105, 338–350, 2001–2002). With respect to the recited "network-threat indicators," Petitioner relies on Sourcefire's disclosures regarding rules using IP addresses or ports, for example, to take an action (e.g., passing or dropping) on a data packet. *Id.* at 39 (citing Ex. 1004, 762–769). Specifically, Petitioner identifies Sourcefire's discussion of "source or destination IP address, source or destination port, protocol, keyword (*e.g.*, malicious URL/URI), etc.[] associated with the particular exploit that the rule was designed to protect" as examples of "data . . . corresponding to characteristics associated with malicious activities" that teach the recited "network-threat indicators." *Id*. at 38–39 (citing Ex. 1004, 34, 762–769). The Petition explains that Sourcefire, thus, teaches receiving the recited "packet-filtering rules" configured to cause a 3D Sensor device to identify packets corresponding to, for example, certain IP addresses identifying a source of malicious activity ("network-threat indicators"). *Id*.

We are persuaded by Petitioner's reasoning and evidence. Patent Owner's arguments, discussed in more detail below, are unpersuasive and are inconsistent with the weight of the record evidence. Thus, we find that Sourcefire teaches limitation 1[a] of claim 1.

In particular, Sourcefire discloses that "[b]y placing 3D Sensors with IPS on key network segments, you can examine the packets that traverse your network for malicious activity," and that the 3D Sensors use "rules . . . to look for the broad range of exploits that attackers have developed." Ex. 1004, 34. Further, Sourcefire describes these rules as follows:

> An *intrusion rule* is a specified set of keywords and arguments on a 3D Sensor with the IPS component that detects attempts to exploit vulnerabilities on your network by analyzing network traffic to check if it matches the criteria in the rule. IPS compares packets against the conditions specified in each rule and, if the packet data matches all the conditions specified in a rule, the rule triggers.

Id. at 761. Consequently, we find that Sourcefire teaches the recited "packet-filtering device" (3D Sensor with IPS), which examines packets using "packet-filtering rules" (intrusion rules). Sourcefire also teaches that intrusion rules are "received" by the packet-filtering device (3D Sensor) from a Defense Center, which is used to manage multiple 3D Sensors and provide them with intrusion policies that include intrusion rules. *See id.* at 34, 105, 338–350, 2001–2002.

Sourcefire indicates that an intrusion rule may specify "source and destination IP addresses," "source and destination ports," and "keywords and their parameters and arguments." *Id.* at 762. Using these aspects of a rule, a user can "restrict packet inspection to the packets originating from specific IP addresses." *Id.* at 766–767; *see also id.* at 768–769 (teaching similar

restrictions for packets originating from specific ports). Based on these disclosures, we find that Sourcefire teaches packet-filtering rules that are "configured to cause the packet-filtering device to identify packets corresponding to," for example, specific source IP addresses (e.g., computers located at those IP addresses).

We further find that Sourcefire teaches the recited "network-threat indicators." As discussed above, a "network-threat indicator" is properly construed as an "indicator that represents the identity of a resource associated with a network threat." The source IP address discussed in Sourcefire identifies the source of a packet. *See id.* at 768–769. As noted above, Sourcefire indicates intrusion rules are used to identify "exploits" from attackers such that 3D Sensors employing those rules examine packets for "malicious activity." *Id.* at 34, 761. Thus, we are persuaded that a person of ordinary skill would understand these disclosures of Sourcefire to teach packet-filtering rules (intrusion rules) configured to cause a packet-filtering device (3D Sensor with IPS) to identify packets corresponding to at least one of a plurality of indicators (source IP addresses) that represent the identity of a resource (computer located at the source IP address) associated with a network threat (exploit or other malicious activity). *See* Ex. 1003 ¶¶ 114–116. Indeed, we note that the Specification of the '722 Patent itself identifies "network addresses" associated with network threats as examples of "network-threat indicators." Ex. 1001, 3:23–24.

Patent Owner disputes that Sourcefire teaches the recited "network-threat indicators" for a number of reasons, all of which are unpersuasive. *See* PO Resp. 29–48. First, Patent Owner asserts that "the source IP address specified in the Rule Header is used merely to 'restrict packet inspection'"

and "not because the IP addresses and ports are associated with a network threat." *Id.* at 32–33. Further, Patent Owner notes that Sourcefire indicates source and destination IP addresses are used, at least in part, to "remov[e] the possibility of the rule triggering against packets whose source and destination addresses *do not* indicate suspicious behavior." *Id.* at 32–33, 40–42 (citing Ex. 1004, 766–767 (emphasis added)). These arguments, however, ignore Sourcefire's teachings about using intrusion rules to detect exploits and malicious activity (*see* Ex. 1004, 34, 761), rather than only identifying "known trusted IP addresses" on a "whitelist" that should not be inspected, as Patent Owner suggests (PO Resp. 40–42). We find that an ordinary artisan would have been taught by Sourcefire's disclosures to use source and destination IP addresses to configure the rule to more accurately target only packets with IP addresses that *do* indicate suspicious behavior, consistent with our construction of "network-threat indicators."

Next, Patent Owner cites particular examples in Sourcefire that it alleges support its position—for instance, the example of a rule shown on pages 763–764 of Sourcefire indicates the rule applies to "traffic coming from any host that is not on your internal network," and that example rule specifies various other criteria that are applied instead of specific network-threat indicators. PO Resp. 33–35, 45–46. Petitioner does not, however, rely solely on that particular example rule—other aspects of the same sections of Sourcefire undermine Patent Owner's position and support Petitioner's view, as discussed above. For example, Sourcefire also provides examples of rule header syntax that would configure the intrusion rule to apply to a specific source IP address. *See* Ex. 1004, 766–767. As a result, Patent Owner's argument is not persuasive.

Similarly, Patent Owner's arguments regarding the example of an "intrusion event" on pages 282–283 of Sourcefire also are unpersuasive because they erroneously focus on only part of Sourcefire's disclosure. *See* PO Resp. 35–38, 46–48. For instance, Patent Owner argues that certain "5-tuple information" (including source IP address) in that particular example was not used in the relevant intrusion rule and, thus, could not teach the network-threat indicator. *Id.* at 36–38. This argument, however, ignores Sourcefire's teachings regarding rules in which source IP addresses *are* used as a network-threat indicator, as discussed above—whether Sourcefire *also* includes examples that may not disclose limitation 1[a] is inapposite. Moreover, we note that Petitioner does not rely on the "intrusion event" disclosure for limitation 1[a], but rather cites it in its arguments relating to limitation 1[e]. *See* Pet. 42–44. Likewise, Patent Owner's argument (PO Resp. 43) that Sourcefire's "Rule Categories" do not include a category based on "traffic identified based upon the identity of a resource associated with a network threat" also is unpersuasive because Petitioner does not rely on those disclosures of Sourcefire.[8]

Patent Owner further argues that "Sourcefire does not disclose any source of information for constructing rules that identify **resources**

---

[8] We note that the "Rule Categories" cited by Patent Owner include categories for rules detecting traffic identified based on, for example, specific communications protocols (e.g., FTP, POP2, NNTP, SNMP), "UNIX or Linux-based remote services," whether the traffic "originate[s] from telnet servers," and whether the traffic is "suspicious traffic sent to or from web servers," as well as a category for "[u]ser-defined rules" created based on the rule customization instructions described in Sourcefire. Ex. 1004, 427–430.

associated with a network attack." PO Resp. 41 (citing Ex. 2002 ¶ 94) (emphasis in original). According to Patent Owner, "[t]hat concept is simply missing from Sourcefire because Sourcefire is not designed to operate on the basis of network threat indicators, but rather on the basis of inspecting content in received traffic for exploits." *Id.* (citing Ex. 2002 ¶ 94). No further explanation is given to support these conclusory statements. For example, Patent Owner does not address why a computer located at a specific source address would not constitute a "resource," or explain why operating on the basis of network-threat indicators and inspecting content in received traffic are mutually exclusive. *See id*. The only evidence cited is the testimony of Dr. Orso, but that testimony likewise fails to provide more than the same conclusory statements—indeed, the cited testimony is nearly a verbatim repetition of Patent Owner's brief, which undermines its credibility. *See id.*; Ex. 2002 ¶ 94; 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight."). As a result, we find this argument unpersuasive and insufficiently supported compared to Petitioner's contentions and evidence, discussed above.

The next argument advanced by Patent Owner is that Sourcefire's teachings do not satisfy the proper construction of "network-threat indicator" because Sourcefire allegedly teaches that the IP addresses used in intrusion rules are only "retroactively discovered to be associated with a network threat after an exploit is found in content received from that IP address."[9]

---

[9] Patent Owner also raises related issues regarding disclosures about the "Sourcefire VRT." PO Resp. 42–43. As Petitioner relies on such

PO Resp. 42 (citing Ex. 2002 ¶ 95); *see* PO Sur-reply 14–15. Aside from Dr. Orso's near-verbatim repetition of these arguments, however, Patent Owner cites no evidence to support its allegation.

Moreover, Patent Owner's characterization of Sourcefire is undercut by the disclosures of Sourcefire relied on by Petitioner. As discussed above, Sourcefire teaches 3D Sensor devices that use intrusion rules to identify exploits and other malicious activity. *See* Ex. 1004, 34, 761. According to Sourcefire, packets are examined to determine whether they match the criteria specified by the rules, in which case the rule would be triggered. *Id.* at 761. Sourcefire also teaches that rules can be selected and enabled "that would detect the attacks you think most likely to occur on your network," including "custom intrusion rules tuned to your environment." *Id.* at 34.

We find that this evidence supports Petitioner's contention that Sourcefire teaches the recited "network-threat indicator" because Sourcefire is describing measures to be taken to protect the system from malicious activity.[10] *See id.* at 34, 761. Patent Owner's allegation essentially characterizes Sourcefire's system as incapable of proactive protection, instead only "retroactively" identifying malicious activity that has already penetrated the system. That characterization, however, is inconsistent with Sourcefire's disclosures discussed above.

---

disclosures for certain dependent claims, we address them below in the context of those dependent claims.

[10] As discussed in more detail below, Sourcefire indicates that the rule may be configured as a "drop rule" such that the packet is dropped instead of being passed through, thereby preventing the packet from causing damage. *See* Ex. 1004, 761.

Patent Owner additionally argues that a person of ordinary skill "would distinguish between the use of network-threat indicators in the claimed invention and Sourcefire's use of signature or patterns," citing a document describing one of Petitioner's products. PO Sur-reply 13–14 (citing Ex. 2001, 3). But Patent Owner does not explain adequately how a description of Petitioner's product—which does not reference Sourcefire or use the term "network-threat indicator"—bears on Sourcefire's teachings or limitation 1[a] (or any specific language of claim 1). *See id*.

In addition, Patent Owner challenges Dr. Staniford's testimony on the grounds that Dr. Staniford applied a different claim construction of "network-threat indicator" than our construction, allegedly construing the term as "any rule that utilizes an IP address, port number, or URL as part of the rule criteria . . . even if the IP address is not associated with a network threat." PO Resp. 39 (citing Ex. 2008, 49:2–50:14). Patent Owner mischaracterizes Dr. Staniford's testimony, however. Dr. Staniford instead testified that he relied on examples of network-threat indicators provided in the Specification of the '722 Patent, indicating that "all of those certainly can be potentially network-threa[t] indicators under the right circumstances." Ex. 2008, 49:2–50:14. In fact, although Dr. Staniford provided his Declaration before our preliminary construction in the Decision on Institution (or, indeed, Patent Owner's Preliminary Response that proposed that construction), he confirmed that he subsequently reviewed our construction and that it does not change his opinions regarding obviousness. *Id.* at 7:23–25, 9:12–18. Thus, we discern no defect in Petitioner's reliance on the testimony of Dr. Staniford here.

For the reasons explained above, we find that Petitioner has shown by a preponderance of the evidence that Sourcefire teaches limitation 1[a].

b. Limitations 1[b]–1[d]

For limitations 1[b] through 1[d], Petitioner relies on Sourcefire's description of applying intrusion rules to packets and taking actions on those packets as specified by the rules. Pet. 39–42. Aside from its arguments discussed above with respect to limitation 1[a], which we addressed above, Patent Owner raises no further arguments regarding claim 1.

More specifically, as discussed above as well for limitation 1[a], Petitioner contends Sourcefire discloses rules that identify packets corresponding to particular source IP addresses, including the IP addresses of network threats (network-threat indicators). *Id.* at 40–41. According to Petitioner, this teaches the recited "determination by the packet-filtering device that the first packet satisfies one or more criteria . . . that correspond to one or more network-threat indicators." *Id*. We agree. Sourcefire discloses that its 3D Sensor devices "analyz[e] network traffic to check if it matches the criteria in the rule." Ex. 1004, 761. As discussed above, Sourcefire teaches the use of source IP addresses as network-threat indicators. Further, Sourcefire expressly teaches using such source IP addresses as criteria for intrusion rules. *See id.* at 764–766.

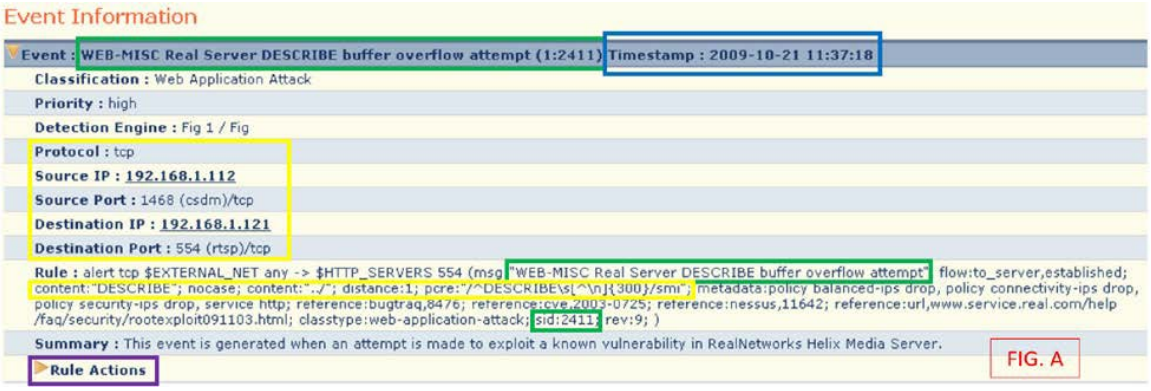
Petitioner also identifies, as the recited "operator," the "rule actions" that are specified by each rule, which are applied to a packet if the packet triggers the rule based on, for example, its source IP address (i.e., "responsive to" the determination that the rule criteria is met). *Id.* at 41–42 (citing Ex. 1004, 276–277, 761, 765). These rule actions include "pass" or "alert," which cause the packet to continue toward its destination. *Id*. We

find that this evidence supports Petitioner's contention that Sourcefire teaches applying an operator specified by the packet-filtering rule and configured to cause the first packet to continue toward its destination, as recited in claim 1.

For the above reasons, we find that a preponderance of the evidence establishes that Sourcefire teaches limitations 1[b] through 1[d] of claim 1.

c. Limitations 1[e] and 1[f]

With respect to limitations 1[e] and 1[f], Petitioner relies on Sourcefire's disclosures relating to intrusion events. Pet. 42–46. For example, Petitioner cites the figure on page 283 of Sourcefire, which is presented with annotations in the Petition (reproduced below):



Pet. 43; *see* Ex. 1004, 283 (original figure). This figure is a screenshot of Sourcefire's "packet view" interface displaying information for an intrusion event (Ex. 1004, 282–283), with Petitioner's annotations. As Petitioner asserts (Pet. 42–44), Sourcefire indicates that its 3D Sensor devices communicate such intrusion event information to the Defense Center. Ex. 1004, 253–254, 290.

Sourcefire discloses that the packet view "indicates why a specific packet was captured by providing information about the intrusion event that

the packet triggered, including . . . the rule that generated the event." Ex. 1004, 290. Petitioner notes Sourcefire's teaching that the intrusion event information includes source and destination IP addresses. Pet. 43; *see* Ex. 1004, 282–283. In light of the teachings of Sourcefire discussed above regarding using, for example, source IP addresses associated with malicious activity as network-threat indicators, we are persuaded that Sourcefire's intrusion event disclosures teach a packet-filtering device (3D Sensor) communicating information from a packet-filtering rule (intrusion rule) that identified a network-threat indicator (e.g., source IP address associated with malicious activity).

As already noted, Patent Owner argues that the specific rule depicted in the example intrusion event above does not use a network-threat indicator. *See* PO Resp. 35–38, 46–48. This argument, however, ignores the other disclosures in Sourcefire identified by Petitioner that teach using source IP addresses and similar information to detect malicious traffic, as discussed above. When taken together, we agree with Petitioner that Sourcefire's disclosures regarding both intrusion rules and intrusion events teach communicating information from a rule that identified a network-threat indicator, as recited in limitation 1[e].

For the recited "data indicative that the first packet was allowed to continue toward the destination of the first packet," Petitioner cites the figure on page 281 of Sourcefire, which is presented with annotations in the Petition (reproduced below):

Drill Down of Destination Port > Drill Down of Events > Table View of Events > Packets

2006-11-11 00:00:00 - 2006-11-11 23:59:00 Static

Search Constraints (Edit Search Save Search) Disabled Columns

Intrusion Events | RNA Events | Hosts | Host Attributes | Services | Client Apps | Flows | Vulnerabilities | Compliance Events | White List Events | Users | Remediationsstions

Time	Priority	Source IP	Destination IP	SRC Port/ICMP Type	DST Port/ICMP Code	Message
2006-11-11 20:20:44	high	10.8.12.23	10.8.11.166	35568/tcp	21 (ftp)/tcp	FTP MKD overflow attempt (1:1973)
2006-11-11 20:20:02	high	172.16.18.151	172.16.18.200	1087/tcp	21 (ftp)/tcp	FTP MKD overflow attempt (1:1973)
2006-11-11 20:19:59	high	192.168.8.112	192.168.8.98	2859/tcp	21 (ftp)/tcp	FTP MKD overflow attempt (1:1973)
2006-11-11 20:19:11	high	10.8.12.23	10.8.11.166	35568/tcp	21 (ftp)/tcp	FTP MKD overflow attempt (1:1973)
2006-11-11 20:18:29	high	172.16.18.151	172.16.18.200	1054/tcp	21 (ftp)/tcp	FTP MKD overflow attempt (1:1973)
2006-11-11 20:18:26	high	192.168.8.112	192.168.8.98	2859/tcp	21 (ftp)/tcp	FTP MKD overflow attempt (1:1973)
2006-11-11 20:17:38	high	10.8.12.23	10.8.11.166	35568/tcp	21 (ftp)/tcp	FTP MKD overflow attempt (1:1973)
2006-11-11 20:16:56	high	172.16.18.151	172.16.18.200	1054/tcp	21 (ftp)/tcp	FTP MKD overflow attempt (1:1973)
2006-11-11 20:16:53	high	192.168.8.112	192.168.8.98	2859/tcp	21 (ftp)/tcp	FTP MKD overflow attempt (1:1973)
2006-11-11 20:16:05	high	10.8.12.23	10.8.11.166	35568/tcp	21 (ftp)/tcp	FTP MKD overflow attempt (1:1973)
2006-11-11 20:15:23	high	172.16.18.151	172.16.18.200	1054/tcp	21 (ftp)/tcp	FTP MKD overflow attempt (1:1973)

View | Copy | Delete | Review | Download Packets
View All | Copy All | Delete All | Review All | Download All Packets

Next
1 2 3 4 5 6 7 8 9 10 > >|
(Showing 1 - 11 of 634)

FIG. B

Pet. 44–45; *see* Ex. 1004, 281 (original figure). This figure is a screenshot of Sourcefire's "table view of intrusion events" (Ex. 1004, 280–281), with Petitioner's annotations. Petitioner notes that this table shows for each event (i.e., each packet), an icon (annotated in red) indicating the result of the rule action applied to that packet. Pet. 44–45. For example, a black down arrow indicates the packet was dropped, whereas no icon indicates the packet was not dropped, i.e., allowed to continue. Ex. 1004, 276–277. We agree with Petitioner that this evidence shows that Sourcefire teaches communicating "data indicative that the first packet was allowed to continue toward the destination of the first packet," as recited in limitation 1[e].

Additionally, we agree with Petitioner that the packet view and table view described and depicted in Sourcefire teach "display of the information . . . corresponding to the packet-filtering rule and the one or more network-threat indicators," as recited in limitation 1[f]. *See* Pet. 45–46; Ex. 1004, 126, 280–283.

For the above reasons, we find that a preponderance of the evidence demonstrates that Sourcefire teaches limitations 1[e] and 1[f] of claim 1.

d. Limitations 1[g]–1[l]

For the remaining limitations of claim 1, Petitioner relies on Sourcefire's description of how a user can use the Sourcefire intrusion event interface to modify rules, which are then applied to packets going forward. Pet. 46–51. The Petition includes a step-by-step explanation of how Sourcefire describes using the intrusion event interface of Sourcefire to select a particular event, select the "Rule Actions" menu in packet view, and change the rule action to drop triggering packets (instead of "alert," which allows a packet to continue while generating an event) such that intrusion policies are updated with the modified rule. *Id.* at 46–49 (citing Ex. 1004, 281–283, 290–297, 358, 359; Ex. 1003 ¶¶ 132–136). According to Petitioner, these disclosures teach "modifying . . . at least one operator specified by the packet-filtering rule to reconfigure the packet-filtering device to prevent packets . . . from continuing toward their respective destinations," and doing so "responsive to" receiving an instruction from a user "invoking an element in . . . the interface," as recited in claim 1. We agree and find that the cited evidence supports Petitioner's contention.

Petitioner further explains how Sourcefire teaches that the rule, when modified to drop packets as described, would prevent a second packet from continuing toward its destination. *Id.* at 50. We agree with Petitioner. In fact, Sourcefire expressly describes "two scenarios" in which a rule is initially set to generate events (but allow a malicious packet through) in a first scenario, but is instead set to drop packets in a second scenario, in which case the "malicious packet" is dropped and "never reaches its target."

Ex. 1004, 435. Further, because drop rules also generate events, we agree with Petitioner that Sourcefire teaches "communicating . . . data indicative that the second packet was prevented from continuing," and displaying that data in the intrusion event interface, as with other intrusion events. *See id.* at 50–51 (citing Ex. 1004, 276, 290; Ex. 1003 ¶ 138).

Patent Owner does not advance any arguments regarding these limitations. We determine that the evidence cited by Petitioner supports its contentions with respect to limitations 1[g] through 1[l], and we find that Sourcefire teaches each of these limitations based on that evidence, as explained above.

e. Conclusion on Claim 1

For the reasons explained above, we find Petitioner has shown by a preponderance of the evidence that Sourcefire teaches each limitation of claim 1.

4. Dependent Claims

a. Claims 8 and 9

Claim 8 recites, "for each packet in the second portion of packets, generating the packet-log entry *while the packet-filtering device is generating one or more flow-log entries for one or more packets in the first portion of packets*" (emphasis added). Thus, claim 8 requires that the packet-log entries for the second portion of packets be generated *at the same time* that flow-log entries for the first portion of packets are generated. Claim 9 depends from claim 8.

Petitioner's argument regarding the above limitation of claim 8 refers to its arguments regarding claim 6. Pet. 65. Claim 6 recites "updating, . . .

based on a packet-log entry, a packet-flow log to indicate" that a packet satisfies one or more criteria and whether the packet was prevented from continuing, or allowed to continue, toward its destination. In its arguments for claim 6, Petitioner mentions a "refresh interval":

> Sourcefire discloses that this count (and therefore the packet-flow log in which it is contained) could be periodically updated. Specifically, Sourcefire discloses that "event preferences" could be selected by the user to configure basic characteristics of event views in the Sourcefire 3D System. [Ex. 1004, 46-47]; [Ex.]1003 ¶ 162. One of these characteristics was the "refresh [or update,] interval" which updated event information (e.g., count (orange)) displayed in the packet flow log at the user-selected refresh interval.

Pet. 60. As to claim 8, Petitioner refers to the above argument and states the following:

> As discussed above with respect to Claim 6, a user could set a "refresh interval" for the event data being displayed such that a packet log entry and a flow log entry was refreshed at a selected time interval which caused the flow log entry to be generated while the packet log entry was being generated. [Ex.]1003 ¶173.

Id. at 65. These largely conclusory arguments, however, fail to explain how refreshing an event view or event summary page, whether at a regular interval or otherwise, teaches *generating* different types of log entries *at the same time* for different portions of packets in the manner claimed. The cited testimony of Dr. Staniford does not provide any further illumination, instead repeating essentially the same conclusory statements made in the Petition. *See* Ex. 1003 ¶¶ 162, 173; 37 C.F.R. § 42.65(a).

Petitioner's Reply also fails to supply the necessary explanation or supporting evidence. Petitioner notes that "flow-log entries are generated from the packet-logs"—thus, flow-log entries must be generated after the

corresponding packet-log entries and would reflect any changes made to those entries. Pet. Reply 19–21. Although true, these facts pertain only to a single portion of packets, i.e., that their packet-log entries are generated first, and that the related flow-log entries are generated afterward. The same is true even considering that this process can occur at a predetermined "refresh interval." Petitioner does not identify any specific teaching or suggestion in Sourcefire that indicates how the generation of log entries for two different portions of packets would operate. Instead, Petitioner relies on a bare assertion—without any specific basis in Sourcefire—that "the processing of the packet-logs and the flow-logs are continually being updated or refreshed." Without sufficient supporting evidence, that bare assertion and the conclusory testimony of Dr. Staniford are inadequate to meet Petitioner's burden to prove the unpatentability of these claims by a preponderance of the evidence.

b. Claims 10 and 14

Claim 10 depends from claim 1 and recites that "each of the plurality of network-threat indicators corresponds to at least one network threat of a plurality of network threats," and that "each of the plurality of packet-filtering rules corresponds to a different network threat of the plurality of network threats." For the latter limitation, Petitioner cites Sourcefire's disclosure of event messages that identify a plurality of network threats (e.g., exploits). Pet. 68 (citing Ex. 1004, 278, 281). Patent Owner does not dispute that Sourcefire teaches this limitation. We find that Petitioner's showing is sufficient because Sourcefire discloses that event messages, such as those cited by Petitioner, are "pulled from the rule" for rule-based

intrusion events and, thus, demonstrate a correspondence between a plurality of rules and a plurality of different network threats. *See* Ex. 1004, 278.

For the "network-threat indicators" limitation of claim 10, Petitioner relies *inter alia* on its arguments for claim 1 regarding network-threat indicators associated with network threats. *See* Pet. 67. For similar reasons discussed above for claim 1, we find those arguments and supporting evidence persuasive. Aside from its arguments relating to claim 1, which we addressed above, Patent Owner additionally argues that an example event message cited in the Petition does not teach the recited network-threat indicators. PO Resp. 48–50 (citing Pet. 67–68). Whether or not that specific example alone teaches network-threat indicators, however, is not the proper inquiry for obviousness. Rather, we consider all of the teachings identified by Petitioner, which we determine support Petitioner's contention that Sourcefire teaches the limitations of claim 10 as explained above.

Claim 14, which also depends from claim 10, recites "determining, by the packet-filtering device, an ordering of the plurality of network threats," and "indicating, in the interface, the ordering." In addition to its arguments for claims 1 and 10, Petitioner relies on Sourcefire's description of its event interface, which allows ordering of displayed intrusion events (and, thus, their associated network threats) in ascending or descending order. Pet. 72 (citing Ex. 1004, 1611–1612). Specifically, Petitioner notes that the "table view" of the interface displays the identification of the network threat associated with each intrusion event, which is ordered when the table entries are ordered. *See* Pet. Reply 23–24 (citing Ex. 1004, 1611–1612; Pet. 45).

Patent Owner argues that the disclosures identified by Petitioner teach only the ordering of events, not network threats. PO Resp. 56–57; PO Sur-

reply 22–23. This argument, however, does not cite or rely on any evidence and, thus, constitutes mere attorney argument, which we find unpersuasive. Upon review of the arguments and evidence presented by Petitioner, we agree with Petitioner's analysis and find that Sourcefire teaches the limitations of claim 14 on that basis.

c. Claims 13, 22, and 23

Claim 13 recites that generating the data indicating whether a packet was prevented from continuing, or allowed to continue, to its destination comprises "generating the data *based on the packet-flow-log entry* that corresponds to the particular network threat" (emphasis added). Petitioner's sole statement regarding this limitation in the Petition is: "The indication in Sourcefire's flow log regarding whether the packets were dropped was generated from data in the event log corresponding to the network threat." Pet. 71. This statement is conclusory, and neither it nor the material cited in support explains sufficiently how Sourcefire teaches the recited limitation.

In its Reply, Petitioner adds that an annotated figure it provided regarding claim 12 shows a depiction in Sourcefire of a flow-log that identifies rules, associated network threats, and associated "block option[s]." Pet. Reply 22–23. But again, Petitioner fails to adequately explain how that figure teaches generating data indicating whether a packet was blocked or allowed *based on the packet-flow-log entry*—indeed, the figure simply depicts packet-flow-log entries. *See id*. Nor do we find persuasive Petitioner's conclusory statement that "[t]his is the same information that is used to generate an entry in the packet-log," for which no evidentiary support is identified. *See id.* at 23. Thus, we conclude that Petitioner did not

show that Sourcefire teaches the limitations of claim 13 by a preponderance of the evidence.

Claim 22 recites, "determining an order of the first network threat relative to the second network threat based on a determination that the first portion of the plurality of network-threat-intelligence reports was received from a greater number of the one or more network-threat-intelligence providers than the second portion of the plurality of network-threat-intelligence reports." Although admitting that Sourcefire does not disclose prioritizing network threats based on the number of network-threat-intelligence providers providing reports, Petitioner asserts doing so would have been obvious because "it was well known and a matter of common sense that agreement between sources would serve to increase confidence in the network threat." Pet. 83–84. The only evidence cited is a paragraph of Dr. Staniford's Declaration, which is essentially identical to the Petition and does not provide any further explanation or evidence. *See* Ex. 1003 ¶ 212.

In its Reply, Petitioner points to arguments it made with respect to claim 21, but again admits that Sourcefire does not disclose prioritizing or ordering network threats based on the *number* of network-threat-intelligence providers, as recited in claim 22. *See* Pet. Reply 24–25. Petitioner also does not identify or present any additional evidence. We conclude that Petitioner did not meet the burden of demonstrating by a preponderance of the evidence that Sourcefire teaches the limitations of claim 22.

Similarly, claim 23 recites ordering network threats "based on data . . . indicating a number of the plurality of different packet-filtering devices that have reconfigured an operator of the first packet-filtering rule to prevent packets . . . from continuing toward their respective destinations." As with

claim 22, Petitioner's contentions regarding this limitation are conclusory and supported only with a citation to testimony from Dr. Staniford that merely parrots the same contentions without providing further explanation or evidence. *See* Pet. 86; Ex. 1003 ¶ 216.

In its Reply, Petitioner directs us to arguments it made with respect to claim 10 regarding Sourcefire's disclosure of event information including "counts" of the number of times a given rule was triggered to produce an event. *See* Pet. Reply 25–26 (citing Pet. 67–68). We are not persuaded, however, that a count of how many times a rule was triggered teaches the recited "number of . . . *different packet-filtering devices* that have *reconfigured an operator*" (emphases added). Petitioner presents only unsupported attorney argument on that issue. *See id*. Thus, we conclude that Petitioner has not met its burden to show the unpatentability of claim 23 by a preponderance of the evidence.

d. Claim 19

Claim 19 depends from claim 10 and recites that receiving the plurality of packet-filtering rules comprises "receiving a plurality of packet-filtering rules generated based on a plurality of network-threat-intelligence reports produced by one or more network-threat-intelligence providers." Petitioner relies on Sourcefire's teachings regarding the "Sourcefire Vulnerability Research Team" ("Sourcefire VRT"). Pet. 75–78. Specifically, Sourcefire describes how the Sourcefire VRT "regularly sends out updates called Security Enhancement Updates, or SEUs, that can contain *new intrusion rules* . . . so you can be sure that you are detecting the most recently released attacks." Ex. 1004, 254. The Sourcefire VRT "continues to add rules as new vulnerabilities and exploits are discovered." *Id.* at 869.

Petitioner also explains how Sourcefire teaches adding information to intrusion rules that reflect reports and other information about a network threat.[11] *See* Pet. 76–77. We are persuaded by Petitioner's arguments and find that the evidence discussed above shows that Sourcefire teaches receiving a plurality of packet-filtering rules (intrusion rules) generated based on a plurality of network-threat-intelligence reports (information on network threats) produced by one or more network-threat-intelligence providers (the Sourcefire VRT or others who produce the information on network threats referenced in the rules). *See* Ex. 1003 ¶¶ 198–199.

Patent Owner disputes that Sourcefire teaches these limitations of claim 19, but we find its arguments unpersuasive. Specifically, Patent Owner asserts that Petitioner has not shown that the information about reports on network threats described in Sourcefire include network-threat indicators. PO Resp. 51–52. As Patent Owner notes (*id.*), the Specification of the '722 Patent describes an embodiment in which "[n]etwork-threat-intelligence providers 130, 132, and 134 may . . . disseminate (e.g., to subscribers) network-threat-intelligence reports that include network-threat indicators . . . associated with the network threats." Ex. 1001, 3:18–26. As discussed above, however, the evidence supports Petitioner's contention that Sourcefire teaches generating intrusion rules to detect network threats based on information about those threats. *See* Pet. 76–78. And as discussed with

[11] In the Reply, Petitioner asserts for the first time that Sourcefire's SEUs teach the recited "network-threat-intelligence reports." Pet. Reply 18. We do not consider this argument because it is was not included in the Petition and, thus, is untimely. Moreover, Petitioner does not explain how intrusion rules are "generated based on" the SEUs when the rules in question are themselves contained in the SEUs. *See* Ex. 1004, 254.

respect to claim 1 above, Sourcefire teaches intrusion rules based on network-threat indicators. Thus, we are persuaded that a person of ordinary skill in the art would have understood Sourcefire to teach generating rules based on information about network threats, including information constituting network-threat indicators that form part of the criteria applied by the rule (e.g., source IP address). *See* Ex. 1003 ¶¶ 198–199.

For the above reasons, we conclude that Petitioner has shown by a preponderance of the evidence that Sourcefire teaches the limitations of claim 19.

e. Claims 2–7, 11, 12, 15–18, 20, 21, 24, and 25

Claims 2–7, 24, and 25 depend from claim 1; claims 11 and 12 depend from claim 10; claims 15–18 depend from claim 14; and claims 20 and 21 depend from claim 19. Petitioner contends these claims are obvious in view of Sourcefire. Pet. 51–65, 69–75, 86–89. Aside from its arguments regarding the claims from which they depend, which are unpersuasive for the same reasons discussed above, Patent Owner raises no other arguments with respect to the limitations of these claims.

Having reviewed Petitioner's arguments and the evidenced cited in support, we agree with the reasoning set forth in the Petition regarding claims 2–7, 11, 12, 15–18, 20, 21, 24, and 25, and determine that the record evidence supports Petitioner's contentions. Therefore, based on the Petition's analysis and the evidence relied on therein, we find that a preponderance of the evidence shows that Sourcefire teaches each limitation of claims 2–7, 11, 12, 15–18, 20, 21, 24, and 25.

f. Conclusion on Dependent Claims

For the reasons explained above, we find Petitioner has shown by a preponderance of the evidence that Sourcefire teaches each limitation of claims 2–7, 10–12, 14–21, 24, and 25. We find that Petitioner has not shown by a preponderance of the evidence that Sourcefire teaches each limitation of claims 8, 9, 13, 22, and 23.

5. Secondary Considerations of Non-Obviousness

Before determining whether a claim is obvious in light of the prior art, we consider any relevant evidence of secondary considerations—i.e., objective indicia—of non-obviousness. *See Graham*, 383 U.S. at 17. Notwithstanding what the teachings of the prior art would have suggested to one of ordinary skill in the art at the time of the invention, the totality of the evidence submitted, including objective evidence of non-obviousness, may lead to a conclusion that the challenged claims would not have been obvious to one of ordinary skill. *In re Piasecki*, 745 F.2d 1468, 1471–72 (Fed. Cir. 1984). Patent Owner presents evidence of three such considerations: (1) long-felt but unmet need/failure of others, (2) industry praise, and (3) commercial success/licensing. PO Resp. 58–67.

"In order to accord substantial weight to secondary considerations in an obviousness analysis, the evidence of secondary considerations must have a nexus to the claims, i.e., there must be a legally and factually sufficient connection between the evidence and the patented invention." *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019) (internal quotations omitted). A nexus is presumed when "the patentee shows that the asserted objective evidence is tied to a specific product and that product 'embodies the claimed features, and is coextensive with them.'" *Id.* (quoting

Polaris Indus., Inc. v. Arctic Cat, Inc., 882 F.3d 1056, 1072 (Fed. Cir. 2018)). If the product is not coextensive with the claims at issue—e.g., if the patented invention is only a component of the product—the patentee is not entitled to a presumption of nexus. *See id.* (citing *Demaco Corp. v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392 (Fed. Cir. 1988)).

a. Long-Felt But Unmet Need and Failure of Others

According to Patent Owner, "[t]he '722 Patent satisfied a long-felt need in the industry that others had failed to solve—namely, how to operationalize threat intelligence to proactively identify network threats." PO Resp. 59. Patent Owner presents evidence praising Patent Owner's "RuleGATE" product while identifying certain purported challenges to "provid[ing] proactive network protection that could scale to larger networks" and "operationalizing threat intelligence." *Id.* at 59–62. Further, Patent Owner identifies evidence about purported advantages of its products, such as "processing hundreds of millions of indicators from thousands of feeds," "better manag[ing] traffic by leveraging [cyber threat intelligence (CTI)] context with highly granular rules in the form of policies that can be automatically enforced," dynamic updating of intelligence, real time reporting of results for "live analytics," "best-in-class performance [due to] the fact that the dynamic security policies implement rules on a packet-by-packet basis." *Id.*

Patent Owner's arguments and evidence, however, are insufficient to establish a nexus between the alleged long-felt but unmet need, and the claimed invention. First, no analysis is presented to demonstrate that any product, including RuleGATE, is coextensive with any claim of the '722 Patent. Thus, Patent Owner is not entitled to a presumption of nexus. *See*

Fox Factory, 944 F.3d at 1373. Patent Owner's conclusory assertion that its "RuleGATE product practices [the '722 Patent and other patents]" is insufficient and unpersuasive. *See* PO Sur-reply 25–26; PO Resp. 62–63.

Second, insufficient analysis is presented to show that the evidence of a purported long-felt but unmet need is connected to the patented invention. The only mention of any challenged claim is a conclusory statement that limitation 1[a] of claim 1 corresponds to "converting indicators to rules that drive actions across a risk spectrum." PO Resp. 62. Patent Owner does not explain how limitation 1[a], or any aspect of any challenged claim, relates to a "risk spectrum." The paper from which Patent Owner derived the reference to a "risk spectrum" (the "ESG Paper") indicates that "converting indicators to rules that drive actions across a risk spectrum" refers to "logging, content capture, mirroring, redirection, shielding, and advanced threat detection." Ex. 2006, 7.[12] Patent Owner makes no attempt to demonstrate that limitation 1[a], or any aspect(s) of any challenged claim, relates to, for example, "content capture" or "mirroring." With respect to other "challenges" reported in the ESG Paper—e.g., "[l]ack of automation" and "the inability to use feeds 'in a meaningful way to live network traffic'" (PO Resp. 61)—Patent Owner provides no analysis as to how the patented invention purportedly meets those challenges.

---

[12] Petitioner argues that the ESG Paper is not objective evidence of non-obviousness because it is a report commissioned and paid for by Patent Owner. Pet. Reply 26–27. We decline to disregard this evidence, or Dr. Orso's testimony about it, entirely. We find, however, that the nature and circumstances around the genesis of the ESG Paper diminish the persuasive weight it should be accorded.

Further, Patent Owner also does not explain how the challenged claims relate to processing "hundreds of millions of indicators," or "leveraging CTI context with highly granular rules in the form of policies that can be automatically enforced," or "dynamic security policies [that] implement rules on a packet-by-packet basis." PO Resp. 62–63. Indeed, these seem clearly outside the scope of the challenged claims. For example, claim 1 recites, at most, a "plurality of network-threat indicators" (i.e., as few as two indicators), not hundreds of millions.

Therefore, we conclude that a nexus was not proven between the purported long-felt but unmet need(s) identified by Patent Owner and the patented invention of the '722 Patent.

b. Industry Praise

Patent Owner cites the ESG Paper (Ex. 2006) as well as a Gartner article (Ex. 2007) and an American Banker article (Ex. 2011) as evidence of industry praise. PO Resp. 63–65. Similar to its long-felt need contentions, however, Patent Owner does not provide sufficient analysis or explanation to establish the requisite nexus. Patent Owner again provides no analysis demonstrating that any Centripetal product is coextensive with the challenged claims, so no presumption of nexus is applied. *See Fox Factory*, 944 F.3d at 1373. Additionally, the cited praise of Centripetal products is not linked sufficiently to the challenged claims, including because Patent Owner failed to address lauded features with no relationship to the claims.

For example, Patent Owner cites the ESG Paper as praising the "high performance" of its product, its ability to process "hundreds of millions of indicators from thousands of feeds," "synthesizing into a network policy," "complex filtering rule[s]" with "at-least a dozen unique fields which had to

be evaluated and applied bi-directionally and without state," etc. Ex. 2006, 7. None of these features appear to be in the challenged claims. Patent Owner does not address whether they are part of the claimed invention or, if not, their relative contribution to the industry praise compared to any actual features of the claimed invention.

Regarding the Gartner article, Patent Owner notes that Gartner praises its product's "ability to instantly detect and prevent malicious network connections based on millions of threat indicators at 10-gigabit speeds," "the largest number of third-party threat intelligence service integrations," and using "5 million indicators simultaneously." Ex. 2007, 5; *see* PO Resp. 64. Again, insufficient analysis is presented to address how these features relate to the challenged claims. Patent Owner's reference to the American Banker article similarly suffers from a lack of explanation. *See* PO Resp. 64–65.

The only nexus explanation provided is a conclusory assertion that "the salutary benefits of [the praised products] are made possible in large part by the '722 Patent's packet-filtering rules, which transform network-threat indicators into actionable rules." *Id.* at 65. Dr. Orso's testimony cited in support of this statement is merely a near-verbatim copy of this conclusory statement with no additional explanation. *See* Ex. 2002 ¶ 123; 37 C.F.R. § 42.65(a). As a result, we find that Patent Owner has not established a sufficient nexus between the cited industry praise and the invention of the challenged claims.

c. Commercial Success and Licensing

Finally, Patent Owner contends that the commercial success of its RuleGATE product as well as a license to the '722 Patent taken by Keysight

Technologies are compelling secondary considerations of non-obviousness. PO Resp. 65–67. We disagree.

First, we note that the sole evidence cited for the commercial success of the RuleGATE product, a declaration by Mr. Jonathan Rogers of Centripetal, makes no mention whatsoever of the ’722 Patent. *See* Ex. 2016. Rather, the Rogers Declaration is testimony that was submitted in a different *inter partes* review challenging a different patent. *See id*. As such, there is no record evidence supporting any nexus between the matters in Mr. Rogers’ testimony on alleged commercial success and the ’722 Patent.

Second, as Patent Owner itself admits (PO Resp. 66), the Keysight license was a “worldwide, royalty-bearing, non-transferable, irrevocable, non-terminable, non-exclusive license to Centripetal’s worldwide patent portfolio.” Ex. 2012, 88. No information is provided about the relevant details of this license—e.g., how many patents comprise the portfolio, the relative contributions of the patents in the portfolio to the value of the license—such that we could discern whether Keysight took the license “out of recognition and acceptance of the subject matter claimed” in the ’713 Patent. *See In re GPAC Inc.*, 57 F.3d 1573, 1580 (Fed. Cir. 1995). In fact, the record evidence indicates that this license was taken to settle litigation (Ex. 2012, 88), which diminishes its probative value as an indicator of non-obviousness. *See GPAC*, 57 F.3d at 1580. As such, we find that Patent Owner has not provided sufficient evidence to establish the requisite nexus between the Keysight license and the ’722 Patent. *See id*.

6. Conclusion as to Obviousness

As discussed above, Petitioner has shown by a preponderance of the evidence that Sourcefire teaches each limitation of claims 1–7, 10–12, 14–

21, 24, and 25. We further determine that Petitioner's showing that the claims are taught by Sourcefire is strong, particularly in comparison to Patent Owner's weak showing with respect to the asserted secondary considerations of obviousness. As discussed above, we find that Patent Owner has not established the requisite nexus between the challenged claims and *any* of the asserted secondary considerations. As such, we are unable to accord them any substantial weight. *See Fox Factory*, 944 F.3d at 1373. Therefore, in weighing the totality of the evidence of record and the strength of the parties' showings on the inquiries underlying the question of obviousness, we conclude that Petitioner has met its overall burden of proving by a preponderance of the evidence that 1–7, 10–12, 14–21, 24, and 25 would have been obvious in view of Sourcefire.

Also as discussed above, we determine that Petitioner has not shown that Sourcefire teaches each limitation of claims 8, 9, 13, 22, and 23. Thus, we conclude that Petitioner has not met its overall burden to prove the unpatentability of these claims.

E. Motions to Exclude and Other Matters

1. Petitioner's Motion to Exclude (Paper 29, "Pet. Mot.")

Petitioner moves to exclude Exhibits 2003, 2005–2007, 2011–2013, and 2016. Pet. Mot. 2. Exhibits 2003 and 2005 did not form the basis for any aspect of this Decision. As such, Petitioner's Motion with respect to those exhibits is moot.

For Exhibit 2016, the Rogers Declaration, Petitioner asserts that it should be excluded under Rules 401, 402, and 403 of the Federal Rules of Evidence. Pet. Mot. 10–11. We agree with Patent Owner that exclusion is unwarranted. Paper 32, 5–7. We note that Patent Owner relies on Exhibit

2016 to support its arguments for commercial success, which specifically note the alleged success of the RuleGATE product. PO Resp. 65. Although the Rogers Declaration addresses a different patent than the '722 Patent, its testimony regarding the RuleGATE product and Centripetal's customers generally meets the threshold for relevance, and its purported shortcomings as evidence go to its persuasive weight rather than its admissibility. We also discern no risk of unfair prejudice. Thus, Petitioner's objections under Rules 401, 402, and 403 are denied.

Petitioner argues that Exhibits 2006, 2007, and 2011–2013 should be excluded under Rules 401, 402, 403, 901, and as hearsay (under Rule 802). Pet. Mot. 7–9. We are not persuaded. Each of these exhibits is cited by Patent Owner as evidence supporting its arguments regarding secondary considerations of non-obviousness, including as evidence of industry praise and the existence of a relevant license. *See* PO Resp. 59–66. Although they may not identify the '722 Patent specifically (Pet. Mot. 7), we determine that they meet the threshold for relevance nonetheless, and we discern no risk of unfair prejudice, confusion, or waste of time. Regarding authentication, we note that the Declaration of Jeffrey H. Price (Ex. 2018) provides evidence of the source of each of these exhibits, and we find that this information along with the distinctive characteristics of the exhibits themselves (including dates, titles, publication names, etc.) provide the necessary basis for authentication.[13] With respect to Petitioner's hearsay objections, we conclude first that Exhibits 2007 and 2011 are not hearsay because they are

[13] We further note that at least Exhibits 2007 and 2011 are printed material purporting to be from news sources, which are self-authenticating under Rule 902(6).

not relied on for the truth of the matters asserted. *See* Fed. R. Evid. 801(c). These exhibits are cited only as evidence of industry praise; their relevance lies in that they include statements from the industry allegedly praising Centripetal's invention, not in whether that praise is true or accurate. *See* PO Resp. 64–65. For the remaining exhibits, we deny Petitioner's hearsay objection under Rule 807 because we conclude that the totality of the circumstances provides sufficient indicia of trustworthiness—for example, these exhibits are contemporaneous documents by third parties produced for purposes that indicate their statements are likely reliable (e.g., Keysight's official Annual Report (Ex. 2012))—and these exhibits generally are highly probative on the points underlying Patent Owner's secondary considerations allegations (e.g., industry praise) compared to different evidence reasonably available to Patent Owner.

For the above reasons, we are not persuaded that any of these exhibits should be excluded and, thus, we deny Petitioner's Motion to Exclude.

2. Patent Owner's Motion to Exclude (Paper 28, "PO Mot.")

Patent Owner moves to exclude Exhibits 1038 and 1042. PO Mot. 1. Exhibit 1038 did not form the basis for any aspect of this Decision. Thus, Patent Owner's Motion is moot as to that exhibit.

For Exhibit 1042 (the Baugher Declaration), Patent Owner objects on the basis of Rule 403 and 37 C.F.R. § 42.61. *Id*. The crux of Patent Owner's objections is that the Baugher Declaration was submitted with Petitioner's Reply instead of the Petition, which Patent Owner considers to be untimely. *Id.* at 1–4. According to Patent Owner, the timing of the Baugher Declaration's submission was unfairly prejudicial to Patent Owner,

including because Patent Owner was denied an opportunity to seek additional discovery related to his testimony. *Id*.

As an initial matter, we note that Patent Owner's objections to the Baugher Declaration did not include any objection based on Rule 403. *See* Paper 21, 3. Thus, Patent Owner did not preserve a Rule 403 objection to the Baugher Declaration, and we deny that objection at least for that reason. *See* 37 C.F.R. § 42.64 (b)(1), (c).

We also agree with Petitioner, however, that the Baugher Declaration was not unfairly prejudicial. *See* Paper 31. As Petitioner explains (*id.* at 2–5), the Baugher Declaration was submitted to address arguments raised in the Patent Owner Response in compliance with our rules. *See* 37 C.F.R. § 42.23(b) ("A reply may only respond to arguments raised in the corresponding opposition, patent owner preliminary response, or patent owner response."). Specifically, the Patent Owner Response asserted that another declarant, Mr. Leone, had insufficiently accounted for his testimony regarding the amount of sales of Sourcefire products. *See* PO Resp. 6–7. Mr. Baugher's testimony corroborated Mr. Leone's testimony and provided information regarding the source for that testimony, which addressed issues raised by Patent Owner. *See* Paper 31, 3.

Although the substance of Mr. Baugher's testimony was known to Petitioner at the time the Petition was filed (*see* PO Mot. 3), that subject matter *was* presented with the Petition in the form of Mr. Leone's testimony. The Baugher Declaration did not introduce any new theory of unpatentability, or any new factual issue regarding the public accessibility of Sourcefire. The issue of whether Sourcefire was disseminated as part of sales of Sourcefire products, and the scope of those sales, was properly

raised in the Petition and supported by the Leone Declaration. *See* Pet. 24 (citing Ex. 1005); *cf. Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369 (Fed. Cir. 2016) (approving of the Board's exclusion of new arguments raised *for the first time* in a reply). Although the Baugher Declaration provided additional evidence relevant to those issues, it was appropriately provided to address specific arguments and allegations in the Patent Owner Response, as explained above. Thus, we determine that the Baugher Declaration was not untimely filed.

Moreover, we note that Patent Owner had the opportunity to depose Mr. Baugher, and did so. *See* Ex. 2017. Patent Owner also had the opportunity to address Mr. Baugher's testimony in its Sur-reply, and did so, including by presenting testimony it elicited during Mr. Baugher's deposition. *See* PO Sur-reply 8–10. Thus, we disagree that Patent Owner was unfairly prejudiced by the timing of the Baugher Declaration.

Patent Owner also asserts that it was prevented from obtaining discovery on purported "restrictions" on the dissemination of Sourcefire that Mr. Baugher allegedly disclosed at this deposition. PO Mot. 3–4. We note that this issue was raised by Mr. Baugher's deposition testimony under questioning by Patent Owner, not the Baugher Declaration. *See id*. Additionally, we note that Patent Owner was previously aware of the issue of restrictions on dissemination and access, which Patent Owner itself raised in its Response. *See* PO Resp. 3–5, 10. Patent Owner did not, however, avail itself of an earlier opportunity to seek discovery on that issue, declining to depose Petitioner's original declarant on public accessibility issues, Mr. Leone. As a result, we conclude that the totality of the circumstances indicates that Patent Owner was not unfairly prejudiced.

For the above reasons, we are not persuaded that any of the exhibits challenged by Patent Owner should be excluded and, thus, we deny Patent Owner's Motion to Exclude.

3. Patent Owner's Request to File a Motion for Supplemental Information

Just prior to the oral hearing, Patent Owner contacted the Board to request authorization to file a motion to submit supplemental information, which was considered at the prehearing conference. *See* Ex. 1046, 4:3–7. Specifically, Patent Owner sought to introduce evidence of the allowance of a patent stemming from a continuation of the application that led to the '722 Patent. *See id.* at 5:23–6:9. We denied the request, principally because the request came very late in the case and, thus, would unfairly prejudice Petitioner as well as disrupt the parties' and the Board's preparations for the oral hearing and the case schedule. *See id.* at 10:3–11:1, 11:23–12:13. Under those circumstances, we were not persuaded that the potential probative value of the proposed evidence—which concerned a related but different patent with different claims[14]—outweighed the potential prejudice to Petitioner and disruption to the case. *See id*.

We note, however, that Patent Owner nonetheless raised the proposed evidence during the oral hearing, our ruling on its request notwithstanding. *See* Tr. 34:14–35:6. We emphasize that the proposed evidence is not part of the record of this case, and we do not consider any arguments pertaining to such evidence. Further, we expect all parties appearing before the Board to

---

[14] We note that the patent application in question was, at the time, still unpublished and not publicly available. *See id.* at 5:14–19.

comply with our rules, and all rulings made by the Board during one of our proceedings.

CONCLUSION[15]

For the foregoing reasons, Petitioner has shown by a preponderance of the evidence that certain challenged claims of the '722 Patent are unpatentable, as summarized in the following table:

Claims	35 U.S.C. §	Reference(s)	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–25	103	Sourcefire	1–7, 10–12, 14–21, 24, 25	8, 9, 13, 22, 23
Overall Outcome			1–7, 10–12, 14–21, 24, 25	8, 9, 13, 22, 23

ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–7, 10–12, 14–21, 24, and 25 of the '722 Patent are held unpatentable as obvious under 35 U.S.C. § 103 in view of Sourcefire;

---

[15] Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding. See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. See 37 C.F.R. § 42.8(a)(3), (b)(2).

FURTHER ORDERED that claims 8, 9, 13, 22, and 23 of the ’722 Patent are not held as obvious under 35 U.S.C. § 103 in view of Sourcefire;

FURTHER ORDERED that Petitioner’s Motion to Exclude (Paper 29) is *denied* as set forth above;

FURTHER ORDERED that Patent Owner’s Motion to Exclude (Paper 28) is *denied* as set forth above;

FURTHER ORDERED that, because this is a final written decision, parties to the proceeding seeking judicial review of this Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

Patrick McPherson
Patrick Muldoon
Joseph Powers
Christopher Tyson
pdmcpherson@duanemorris.com
pcmuldoon@duanemorris.com
japowers@duanemorris.com
cjtyson@duanemorris.com

PATENT OWNER:

James Hannah
Jeffrey Price
Jonathan Caplan
Michael Lee
Bradley Wright
jhannah@kramerlevin.com
jprice@kramerlevin.com
mhlee@kramerlevin.com
bwright@bannerwitcoff.com