Trials@uspto.gov
571-272-7822

Paper 40
Date: February 9, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, LLC,
Patent Owner.

IPR2021-01147
Patent 10,542,028 B2

Before KEVIN F. TURNER, BRIAN J. McNAMARA, and LYNNE E. PETTIGREW, *Administrative Patent Judges*.

PETTIGREW, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 314

I. BACKGROUND

Petitioner, Palo Alto Networks, Inc., challenges claims 1–21 ("the challenged claims") of U.S. Patent No. 10,542,028 B2 (Ex. 1001, "the '028 patent"). We have jurisdiction under 35 U.S.C. § 6, and we issue this Final Written Decision under 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons discussed below, Petitioner has shown, by a preponderance of the evidence, that claims 1–21 of the '028 patent are unpatentable.

A. Procedural History

Petitioner filed a Petition for *inter partes* review of the challenged claims. Paper 2 ("Pet."). Patent Owner, Centripetal Networks, LLC,[1] filed a Preliminary Response. Paper 7. With our authorization, Petitioner filed a Preliminary Reply (Paper 8) and Patent Owner filed a Preliminary Sur-reply (Paper 9) to address Board discretion under 35 U.S.C. § 314(a). Applying the standard set forth in 35 U.S.C. § 314(a), which requires demonstration of a reasonable likelihood that Petitioner would prevail with respect to at least one challenged claim, we instituted an *inter partes* review of the challenged claims. Paper 10 ("Institution Decision" or "Inst. Dec.").

Following institution, Patent Owner filed a Patent Owner Response (Paper 19, "PO Resp."), Petitioner filed a Reply (Paper 26, "Pet. Reply"), and Patent Owner filed a Sur-reply (Paper 28, "PO Sur-reply"). A consolidated oral hearing for IPR2021-01147 and IPR2021-01148 was held on November 1, 2022, and a copy of the hearing transcript has been entered into the record. Paper 35.

[1] Patent Owner filed a notice indicating that, on December 30, 2022, its corporate name changed from Centripetal Networks, Inc. to Centripetal Networks, LLC. Paper 36.

B. Real Parties-in-Interest

Petitioner identifies Palo Alto Networks, Inc. as the real party-in-interest. Pet. 4. Patent Owner identifies Centripetal Networks, LLC as the real party-in-interest. Paper 36, 1.

C. Related Matters

Petitioner and Patent Owner identify the following district court proceeding involving the '028 patent: *Centripetal Networks, Inc. v. Palo Alto Networks, Inc.*, No. 2:21-cv-00137 (E.D. Va., filed Mar. 12, 2021). Pet. 4; Paper 3, 1.

Additionally, Petitioner cites to the Final Written Decision in an *inter partes* review involving U.S. Patent No. 9,413,722 B2 (Ex. 1029, "the '722 patent"), which is related to the '028 patent. *See, e.g.*, Pet. 1–2 (citing *Cisco Sys., Inc. v. Centripetal Networks, Inc.*, IPR2018-01760, Paper 41 (PTAB May 18, 2020) (Ex. 1031, "IPR2018-01760 FWD")); *see also Centripetal Networks, Inc. v. Cisco Sys., Inc.*, 847 F. App'x 881 (Fed. Cir. 2021) (affirming Board's Final Written Decision in IPR2018-01760) (Ex. 1053).

D. Overview of the '028 Patent

The '028 patent relates to "rule-based network-threat detection." Ex. 1001, 1:48–49. The '028 patent 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 1:53–55. The packet-filtering rule criteria may correspond to one or more "network threat indicators." *Id.* at 1:55–57. Examples of network-threat indicators include "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

3:27–38. Network-threat-intelligence providers may be associated with services that monitor network threats and disseminate network-threat-intelligence reports that include network-threat indicators. *Id.* at 3:22–27. Network-threat-intelligence providers may communicate network-threat-intelligence reports to rule providers, which generate packet-filtering rules based on the network-threat-intelligence reports. *Id.* at 4:36–59, 5:4–9, Figs. 3A, 3B. A rule provider may communicate packet-filtering rules to a packet-filtering device, which may update its packet-filtering rules to include the rules generated by the rule provider. *Id.* at 5:9–13, Fig. 3B. A packet-filtering rule may specify an "operator" to be applied by the packet-filtering device when the rule is triggered, the operator being configured to cause the device to prevent the packet from continuing toward its destination or allow the packet to continue toward its destination. *Id.* at 1:57–61.

The packet-filtering device may generate a log entry comprising information from the packet-filtering rule that identifies the network-threat indicators specified in the rule and indicates whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination. *Id.* at 1:61–67. The

packet-filtering device generates two types of log data—packet log data and flow log data, as shown in Figure 5G of the '028 patent, reproduced below:

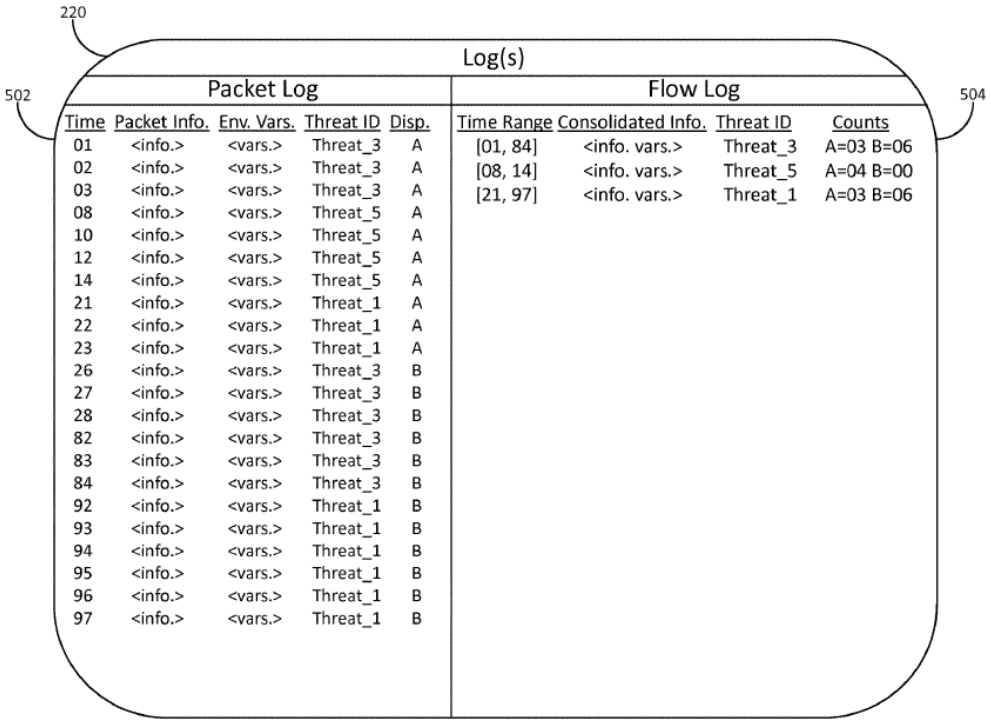

FIG. 5G

Id. at 6:34–39. Figure 5G, above, shows packet log data (left side) and flow log data (right side) generated by a packet-filtering device. *Id.* at 6:34–39, 7:31–38. Each packet log entry includes data for an individual packet that has been filtered by the packet-filtering device. *Id.* at 6:39–40, 7:31–34. As shown in Figure 5G, each packet log entry includes a hit time for the packet (e.g., the time when the packet-filtering device received the packet), data derived from the packet (e.g., source address, destination address, port number, protocol type, domain name, URL, URI, or the like), environmental variables, a Threat ID, and an indication of whether the packet-filtering device prevented the packet from continuing toward its destination or allowed it to continue toward its destination. *Id.* at 6:40–63. Each flow log

entry consolidates, compresses, or summarizes entries of the packet log. *Id.* at 7:38–39.

The packet-filtering device may communicate flow log information to a user device, which presents the information in a user interface. *Id.* at 7:52–8:17. For example, Figure 6E of the '028 patent, reproduced below, shows an interface providing data from flow log entries:

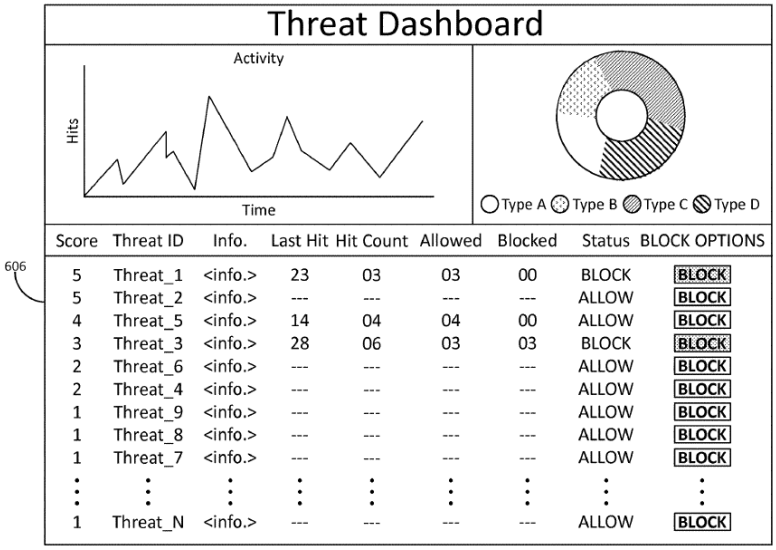

FIG. 6E

Figure 6E, above, is a "Threat Dashboard" interface with entries corresponding to network threats including, for each threat, information from a flow log and the status of the operator included in the rule associated with the threat. *Id.* at 8:5–17.

Figure 7 of the '028 patent, reproduced below, is a flow chart illustrating an embodiment of the disclosed method:

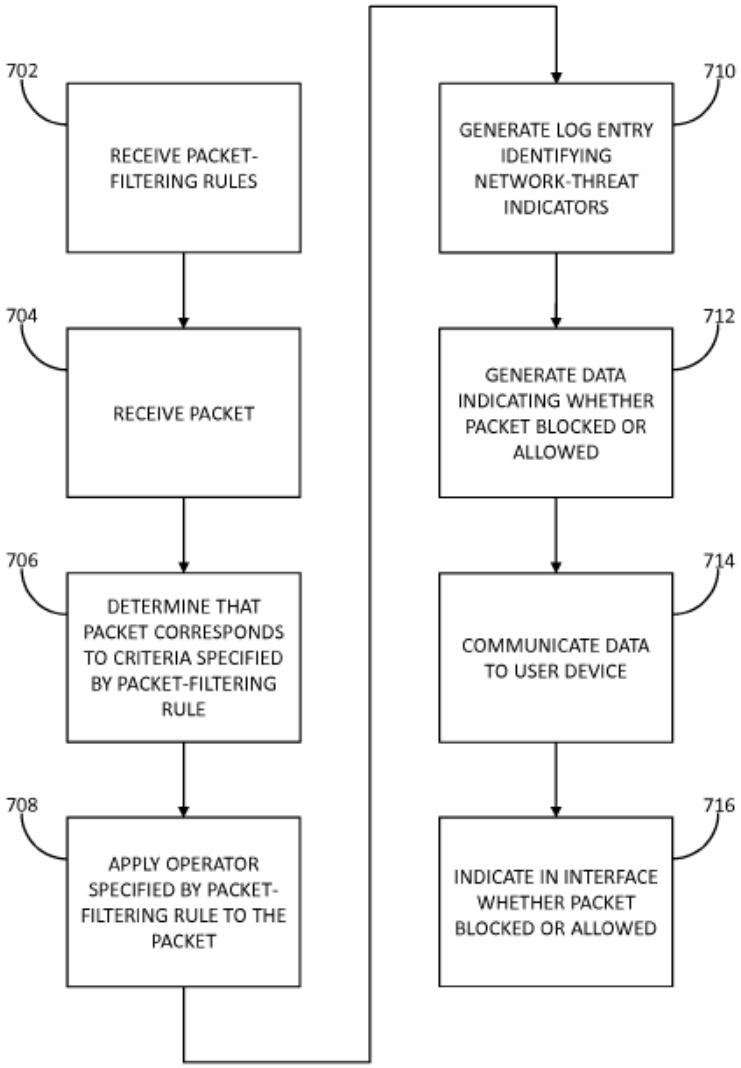

FIG. 7

Figure 7, above, depicts an illustrative method for rule-based network-threat detection. *Id.* at 16:14–15; *id.* at 16:16–63 (describing in detail each step depicted in Figure 7).

E. Challenged Claims

Challenged claims 1, 8, and 15 are independent, claims 2–7 depend directly or indirectly from claim 1, claims 9–14 depend directly or indirectly from claim 8, and claims 16–21 depend directly or indirectly from claim 15. Claim 1 is illustrative of the claimed subject matter and is reproduced below:

1. A method, comprising:

[1.a1] 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, [1.a2] wherein the plurality of network-threat indicators are associated with network-threat-intelligence reports supplied by one or more independent network-threat-intelligence providers;

[1.b] receiving, by the packet filtering device, a plurality of packets that comprises a first packet and a second packet;

[1.c1] responsive to a determination by the packet filtering device that the first packet satisfies a first packet filtering rule, of the plurality of packet filtering rules, based on one or more network-threat indicators, of the plurality of network-threat indicators, specified by the first packet filtering rule:

applying, by the packet filtering device and to the first packet, an operator specified by the first 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; and

[1.c2] communicating, by the packet filtering device, information 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;

[1.d] receiving, by the packet filtering device, an update to at least one packet filtering rule;

[1.e] modifying, by the packet filtering device and based on the received update to the at least one packet filtering rule, at least one operator specified by the first packet filtering rule

to reconfigure the packet filtering device to prevent packets corresponding to the one or more network-threat indicators from continuing toward their respective destinations; and

[1.f1] responsive to a determination by the packet filtering device that the second packet satisfies the first packet filtering rule:

preventing, by the packet filtering device and based on the modified at least one operator specified by the first packet filtering rule, the second packet from continuing toward a destination of the second packet; and

[1.f2] communicating, by the packet filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet.

Ex. 1001, 17:47–18:28 (annotated to include Petitioner's identification of claim limitations).

F. Asserted Ground of Unpatentability

We instituted *inter partes* review of the challenged claims based on the following ground of unpatentability asserted by Petitioner:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–21	103	Sourcefire[2]

Inst. Dec. 2, 5; *see* Pet. 7.

G. Testimonial Evidence

In support of the unpatentability contentions in its Petition, Petitioner relies on a declaration of Dr. Wenke Lee. *See* Ex. 1003. Patent Owner cross-examined Dr. Lee via deposition. *See* Exs. 2037, 2038.

In support of its Patent Owner Response, Patent Owner relies on a declaration of Dr. Alessandro Orso. *See* Ex. 2019. Petitioner cross-examined Dr. Orso via deposition. *See* Ex. 1073.

[2] Sourcefire 3D System User Guide, Ver. 4.10, Mar. 16, 2011 (Ex. 1004, "Sourcefire").

II. DISCUSSION

A. Principles of Law

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 ordinary skill in the art; and (4) when in evidence, objective indicia of non-obviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

To prevail on its challenges to Patent Owner's claims, Petitioner must demonstrate by a preponderance of the evidence that the claims are unpatentable. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d). "In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable." *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify "with particularity . . . the evidence that supports the grounds for the challenge to each claim")).

B. 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. 17; *see* Ex. 1003 ¶ 31. In addition, Petitioner indicates 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." Pet. 17; *see* Ex. 1003 ¶ 31. Petitioner further asserts that "[a]dditional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education." Pet. 17; *see* Ex. 1003 ¶ 31.

In the Institution Decision, we noted that Patent Owner did not dispute Petitioner's assessment of the level of ordinary skill in the art, and we adopted Petitioner's assessment for purposes of institution based on the information presented in the Petition and Dr. Lee's testimony. Inst. Dec. 17 (citing Ex. 1003 ¶¶ 30–32). Patent Owner does not dispute the level of ordinary skill in the art proposed by Petitioner and adopted at institution. *See* PO Resp.

On the complete record, we maintain the definition of the level of ordinary skill in the art adopted at institution, which is consistent with the '028 patent and the prior art of record.

C. Claim Construction

In this *inter partes* review, we apply the same claim construction standard that would be used in a civil action under 35 U.S.C. § 282(b). 37 C.F.R. § 42.100(b) (2019). In applying this standard, we generally give claim terms their ordinary and customary meaning as would be understood by a person of ordinary skill in the art at the time of the invention and in the context of the entire patent disclosure. *See id.*; *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005) (en banc).

Petitioner proposes a construction of "network-threat indicators," and Patent Owner proposes a construction of the longer phrase in claim 1 containing that term. Patent Owner also proposes an explicit construction of

"responsive to." We address these two claim terms below. No other claim terms in the '028 patent require construction for purposes of this Decision. *See Realtime Data LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) ("The Board is required to construe 'only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy." (quoting *Vivid Techs., Inc. v. Am. Sci. Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

1. "network-threat indicators are associated with network-threat-intelligence reports supplied by one or more independent network-threat-intelligence providers"

Petitioner argues that the term "network-threat indicator" should be construed to mean "indicator that represents the identity of a resource associated with a network threat." Pet. 19. Petitioner asserts that "[t]his construction is consistent with the specification, which provides examples of 'network-threat indicators' including 'network addresses, ports, fully qualified domain names (FQDNs), uniform resource locators (URLs), uniform resource identifiers (URIs), or the like.'" *Id.* (quoting Ex. 1001, 3:27–31) (citing Ex. 1001, 1:26–27, 4:42–44). Petitioner also notes that the Board adopted this construction in the IPR2018-01760 FWD, involving the related '722 patent and the same written description as the '028 patent, and Patent Owner did not challenge the construction in its appeal to the Federal Circuit. *Id.* at 19–20 (citing Ex. 1031, 8; *Centripetal Networks*, 847 F. App'x at 887 (Ex. 1053)). Petitioner further indicates that, in a district court proceeding involving the '722 patent,[3] Patent Owner adopted a construction of "network-threat indicator" similar to that proposed by Petitioner here.

[3] *Centripetal Networks, Inc. v. Keysight Techs., Inc.*, No. 2:17-cv-00383 (E.D. Va.).

Pet. Reply 5 (citing Ex. 1093, 21 (Dkt. 117) (Patent Owner adopting defendant's proposed construction); Ex. 1094, 5–6 (Dkt. 104) (defendant proposing that "network-threat indicators" be construed as "indicators of packets associated with network threats, such as network addresses, ports, domain names, uniform resource locators (URLs), or the like")).

Patent Owner contends that the longer claim phrase "network-threat indicators . . . associated with network-threat-intelligence reports supplied by one or more independent network-threat-intelligence providers," recited in the independent claims, means "at least one indicator that represents the identity of a resource *previously determined* to be associated with a network threat in a network threat intelligence report." PO Resp. 19 (emphasis added); *see* PO Sur-reply 3–4; Ex. 2019 ¶ 61. Patent Owner asserts that the "claims are written in the past tense, indicating a previous occurrence." PO Resp. 20. For example, Patent Owner contends, the independent claims require network-threat indicators to be "*associated with* network-threat-intelligence reports *supplied by* . . . network-threat-intelligence providers." *Id.* (emphasis modified) (quoting Ex. 1001, 17:52–55, 19:43–46, 21:36–39). Patent Owner also contends that the specification contains similar statements, such as "network-threat-intelligence providers . . . that *provided* the network-threat-intelligence reports"). *Id.* (quoting Ex. 1001, 5:38–39) (citing Ex. 1001, 1:52–55, 5:2–3, 5:6–8, 5:48–50, 5:51–53, 5:64–65, 5:67–6:1).

According to Patent Owner, "[t]here is no dispute that 'network-threat indicators' must come from a 'network-threat-intelligence report'" because "[t]he specification is clear the reports include network-threat indicators." PO Resp. 19 n.1. Patent Owner contends that a person of ordinary skill in the art would have understood "as a matter of simple logic that these

[network-threat-intelligence] reports and indicators of a resource included in those reports must have been previously determined to be associated with a network threat at the time the 'network-threat-intelligence providers' supply the 'network-threat-intelligence reports.'" *Id.* at 20 (citing Ex. 2019 ¶¶ 62–63). In other words, Patent Owner contends, "to appear in a network-threat-intelligence report, the network-threat indicator must already identify a known network-threat resource." *Id.* at 21 (citing Ex. 2019 ¶¶ 62–63).

Patent Owner further contends that the claims refer to "network-threat indicators" "in a backward-looking manner" because they recite "receiving . . . 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." PO Resp. 21 (quoting Ex. 1001, 17:48–51, 19:40–43, 21:33–36). In Patent Owner's view, for the packet filtering device "[t]o be capable of identifying packets corresponding to network-threat indicators, the network-threat indicator must already have been known and the resource it identifies must have already been determined to be associated with a network threat." *Id.* (citing Ex. 2019 ¶¶ 62–63).

Patent Owner additionally contends that "[t]he specification repeatedly and consistently describes 'network-threat intelligence reports' as including 'network-threat indicators' identifying resources already known to be 'associated' with network threats." PO Resp. 22 (citing Ex. 1001, 3:22–31, 4:36–44, 4:47–58, 4:65–5:9, 5:36–37, 5:50–56). Moreover, Patent Owner continues, the specification explains how rule providers generate packet-filtering rules "based on" the "provided" reports and their network-threat indicators, which may occur only if the resources identified by the network-threat indicators have already been determined to be associated with network threats at the time the rules are generated. *Id.* at 22–23 (citing

Ex. 1001, 5:4–9, 5:14–26, 5:50–56, 5:65–6:4; Ex. 2019 ¶¶ 62–63). Patent Owner reiterates that the received packet filtering rules must include network-threat indicators that "identify a resource already known, or previously determined to be associated with a network threat in a network-threat-intelligence report." PO Sur-reply 4 (citing PO Resp. 20–24; Ex. 2019 ¶¶ 62–64).

We begin with the language of the claims. *See Phillips*, 415 F.3d at 1312. The independent claims of the '028 patent recite that the "network-threat indicators *are associated with* network-threat-intelligence reports." Ex. 1001, 17:52–54, 19:43–45, 21:36–38 (emphasis added). Contrary to Patent Owner's arguments, nothing in the claim language indicates that the network-threat indicators "must come from" or be "included in" a network-threat-intelligence report. *See* PO Resp. 19 n.1, 20; Pet. Reply 5–6 (citing PO Resp. 19 n.1, 22, 28–41). Thus, we are not persuaded by Patent Owner's claim construction arguments to the extent they are premised on an understanding that network-threat indicators must "come from" or be "included in" a network-threat-intelligence report.

Moreover, we do not agree with Patent Owner that the claims are written in the past tense or use backward-looking language in a way that indicates that a network-threat indicator must represent the identity of a resource previously determined to be associated with a network threat in a network-threat-intelligence report. The relevant claim language involving network-threat indicators and network-threat-intelligence reports recites that "network-threat indicators *are associated with* network-threat-intelligence reports." This language describes network-threat indicators as currently being associated with network-threat-intelligence reports, not as being *previously determined* to be associated with network threats or network-

threat-intelligence reports. Furthermore, we do not see how the claim language reciting "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" cited by Patent Owner requires a network-threat indicator to have been previously determined to be associated with a network threat.

We turn next to the specification. *See Phillips*, 415 F.3d at 1315. Patent Owner cites passages disclosing that network-threat-intelligence reports may include network-threat indicators and argues that these network-threat indicators identify resources previously determined to be associated with network threats. PO Resp. 22 (citing Ex. 1001, 3:22–31, 4:36–44, 4:47–58, 4:65–5:9, 5:36–37, 5:50–56). The claims of the '028 patent, however, do not require network-threat indicators to be "included" in network-threat-intelligence reports, but instead recite that "network-threat indicators are associated with network-threat-intelligence reports." Patent Owner also cites passages allegedly showing that packet filtering rules can be generated "based on" network-threat-intelligence reports only if the resources identified by the network-threat indicators have already been determined to be associated with network threats at the time the rules are generated, but the claims of the '028 patent do not recite packet filtering rules "based on" network-threat-intelligence reports. We are not persuaded by Patent Owner's specification arguments, at least because they relate to aspects of disclosed embodiments that are not specifically claimed. Furthermore, Patent Owner does not cite, nor do we see, any disclosure in the specification describing "network-threat indicators associated with network-threat-intelligence reports," as recited in the independent claims, as

identifying a resource previously determined to be associated with a network threat.

As for the term "network-threat indicator" itself, the specification provides examples of network-threat indicators that include "network addresses, ports, fully qualified domain names (FQDNs), uniform resource locators (URLs), uniform resource identifiers (URIs), or the like," and describes them as "associated with network threats." Ex. 1001, 3:27–31. We agree with Petitioner that this disclosure supports its proposed construction of "network-threat indicator" as an "indicator that represents the identity of a resource associated with a network threat." *See* Pet. 19. Patent Owner does not specifically challenge Petitioner's construction of "network-threat indicator" other than arguing that it does not account for requirements of the full phrase "network-threat indicators . . . associated with network-threat-intelligence reports supplied by . . . independent network-threat-intelligence providers." *See, e.g.*, PO Sur-reply 3–5.

For these reasons, we construe "network-threat indicator" to mean "indicator that represents the identity of a resource associated with a network threat." We decline Patent Owner's invitation to read into the longer phrase "network-threat indicators are associated with network-threat-intelligence reports supplied by one or more independent network-threat-intelligence providers" a requirement that a network-threat indicator represent the identity of a resource *previously determined* to be associated with a network threat in a network-threat-intelligence report. Instead, we find that no construction of that longer claim phrase is necessary.

2. "responsive to"

The independent claims recite steps of "applying" operators and "communicating" information "responsive to a determination by [a] packet

filtering device that . . . [a] packet satisfies a . . . packet filtering rule . . . based on . . . network-threat indicators . . . specified by the . . . packet filtering rule." *E.g.*, Ex. 1001, 17:59–18:7. Patent Owner argues that the "responsive to" language requires the applying and communicating steps to "be performed in reaction to a packet satisfying a packet-filtering rule based on network-threat indicators included in 'network-threat-intelligence reports' supplied by an 'independent network-threat-intelligence provider.'" PO Resp. 26 (emphasis added) (citing Ex. 2019 ¶¶ 66–69). In Patent Owner's view, this language "establishes a clear cause-and-effect relationship between (i) a packet satisfying a packet-filtering rule . . . and (ii) the subsequent application of an operator that allows the packet and communication of data indicating the packet was allowed." *Id.* (citing Ex. 2019 ¶ 67).

As discussed in the previous section, the claims do not require network-threat indicators to be "included in" network-threat-intelligence reports, so we disagree with that portion of Patent Owner's proposed construction. Petitioner does not otherwise challenge Patent Owner's construction of "responsive to," primarily disputing Patent Owner's characterization of the prior art with respect to this limitation. *See* Pet. Reply 16–18. To the extent interpretation of this term is necessary, we consider the meaning of the claim language in the context of determining whether the prior art teaches or suggests the limitations at issue.

D. Obviousness over Sourcefire

Petitioner contends that claims 1–21 of the '028 patent are unpatentable under 35 U.S.C. § 103 as obvious over Sourcefire. Pet. 21–77 (citing Ex. 1003). Patent Owner disagrees, arguing that Petitioner does not show that Sourcefire teaches or suggests every limitation of the independent

claims or explain sufficiently why Sourcefire renders the claims obvious. PO Resp. 28–62. For the reasons discussed below, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 1–21 are unpatentable for obviousness over Sourcefire.

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 each can run the Sourcefire "Intrusion Prevention System" (IPS), which allows monitoring of networks for attacks by examining packets for malicious activity. *Id.* at 33–34. The 3D Sensors running IPS use "rules . . . to look for the broad range of exploits that attackers have developed." *Id.* at 34. Users can create custom "intrusion rules" to examine packets for attacks, and users can manage the rules across all the 3D Sensors in the system through a centralized "Defense Center." *Id.* at 34, 254.

An intrusion rule detects attempts to exploit vulnerabilities on a network by analyzing network traffic to determine whether it matches criteria in the rule. *Id.* at 761. 3D Sensors with IPS compare packets against the conditions specified in each rule and, if the conditions are met, the rule triggers. *Id.* Intrusion rules can be "pass" rules, "alert" rules, or "drop" rules. *Id.* If a pass rule is met, the packet is ignored and allowed to continue. *Id.* If an alert rule is met, an "intrusion event" is generated. *Id.* If a drop rule is met, the packet is dropped and an intrusion event is generated. *Id.*

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

A rule includes a rule header and a rule options section. *Id.* at 762. The rule header includes source and destination IP addresses and ports and a parameter that specifies the action the system takes when a packet triggers the rule. *Id.* at 762–69. The rule options section includes keywords and their parameters and arguments, which may include "contextual information that describes the vulnerability that the rule detects attempts to exploit," and may include "external references to vulnerability databases." *Id.* at 770–71.

When a 3D Sensor with IPS identifies a possible intrusion, it generates an intrusion event, which is a record including "the date, time, and the type of exploit, as well as other contextual information about the source of the attack and its target," along with the details of the packet or packets that triggered the rule. *Id.* at 276, 2084. Sourcefire describes workflows, populated with intrusion event information, that allow a user to view and analyze intrusion events. *Id.* at 274–82. Viewable information includes an "Inline Result" indicating whether packets that triggered the rule were dropped or allow to continue. *Id.* at 276–77. The interface allows a user to view the specific rule triggered for each event and to modify the operator of the rule. *Id.* at 281–83, 293–99.

2. Collateral Estoppel

Throughout its unpatentability analysis, Petitioner contends that collateral estoppel precludes Patent Owner from arguing that Sourcefire does not teach various claim limitations similar to those in claims of the '722 patent determined to be unpatentable in the Board's final written decision in IPR2018-01760. Pet. 32, 35, 38, 40, 42–44, 46–48, 50, 52, 55, 58, 61, 64–65, 69, 71, 74 (citing Ex. 1030 (petition in IPR2018-01760); Ex. 1031 (IPR2018-01760 FWD)); Pet. Reply 2–4; *see also Centripetal Networks, Inc. v. Cisco Sys.*, 847 F. App'x 881 (Fed. Cir. 2021) (opinion

affirming IPR2018-01760 FWD) (Ex. 1053). In response, Patent Owner argues that collateral estoppel does not apply because (1) this proceeding involves a different claim construction standard (i.e., the *Phillips* standard rather than the broadest reasonable interpretation standard applied in the IPR2018-01760 FWD), (2) the claim language is not the same, and (3) the relevant issues were not actually litigated and decided in IPR2018-01760. PO Resp. 31–33, 59 n.6, 62 n.8; PO Sur-reply 1–2, 6–8.

"Issue preclusion [i.e., collateral estoppel] is appropriate only if: (1) the issue is identical to one decided in the first action; (2) the issue was actually litigated in the first action; (3) resolution of the issue was essential to a final judgment in the first action; and (4) plaintiff had a full and fair opportunity to litigate the issue in the first action." *In re Freeman*, 30 F.3d 1459, 1465 (Fed. Cir. 1994); *see also MaxLinear, Inc. v. CF CRESPE LLC*, 880 F.3d 1373, 1376 (Fed. Cir. 2018) (holding that issue preclusion applies in the administrative context).

We agree with Patent Owner regarding the applicability of collateral estoppel. As Patent Owner points out, the claims of the '722 patent determined to be unpatentable in IPR2018-01760 were subject to a different claim construction standard than the claims in this proceeding. Moreover, as discussed herein, the claims of the '028 patent and those of the '722 patent have some similarities, but the claim recitations are not identical. Therefore, we evaluate the arguments and evidence presented in this proceeding to determine whether Petitioner has demonstrated, by a preponderance of the evidence, that the challenged claims are unpatentable, rather than assuming that Patent Owner is generally estopped from asserting that Sourcefire does not teach or suggest the limitations of the challenged claims. Nevertheless,

where appropriate, we consider the Petition's citations to the Board's IPR2018-01760 FWD, which is part of the record in this proceeding.

3. Independent Claims 1, 8, and 15

Petitioner asserts that independent claim 1, a method claim, is representative of independent claim 8, a device claim, and independent claim 15, directed to one or more non-transitory computer-readable media. Pet. 32. With the exception of the preambles of each claim and limitation [8.a], reciting "at least one processor; and memory comprising instructions that, when executed by the at least one processor, cause the packet filtering device to [perform recited functions]," Petitioner addresses the limitations of the independent claims together. *Id.* at 32–48. We concur with Petitioner's analysis and address the preambles of the independent claims and the remaining limitations of claim 1 below. Patent Owner does not dispute Petitioner's contentions regarding the correspondence of limitations for the independent claims.

a. Preambles and Limitation [8.a]

With respect to the preamble of claim 1, Petitioner asserts that Sourcefire discloses a method for aggregating network intelligence while defending the network against external threats. Pet. 32–33 (citing Ex. 1004, 33). With respect to claim 8, Petitioner asserts that Sourcefire discloses a packet filtering device (e.g., 3D Sensor with IPS) comprising instructions (e.g., 3D System software installed on the 3D Sensor) that, when executed by at least one processor (e.g., CPU), cause the packet filtering device to perform the subsequent actions. *Id.* at 33–34 (citing Ex. 1004, 33, 68, 90, 107, 204). With respect to claim 15, Petitioner asserts that Sourcefire discloses one or more non-transitory computer-readable media (e.g., memory and disk storage) comprising instructions (e.g., 3D System software

installed on the 3D Sensor) that, when executed by one or more processors (e.g., CPU), cause the packet filtering device to perform the subsequent actions. *Id.* (citing Ex. 1004, 33, 68, 90, 107, 204).

Patent Owner does not advance any arguments regarding the preambles of claims 1, 8, and 15 and limitation [8.a]. *See* PO Resp. 28–56. Having considered Petitioner's arguments and supporting evidence, we are persuaded that Sourcefire teaches the preambles of claims 1, 8, and 15 and limitation [8.a].[5]

b. Limitations [1.a1] and [1.a2]

Limitation [1.a1] of claim 1 recites the step of "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 as the recited "packet filtering device." Pet. 34–38 (citing Ex. 1004, 34, 107, 254); *see* Ex. 1003 ¶ 137. For the recited "packet filtering rules," Petitioner asserts that Sourcefire's 3D Sensor receives from the Defense Center intrusion policies that include custom intrusion rules created by a user on the Defense Center, intrusion rules developed by the Sourcefire Vulnerability Research Team (VRT), and Security Enhancement Updates (SEUs) that can contain new and updated intrusion rules. Pet. 34–38 (citing Ex. 1004, 34, 35, 105, 107, 117, 254, 2084, 2093); *see* Ex. 1003 ¶¶ 137–138. With respect to the recited "network-threat indicators," Petitioner relies on Sourcefire's disclosure regarding custom intrusion rules that can be created by a user to examine packets and match traffic traveling to or from specific

[5] We need not determine whether the preambles are limiting because Petitioner shows that Sourcefire teaches them.

source and destination IP addresses or ports associated with a network threat. Pet. 34–38 (citing Ex. 1004, 254, 861–63, 761, 766–67); *see* Ex. 1003 ¶ 139. As Dr. Lee points out, the '028 patent identifies network addresses and ports as examples of "network-threat indicators." *See* Ex. 1001, 3:27–38; Ex. 1003 ¶ 139.

Limitation [1.a2] further recites that "the plurality of network-threat indicators are associated with network-threat-intelligence reports supplied by one or more independent network-threat-intelligence providers." Petitioner relies on Sourcefire's disclosure that an intrusion rule may include one or more references to "external web sites" that "provide data on known exploits." Pet. 38 (citing Ex. 1004, 763, 776). Sourcefire provides examples of external web sites (i.e., external attack identification systems), including Bugtraq, CVE, and Nessus, that identify specific network vulnerabilities maintained in databases. *See id.* at 38–39 (citing Ex. 1004, 763 (intrusion rule referring to "bugtraq, 1818," "cve, 1999-0191," and "nessus, 10360"), 776 (table listing "some of the external systems that can provide data on known exploits and attacks," including Bugtraq and CVE), 1060, 1067). Citing the testimony of Dr. Lee, Petitioner contends that a person of ordinary skill in the art would have understood that such external websites are "independent network-threat-intelligence providers" that provide "network-threat-intelligence reports" identifying network vulnerabilities. *Id.* at 38 (citing Ex. 1003 ¶ 142).

In view of these teachings in Sourcefire, Petitioner contends that a person of ordinary skill in the art would have understood that intrusion rules received from Sourcefire's Defense Center are based on reports from independent network-threat-intelligence providers. *Id.* at 38–39 (citing Ex. 1004, 283, 776, 873–74 (referring to, for example, "rules based on all or

part of the Bugtraq ID," "rules based on all or part of the CVE number," and "rules based on all or part of the Nessus ID"); Ex. 1003 ¶ 142). At a minimum, Petitioner argues, a person of ordinary skill in the art would have been motivated to have Sourcefire's 3D Sensors apply intrusion rules to identify packets corresponding to at least one of a plurality of network-threat indicators associated with the reports supplied periodically by the independent network-threat-intelligence providers because doing so would increase network security by monitoring for newly identified threats. *Id.* (citing Ex. 1003 ¶ 143). Petitioner and Dr. Lee also note that the Board found in the IPR2018-01760 FWD that Sourcefire teaches a similar claim limitation in the '722 patent. *Id.* at 38 (citing Ex. 1031, 40–42); Ex. 1003 ¶ 141 (citing Ex. 1031, 40–42).

Patent Owner disputes that Sourcefire teaches or suggests "network-threat indicators . . . associated with network-threat-intelligence reports." PO Resp. 28–44. First, Patent Owner argues that the alleged network-threat-intelligence reports from the external attack identification systems named in Sourcefire and cited by Petitioner (i.e., Bugtraq, CVE, and Nessus) do not include source and destination IP addresses or any other indicator that represents the identity of a resource associated with a network threat. *Id.* at 30–31 (citing Pet. 23–26, 37–40; Ex. 1004, 763, 776; Ex. 2019 ¶¶ 77–78); *see id.* at 39 (similarly arguing that "[t]he cited portions of Sourcefire . . . include no indication that the information received from external attack identification systems include any indication of the identify of a resource associated with the network threat"). These external attack identification systems, Patent Owner contends, "provide data on known exploits and attacks" but provide no information indicating the source of malicious traffic exploiting vulnerabilities. *Id.* at 30–31 (citing Ex. 1004, 763; Ex. 2019

¶¶ 77–78); *see id.* at 40 (citing Ex. 1004, 776; Ex. 2010, Ex. 2013; Ex. 2019 ¶¶ 77–81). Patent Owner argues that Sourcefire does not explain where the IP addresses (which Petitioner alleges are "network-threat indicators") would have come from, if not from the user, and, in any event, they do not come from reports issued by the external attack identification systems named in Sourcefire. *Id.* at 33 (citing Ex. 2019 ¶¶ 77–81); *id.* at 39 (citing Pet. 38–39). Patent Owner concludes that Petitioner has failed to show that Sourcefire teaches "network-threat-intelligence reports" that are "supplied by one or more independent network-threat-intelligence providers" and that "include" at least one indicator that represents the identity of a resource associated with a network threat (i.e., a network-threat indicator). *Id.* at 33.

As an initial matter, claim 1 does not require the network-threat indicators to "come from" or be "included in" the network-threat-intelligence reports, as discussed above in our claim construction section. *See supra* § II.C.1. Instead, the claimed network-threat indicators are only "associated with" the network-threat-intelligence reports. Therefore, it is not necessary for Sourcefire to disclose network-threat indicators *included in* network-threat-intelligence reports, as Patent Owner argues, in order for Sourcefire to teach or suggest the recited claim limitations.

Patent Owner's arguments also assume that an obviousness analysis must consider only three particular examples of external attack identification systems referred to in Sourcefire—Bugtraq, CVE, and Nessus. We disagree. The Petition asserts that "Sourcefire discloses that an intrusion rule may include, as part of the rule, one or more references to a specific network vulnerability identified by 'external web sites'" and then identifies three external web sites shown in a Sourcefire graphic illustrating portions of a rule. Pet. 38 (citing Ex. 1004, 763). The Petition also cites a Sourcefire

table listing "some of the external systems that can provide data on known exploits and attacks." Ex. 1004, 776; *see* Pet. 38–39 (citing Ex. 1004, 763; Ex. 1003 ¶¶ 142–143); Pet. Reply 8–9 (citing Ex. 1004, 776; Ex. 1003 ¶ 142; Ex. 2037, 100:7–101:4). We remain persuaded that the Petition cites those three systems as examples of external attack identification systems (i.e., network-threat-intelligence providers), and a person of ordinary skill in the art would have understood that Sourcefire teaches, or at least suggests, other external systems that identify network vulnerabilities. *See* Pet. 38–39 (citing Ex. 1004, 283, 762–63, 776); Pet. Reply 8–9; Ex. 2037, 88:10–11 (Dr. Lee testifying that Sourcefire lists "examples of threat information providers"); Inst. Dec. 29–30.

Furthermore, as Petitioner highlights in its Reply, Dr. Lee's testimony cited in the Petition demonstrates, with evidentiary support, that independent network-threat-intelligence providers that distributed listings of network-threat indicators, upon which packet filtering rules were based, were well-known in the art. *See* Pet. Reply 10–11 (citing Ex. 1003 ¶¶ 55–56, 71, 75–82, 142–143; Ex. 1039 ¶ 86; Ex. 1005; Ex. 1044); Pet. 38–39 (concluding that a person of ordinary skill in the art "would have understood that the rules provided by the Defense Center are based on reports from independent network-threat-intelligence providers, or at minimum would have found it obvious to use such reports for such purpose") (citing Ex. 1003 ¶¶ 142–143). Dr. Lee also notes that the background section of the '028 patent states that organizations "subscribe to network-threat services that periodically provide information associated with network threats, for example, reports that include listings of network-threat indicators." Ex. 1003 ¶ 143 (quoting Ex. 1001, 1:23–26). We do not understand Petitioner to be relying on this disclosure other than as corroboration for

Dr. Lee's other testimony on this point, and we agree that it provides further support for the understanding espoused by Dr. Lee. *See* Pet. 38–39; Pet. Reply 11–13.

Patent Owner also argues that source and destination IP addresses in an intrusion rule do not identify a resource that has been *previously determined* to be associated with a network threat. PO Resp. 33–38. That argument relies on Patent Owner's proposed claim construction of "network-threat indicator," which we have not adopted. *See supra* § II.C.1. Therefore, we find this argument to be unpersuasive.

For these reasons, we are persuaded by Petitioner's arguments and supporting evidence that a person of ordinary skill in the art would have understood Sourcefire to teach or suggest creating intrusion rules (i.e., "packet filtering rules") to identify packets corresponding to network-threat indicators, such as source and destination IP addresses, associated with network-threat-intelligence reports supplied by independent network-threat-intelligence providers. Patent Owner's arguments do not undermine Petitioner's showing. Thus, we are persuaded that Sourcefire teaches or suggests limitations [1.a1] and [1.a2].

c. Limitation [1.b]

For limitation [1.b], which recites "receiving, by the packet filtering device, a plurality of packets that comprises a first packet and a second packet," Petitioner relies on Sourcefire's description of a 3D Sensor with IPS (i.e., the claimed packet filtering device) examining packets (including first and second packets) that traverse the network for malicious activity. Pet. 40–41 (citing Ex. 1004, 276, 281; Ex. 1003 ¶¶ 144–146).

Patent Owner does not advance any arguments regarding this limitation. *See* PO Resp. 28–56. Having considered Petitioner's arguments

and supporting evidence, we are persuaded that Sourcefire teaches limitation [1.b].

d. Limitations [1.c1] and [1.c2]

These limitations require "a determination by the packet filtering device that the first packet satisfies a first packet filtering rule . . . based on one or more network-threat indicators . . . specified by the first packet filtering rule," and, "responsive to" that determination, applying an operator specified by the rule to cause the packet filtering device to allow the first packet to continue toward a destination (limitation [1.c1]), and communicating information that identifies the one or more network-threat indicators and data indicating that the first packet was allowed to continue toward the destination (limitation [1.c2]). Ex. 1001, 17:59–18:7.

For the recited "determination," Petitioner cites Sourcefire's disclosure of intrusion rules that are triggered when the 3D Sensor with IPS receives packets that match the conditions specified in a rule. Pet. 41–42 (citing Ex. 1004, 435, 761, 765; Ex. 1003 ¶¶ 147–149). Petitioner identifies as the recited "operator" the "action the system takes when a packet triggers a rule," as specified by a parameter in the rule header. *Id.* (citing Ex. 1004, 761, 765). In particular, an alert rule with a rule state of "Generate Events" is configured to allow the packet that triggered the rule to continue toward its destination. *Id.* (citing Ex. 1004, 435). Regarding the "communicating" step, Petitioner asserts that an alert rule in Sourcefire generates an intrusion event, which is a record of traffic that violates the intrusion policy and contains information such as the source and destination IP addresses (i.e., network-threat indicators), and communicates the intrusion event to the Defense Center. *Id.* at 42–43 (citing Ex. 1004, 122, 256, 254, 276, 435; Ex. 1003 ¶¶ 152–153). Petitioner also cites Sourcefire's teaching that an

intrusion event generated by an alert rule includes an "Inline Result" indicating that the triggered rule allowed the packet to continue toward its destination. *Id.* at 43–44 (citing Ex. 1004, 276, 435). Additionally, Petitioner and Dr. Lee note that the Board found in the IPR2018-01760 FWD that Sourcefire teaches similar limitations in claim 1 of the '722 patent.[6] *Id.* at 42–43 (Ex. 1031, 29–33); Ex. 1003 ¶¶ 148, 151 (citing Ex. 1031, 29–33).

Patent Owner disputes that Sourcefire teaches applying an operator and communicating information "responsive to a determination" that a packet satisfies the rule "based on" the network-threat indicators identified by Petitioner (i.e., source and destination IP addresses). PO Resp. 44–56. According to Patent Owner, Sourcefire's 3D Sensors use intrusion rules to detect intrusion attempts based on the content of the packets received, not based on IP addresses. *Id.* at 45 (citing Ex. 2019 ¶¶ 83–89). Patent Owner asserts that Sourcefire's 3D Sensors perform the action specified in the intrusion rule only if a packet's contents match the specified keywords in the

---

[6] Claim 1 of the '722 patent recites

> responsive to a determination by the packet-filtering device that the first packet satisfies one or more criteria, specified by a packet-filtering rule . . . , that correspond to one or more network-threat indicators . . . : 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 [and] 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.

Ex. 1029, 17:24–39.

intrusion rule. *Id.* (citing Ex. 1004, 761–62, 766–67; Ex. 2019 ¶¶ 83–89). In contrast, Patent Owner contends, IP addresses in the intrusion rule header are not keywords and are used only to determine whether to further evaluate a packet's contents against the keywords in the rule. *Id.* (citing Ex. 1004, 761–62, 766–67; Ex. 2019 ¶¶ 83–89). Thus, Patent Owner contends that Sourcefire's 3D Sensors do not use the value in the packet header's IP address field to determine whether to perform the rule's action or generate an intrusion event. *Id.* at 46–47 (citing Ex. 1004, 404–05, 761–64, 766–67, 769–70, 776–77; Ex. 2019 ¶¶ 83–89). In other words, Patent Owner argues that because a packet can match the IP addresses in a rule header without triggering a rule (i.e., when the packet's contents do not match the rule's keywords), it follows that Sourcefire does not teach applying the rule's operator "responsive to a determination" that a packet satisfies the rule "based on" IP addresses. *See* PO Resp. 47 (citing Ex. 1004, 404–05, 761–62, 766–67, 769–70, 776–77; Ex. 2019 ¶ 88).

We agree with Petitioner that Sourcefire teaches or suggests limitations [1.c1] and [1.c2]. Sourcefire explains that the "rules engine inspects the packet headers and payloads to determine whether they trigger any of the . . . rules." Ex. 1004, 258–59 (emphasis added); *see* Pet. 26–27; Pet. Reply 17. When a rule includes conditions in both its header and options section, Sourcefire teaches that a packet must match all the conditions specified in a rule to trigger the rule and perform the operator specified in the rule. Ex. 1004, 761 ("[I]f the packet data matches all the conditions specified in a rule, the rule triggers."). As Dr. Lee explains, traffic matches a rule in Sourcefire when it "match[es] all the conditions, in the rule header and also in the content, meaning the optional part." Ex. 2038, 71:14–19; *see* Pet. Reply 17; PO Sur-reply 22. Patent Owner's

expert, Dr. Orso, agrees that "[i]f the rule header matches, and then the keywords and argument match, then the rule is triggered." Ex. 1095, 57:2–58:1; *see* Pet. Reply 18; PO Sur-reply 22. Because a rule is triggered when a packet matches source and destination IP addresses in the rule header (and any criteria in the rule options section), we find that Sourcefire's 3D Sensor makes a "determination" that a packet satisfies the rule "based on" one or more of those source and destination IP addresses (i.e., the claimed network-threat indicators), as required by limitation [1.c1].

We also find that Sourcefire teaches applying an operator and communicating information "responsive to" the determination that a packet satisfies the rule based on the source and destination IP addresses. Patent Owner argues in the Sur-reply that, even if Sourcefire's rules are triggered "based on" criteria in the rule header, "this does not determine whether the specified operators of those intrusion rules are performed in reaction to ('responsive to') a packet matching specified IP addresses in the rule header." PO Sur-reply 22. We disagree. Rather than requiring that the operator be applied responsive to a packet matching IP addresses, as Patent Owner asserts, the claim language requires applying the operator responsive to a determination that the rule is satisfied. Thus, when a Sourcefire rule contains conditions in addition to IP addresses in the rule header, the operator is applied when the packet matches all the conditions. That "applying" step is "responsive to" a determination that the packet satisfies the rule, thus meeting the requirements of the claim.

For these reasons, we are persuaded by Petitioner's arguments and supporting evidence that Sourcefire teaches or suggests limitations [1.c1] and [1.c2]. Patent Owner's arguments do not undermine Petitioner's persuasive showing.

e. Limitations [1.d], [1.e], [1.f1], and [1.f2]

Claim 1 additionally requires the packet filtering device to receive an update to at least one packet filtering rule (limitation [1.d]) and modify, based on the update, "at least one operator specified by the first packet filtering rule to reconfigure the packet filtering device to prevent packets corresponding to the one or more network-threat indicators from continuing toward their respective destinations" (limitation [1.e]). Ex. 1001, 18:8–16. Finally, claim 1 requires "a determination by the packet filtering device that the second packet satisfies the first packet filtering rule" and, responsive to that determination and based on the modified operator, preventing the second packet from continuing toward a destination (limitation [1.f1]), and communicating data indicating that the second packet was prevented from continuing toward its destination (limitation [1.f2]). *Id.* at 18:17–28.

Noting that the claim language does not "limit who or what creates or generates the update," Petitioner cites Sourcefire's description of the Defense Center pushing to the 3D Sensors both "Security Enhancement Updates (SEUs), which can contain new and updated intrusion rules," and existing custom intrusion rules that have been modified on the Defense Center using the Defense Center's user interface. Pet. 44–45 (citing Ex. 1004, 35, 103, 117, 173, 864, 2094; Ex. 1003 ¶¶ 156–159); *see* Ex. 1003 ¶¶ 158–159 (citing Ex. 1004, 280–84, 290–99) (explaining how a rule's operator can be updated via the Defense Center user interface). At a minimum, Petitioner contends, "receiving updates to existing rules was well-known [to a person of ordinary skill in the art] to provide enhanced security by responding to changing network conditions." Pet. 44 (citing Ex. 1003 ¶ 159).

As for modifying an operator so that the first packet filtering rule prevents packets corresponding to network-threat indicators from continuing toward their respective destinations, Petitioner relies on Sourcefire's teaching that a rule can be changed from an alert rule to a drop rule by changing the rule state from "Generate Events" to "Drop and Generate Events." *Id.* at 45–47 (citing Ex. 1004, 358–59, 435; Ex. 1003 ¶¶ 160–163). Petitioner contends that a person of ordinary skill in the art would have understood that when the 3D Sensor receives an updated intrusion rule (either modified on the Defense Center or included in an SEU) that was changed from an alert rule to a drop rule, the rule on the 3D Sensor (i.e., the packet filtering device) is modified to drop packets that trigger the rule, i.e., to prevent them from continuing toward their destinations. *Id.* at 46 (citing Ex. 1003 ¶¶ 162–163).

Petitioner further explains that after the rule's operator has been modified by changing the rule to a drop rule with a rule state of "Drop and Generate Events," the rule will prevent a second packet satisfying the rule from continuing toward its destination because the packet will be dropped. *Id.* at 47 (citing Ex. 1004, 341, 358–59, 435; Ex. 1003 ¶¶ 164–166). Finally, Petitioner asserts that a drop rule in Sourcefire generates an intrusion event that includes an "Inline Result" indicating that IPS dropped the packet that triggered the rule. *Id.* at 48 (citing Ex. 1004, 276, 435; Ex. 1003 ¶¶ 167–169).

Patent Owner does not advance any arguments regarding these limitations. *See* PO Resp. 28–56. Having considered Petitioner's arguments and supporting evidence, we are persuaded that Sourcefire teaches limitations [1.d], [1.e], [1.f1]. and [1.f2].

f. Conclusion for Independent Claims 1, 8, and 15

For the reasons explained above, we are persuaded that Sourcefire teaches or suggests all the limitations of independent claims 1, 8, and 15. We weigh this evidence of obviousness together with Patent Owner's evidence of objective indicia of non-obviousness, *infra* § II.D.10, before reaching our final determination as to patentability of claims 1, 8, and 15.

4. Dependent Claims 2, 9, and 16

Claim 2 depends from claim 1 and further recites "causing, by the packet filtering device and in a user interface, display of data indicative that the first packet was allowed to continue toward the destination of the first packet," and "causing, by the packet filtering device, and in the user interface, display of second data indicative that the second packet was prevented from continuing toward the destination of the second packet." Ex. 1001, 18:29–37. Claims 9 and 16 depend from claims 8 and 15, respectively, and recite substantially the same limitations as claim 2. *Id.* at 20:13–23, 22:4–13.

For these limitations, Petitioner cites Sourcefire's description of a local web interface (i.e., a user interface) on a 3D Sensor running IPS that allows a user to review intrusion events. Pet. 49, 51 (citing Ex. 1004, 35). As discussed above, an intrusion event includes an Inline Result indicating that a packet triggered an alert rule that allowed the packet to continue toward its destination or a drop rule that prevented the packet from continuing toward its destination. *See id.* at 50–53 (citing Ex. 1004, 276, 435). With respect to display of data, Petitioner cites Sourcefire's description of workflows that allow the user to view intrusion event data via drill-down pages and table views. *Id.* (citing Ex. 1004, 267–68, 274, 280, 282, 284, 1574). Petitioner contends that a person of ordinary skill in the art

would have understood that enabling the Inline Result column in a drill-down page would display event data that includes the Inline Result indicating whether a packet was dropped or allowed to continue. *Id.* at 50, 52–53 (citing Ex. 1003 ¶¶ 173, 176).

Patent Owner does not advance any arguments regarding these claims other than those discussed above with respect to the independent claims. *See* PO Resp. 56–62. Based on Petitioner's arguments and supporting evidence, we are persuaded that Sourcefire teaches the limitations of claims 2, 9, and 16.

5. Dependent Claims 3, 10, and 17

Claim 3 depends from claim 1 and further recites:

> generating, by the packet filtering device and responsive to the determination by the packet filtering device that the first packet satisfies the first packet filtering rule, a packet log entry comprising a first threat identifier corresponding to the first packet and data indicating that the packet filtering device allowed the first packet to continue toward the destination of the first packet.

Ex. 1001, 18:38–45. Claims 10 and 17 depend from claims 8 and 15, respectively, and recite substantially the same limitations as claim 3. *Id.* at 20:24–33, 22:15–24.

Petitioner contends that an intrusion event generated by Sourcefire's 3D Sensor (i.e., packet filtering device) when a packet triggers an alert rule (i.e., responsive to the determination that a packet satisfies a packet filtering rule) is a "packet log entry" as claimed. Pet. 55–57 (citing Ex. 1004, 260, 276–78, 761; Ex. 1003 ¶ 181). An intrusion event is stored in Sourcefire's Event Database and is "a record of the date, time, and the type of exploit, and contextual information about the source of the attack and its target." Ex. 1004, 260, 276, 2084. Among other information, an intrusion event

includes an Inline Result and a Message, which is "explanatory text for the event" pulled from the triggered rule. *Id.* at 276, 278. As discussed previously, the Inline Result for an intrusion event generated when an alert rule is triggered indicates that the packet was allowed to continue toward its destination, as required by claim 3. *See id.* at 276. Petitioner contends that a "threat identifier" is an "identifier that represents a threat or information about a threat" and that an intrusion event (i.e., packet log entry) includes a threat identifier because the Event Message is "meaningful text that . . . gives immediate insight into the nature of the vulnerability that the rule detects attempts to exploit." Pet. 57 (quoting Ex. 1004, 772); *see id.* at 55 (citing Ex. 1004, 276–78).

Patent Owner does not advance any arguments regarding these claims other than those discussed above with respect to the independent claims. *See* PO Resp. 56–62. Based on Petitioner's arguments and supporting evidence, we are persuaded that Sourcefire teaches the limitations of claims 3, 10, and 17.

6. Dependent Claims 4, 11, and 18

Claim 4 depends from claim 3 and further recites "updating, by the packet filtering device and responsive to the determination by the packet filtering device that the first packet satisfies the first packet filtering rule, a packet flow entry corresponding to the generated packet log entry" and "wherein the packet flow entry consolidates a plurality of packet log entries commonly corresponding to the first threat identifier." Ex. 1001, 18:46–54. Claims 11 and 18 depend from claims 10 and 17, respectively, and recite substantially the same limitations as claim 4. *Id.* at 20:34–44, 22:25–35.

For the claimed "packet flow entry," Petitioner cites Sourcefire's "drill-down pages" that display table entries populated with intrusion event

data consolidated by specific type of information and displaying the count of events that match the specified type of information. Pet. 58–61 (citing Ex. 1004, 278, 280–81, 2078). In one example, Sourcefire provides the count of events for three different threat identifiers. Ex. 1004, 281. For the step of "updating" the packet flow entry "responsive to the determination" that the first packet satisfies the first packet filtering rule, Petitioner asserts that Sourcefire's drill-down pages are refreshed periodically to include "new events." Pet. 59–60 (citing Ex. 1004, 45–47, 1599, 1604). Petitioner contends that a person of ordinary skill in the art would have understood that when the drill-down pages are refreshed, if the packet filtering device has determined that a packet satisfies the packet filtering rule (and thus generated an intrusion event), the count of events in the corresponding drill-down entry is updated in response to that determination. *Id.* at 59 (citing Ex. 1003 ¶ 189). At a minimum, Petitioner contends, a person of ordinary skill in the art would have found it obvious to update the drill-down page in response to an intrusion event to beneficially provide the network administrator with the most current information needed for assessing network threats. *Id.* (citing Ex. 1003 ¶ 189). Additionally, Petitioner and Dr. Lee note that the Board found in the IPR2018-01760 FWD that Sourcefire teaches a similar "updating" limitation in claim 6 of the '722 patent.[7] *Id.* at 58 (Ex. 1031, 42); Ex. 1003 ¶ 186 (citing Ex. 1031, 42).

Patent Owner argues that Petitioner has not shown that Sourcefire discloses updating a packet flow entry "responsive to" the determination that

[7] Claim 6 of the '722 patent recites, in relevant part, "responsive to the determination by the packet-filtering device that the packet satisfies the one or more criteria [specified by the rule], updating . . . a packet-flow log." Ex. 1029, 19:13–17.

a packet satisfies the packet filtering rule. PO Resp. 56–60. Specifically, Patent Owner argues that Sourcefire's periodic refreshing at a user-controlled "refresh interval" does not show that the refresh is caused by or in reaction to a packet triggering the intrusion rule. *Id.* at 57–58 (citing Ex. 1029 ¶¶ 90–91). Instead, Patent Owner argues, the refresh and update to the count of events would be in reaction to and caused by the start of a new refresh interval. *Id.* at 58.

We are persuaded by Petitioner's argument and evidence that Sourcefire teaches or suggests updating the packet flow entry responsive to a determination that the first packet satisfies the first packet filtering rule. Sourcefire teaches updating drill-down pages to reflect new intrusion events detected by the 3D Sensor when a packet satisfies an intrusion rule. Ex. 1004, 1599, 1604. An entry in a drill-down page is updated with a new count of events only after a new intrusion event occurs, not every time a new refresh interval begins. *See id.* But when a new intrusion event is detected, the count is updated the next time the drill-down page is refreshed. *See id.*; Pet. Reply 20. In view of these teachings, we agree with Petitioner and Dr. Lee that "if the packet filtering device has determined that the first packet satisfies the first packet filtering rule . . . the corresponding drill-down entry is updated *in response to* that determination having been made." Ex. 1003 ¶ 189 (emphasis added); *see* Pet. 59; Pet. Reply 20.

For these reasons, we are persuaded by Petitioner's arguments and supporting evidence that Sourcefire teaches or suggests the limitations of claims 4, 11, and 18. Patent Owner's arguments do not undermine Petitioner's persuasive showing.

7. Dependent Claims 5, 12, and 19

Claim 5 depends from claim 1 and further recites "wherein each of the plurality of network-threat indicators corresponds to a respective network threat," and, responsive to a determination that each packet satisfies a packet filtering rule, "generating . . . a packet log entry comprising information" identifying the rule and whether the packet filtering device prevented the packet from continuing toward a destination of the packet or allowed the packet to continue toward the destination," and "updating . . . a packet flow log" to indicate that the rule was satisfied and whether the packet filtering device prevented the packet from continuing or allowed it to continue. Ex. 1001, 18:55–19:10. Claims 12 and 19 depend from claims 8 and 15, respectively, and recite substantially the same limitations as claim 5. *Id.* at 20:45–21:2, 22:36–61.

Petitioner contends that a person of ordinary skill in the art would have understood that for each rule in Sourcefire, the conditions specified (e.g., source IP address) correspond to a particular network threat. Pet. 61–62 (citing Ex. 1004, 42–30, 2084; Ex. 1003 ¶¶ 190–191). For the "generating" and "updating" limitations, Petitioner presents analysis similar to that for claims 2–4. Pet. 63–68. For instance, with respect to generating a packet log entry, Petitioner cites Sourcefire's description of an intrusion event that includes an Inline Result indicating that a packet triggered an alert rule that allowed the packet to continue toward its destination or a drop rule that prevented the packet from continuing toward its destination. *Id.* at 64 (citing Ex. 1004, 276, 281; Ex. 1003 ¶¶ 194–197). With respect to updating a packet flow log, Petitioner refers again to Sourcefire's drill-down pages. *Id.* at 65–68 (citing Ex. 1004, 45–47, 276, 280–82, 435, 1574, 1599, 1604, 2078; Ex. 1003 ¶¶ 198–202).

Patent Owner does not advance any arguments regarding these claims other than those discussed above with respect to the independent claims and with respect to similar language in claim 4. *See* PO Resp. 61–62. Based on Petitioner's arguments and supporting evidence, we are persuaded that Sourcefire teaches the limitations of claims 5, 12, and 19.

8. Dependent Claims 6, 13, and 20

Claim 6 depends from claim 5 and further recites "determining, by the packet filtering device and based on data of the packet flow log, an ordering of the plurality of network threats" and "communicating" data indicative of the ordering. Ex. 1001, 19:12–18. Claims 13 and 20 depend from claims 12 and 19, respectively, and recite substantially the same limitations as claim 6. *Id.* at 21:3–10, 22:62–23:2.

For the claimed "ordering," Petitioner points to Sourcefire's disclosure that data in a drill-down workflow page can be sorted based on "any available column." Pet. 69–70 (citing Ex. 1004, 278, 281, 1612, 1619–20; Ex. 1003 ¶¶ 204–206). For example, Petitioner asserts that the count column could be sorted in ascending order or descending order. *Id.* at 70 (citing Ex. 1004, 278, 1612). Petitioner also asserts that Sourcefire teaches "communicating" a drill-down page showing sorted data for viewing on a web browser. *Id.* at 71 (citing Ex. 1004, 35, 37–38; Ex. 1003 ¶¶ 207–209).

Patent Owner does not advance any arguments regarding these claims other than those discussed above with respect to the claims from which they depend. *See* PO Resp. 61–62. Based on Petitioner's arguments and supporting evidence, we are persuaded that Sourcefire teaches the limitations of claims 6, 13, and 20.

9. Dependent Claims 7, 14, and 21

Claim 7 depends from claim 6 and further recites that the "ordering" comprises at least one of several alternatives, including determining a number of packets corresponding to the network threat that were allowed to continue or determining a number of packets corresponding to the threat that were prevented from continuing. Ex. 1001, 19:19–34. Claims 14 and 21 depend from claims 13 and 20, respectively, and recite substantially the same limitations as claim 7. *Id.* at 21:11–28, 23:3–22.

Petitioner contends that a person of ordinary skill in the art would have understood that Sourcefire's drill-down page could be sorted first by the Inline Result column (indicating whether packets were allowed to continue or were prevented from doing so) and next by the count column. Pet. 73–76 (citing Ex. 1004, 276, 282, 1612, 1619–20; Ex. 1003 ¶¶ 211–213).

Patent Owner does not advance any arguments regarding these claims other than those discussed above with respect to the claims from which they depend. *See* PO Resp. 61–62. Based on Petitioner's arguments and supporting evidence, we are persuaded that Sourcefire teaches the limitations of claims 7, 14, and 21.

10. Objective Indicia of Non-obviousness

Objective indicia of nonobviousness may include long-felt but unsolved need, failure of others, unexpected results, commercial success, copying, licensing, industry praise, and expert skepticism. *Mintz v. Dietz & Watson, Inc.*, 679 F.3d 1372, 1379 (Fed. Cir. 2012). Objective indicia are only relevant to the obviousness inquiry if there is a nexus between the claimed invention and the objective indicia of nonobviousness. *In re Affinity Labs of Tex., LLC*, 856 F.3d 883, 901 (Fed. Cir. 2017). A rebuttable

presumption of nexus applies only "when [a patent owner] shows that the asserted objective evidence is tied to a specific product and that product 'embodies the claimed features, and is coextensive with [the claims].'" *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019) (quoting *Polaris Indus. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1072 (Fed. Cir. 2018)). On the other hand, a patent owner is not entitled to a presumption of nexus if the patented invention is only a component of a commercially successful machine or process. *Id.* (reaffirming the importance of the "coextensiveness" requirement).

Applying *Fox Factory*, the Board uses a two-step analysis in evaluating nexus between the claimed invention and objective evidence of nonobviousness, also referred to as secondary considerations. *Lectrosonics, Inc. v. Zaxcom, Inc.*, IPR2018-01129, Paper 33 at 33 (PTAB Jan. 24, 2020) (precedential). We first consider whether the patent owner has demonstrated "that its products are coextensive (or nearly coextensive) with the challenged claims," resulting in a rebuttable presumption of nexus. *Id.* at 33. If not, that "does not end the inquiry into secondary considerations"; "the patent owner is still afforded an opportunity to prove nexus by showing that the evidence of secondary considerations is the 'direct result of the unique characteristics of the claimed invention.'" *Id.* (quoting *Fox Factory*, 944 F.3d at 1373–75).

Here, Patent Owner asserts objective evidence of nonobviousness in the form of industry praise of the invention. PO Resp. 62–67. Specifically, Patent Owner argues that industry praise of the combinations of features in its RuleGate appliance (Exs. 2027, 2028) demonstrates nonobviousness of the challenged claims. *Id.* at 64–67. Patent Owner argues that the praise has a clear nexus to the challenged claims because the praised "[t]hreat feeds . . .

from various open source and enterprise services" are "examples of the 'network-threat-intelligence reports supplied by one or more independent network-threat-intelligence providers' recited in the Challenged Claims." *Id.* at 64–65 (citing Ex. 2027, 1–2; Ex. 2019 ¶¶ 93–94). Patent Owner argues that the nexus extends to RuleGate's ability to "quickly take action or correlate and inform administrators of breaches." *Id.* at 65–66 (citing Ex. 2027, 3; Ex. 2019 ¶¶ 93–94). Patent Owner also argues that Cisco "bragged about the advantages of the combination of features that were included in Cisco's Stealthwatch product," including knowledge of known bad hosts and continuous threat feeds, and that those advantages parallel the "network-threat indicators" and "network-threat-intelligence reports supplied by . . . independent network-threat-intelligence providers" recited in the challenged claims. *Id.* at 66–67 (citing Ex. 2019 ¶ 96; Ex, 2026, 2–3; Ex. 2025, 49–50).

Petitioner argues that there is no presumption of nexus because Patent Owner fails to show that Centripetal's RuleGate appliance embodies the claimed features of the '028 patent and is coextensive with them. Pet. Reply 21. For example, Petitioner contends that Patent Owner has not shown that RuleGate is a device that receives packet filtering rules, as recited in the challenged claims, and also argues that Patent Owner has admitted that "RuleGate practices many of [Patent Owner's] patents and the purported inventions therein—firmly rebutting any contention that [RuleGate] is coextensive with any Challenged Claim, or that the evidence has any requisite nexus." *Id.* at 21–22. Petitioner also argues that Patent Owner has not demonstrated a factual nexus between the praise for RuleGate and the claimed invention. *Id.* at 22–23. With respect to Cisco's Stealthwatch product, Petitioner argues that the purported praise relates to

limitations known in the prior art, which cannot form the basis for a nexus. *Id.* at 23–24 (citing *In re Huai-Hung Kao*, 639 F.3d 1057, 1068, 1074 (Fed. Cir. 2011)). Petitioner also notes that Patent Owner has not shown that Stealthwatch embodies the claims of the '028 patent because the cited district court decision (Ex. 2025) did not involve the '028 patent and also "was vacated in its entirety." *Id.* at 24 (citing Ex. 1092, 2–3).

We determine that Patent Owner has failed to establish a nexus between the claimed invention and the submitted evidence relating to RuleGate. First, we agree with Petitioner that claimed features at most constitute a small part of the commercial product so that the product and claims are far from being coextensive, and therefore Patent Owner is not entitled to a presumption of nexus. We also agree with Petitioner that Patent Owner has not established a factual nexus by showing that the industry praise is the "direct result of the unique characteristics of the claimed invention." *Fox Factory*, 944 F.3d at 1374. We are persuaded by Petitioner that the praise for RuleGate relied on by Patent Owner is directed to features not recited in the challenged claims, such as the ability to "quickly take action or correlate and inform administrators of breaches," "generat[ing] a PCAP [packet capture] of the incident," and "validating" which vendor rules are triggered. *See* Pet. Reply 23; PO Resp. 64–65 (citing Ex. 2027, 1–4).

With respect to Cisco's Stealthwatch product, Patent Owner appears to suggest that its features are coextensive with the claims of the '028 patent because Cisco "copied Centripetal's innovations." PO Resp. 66 (citing Ex. 2025, 149–57). We agree with Petitioner that Patent Owner has not shown that Stealthwatch embodies the claimed features of the '028 patent based on a now-vacated decision that did not involve the '028 patent, and thus Patent Owner is not entitled to a presumption of nexus. *See* Pet.

Reply 24. We also agree with Petitioner that Patent Owner has not established a factual nexus by showing that the alleged praise relating to knowledge of known bad hosts and threat feeds results from "unique characteristics" of the claimed invention rather than what was known in the prior art. *See* Pet. Reply 23–24.

For at least these reasons, we determine that Patent Owner has not established a nexus between the purported industry praise and the claimed invention. Accordingly, we find that Patent Owner's evidence of secondary considerations does not weigh in favor of nonobviousness.

11. Conclusion as to Obviousness

Having considered the *Graham* factors, and weighing the evidence of obviousness together with Patent Owner's objective evidence of nonobviousness, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–21 of the '028 patent are unpatentable under 35 U.S.C. § 103 as obvious over Sourcefire.

III. CONCLUSION[8]

For the foregoing reasons, we determine Petitioner has shown by a preponderance of the evidence that claims 1–21 of the '028 patent are unpatentable. The chart below summarizes our conclusions:

Claim(s)	35 U.S.C. §	References/Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–21	103	Sourcefire	1–21	
Overall Outcome			1–21	

IV. ORDER

Accordingly, it is

ORDERED that claims 1–21 of the '028 patent have been shown to be unpatentable; and

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

[8] 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. 16654 (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).

PETITIONER:

Scott A. McKeown
Mark Rowland
James R. Batchelder
Andrew Radsch
ROPES & GRAY LLP
scott.mckeown@ropesgray.com
mark.rowland@ropesgray.com
james.batchelder@ropesgray.com
andrew.rasch@ropesgray.com

PATENT OWNER:

James Hannah
Jeffrey H. Price
KRAMER LEVIN NAFTALIS & FRANKEL LLP
jhannah@kramerlevin.com
jprice@kramerlevin.com

Bradley C. Wright
Scott M. Kelly
Blair A. Silver
BANNER & WITCOFF, LTD.
bwright@bannerwitcoff.com
skelly@bannerwitcoff.com
bsilver@bannerwitcoff.com