

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC. and
PALO ALTO NETWORKS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, LLC,
Patent Owner.

Case IPR2023-00446¹
U.S. Patent No. 10,567,343

PATENT OWNER'S SUR-REPLY

¹ IPR2023-01353 has been joined with this proceeding.

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. THE CHALLENGED CLAIMS ARE PATENTABLE	3
A. Sourcefire in View of Emerging Threats Does Not Disclose rules “configured to prevent an exfiltration operation”	3
1. Undisputed Evidence Contradicts Petitioner’s Conclusory Motivation to Modify Emerging Threats’ Rules to Drop Traffic	4
2. There is No Claim Construction Dispute.....	8
B. Sourcefire in View of the Identified Emerging Threats Rules Does Not Disclose the Claimed Packet-Filtering Rule.....	10
1. Rule 2003021 Does Not Prevent Exfiltration Operations	10
2. The Other Rules Do Not Match Any Application Layer Header Field.....	12
C. Claims 5 and 12	14
D. Evidence of Secondary Considerations Demonstrate Non- Obviousness of the Challenged Claims.....	16
1. Recognition of a Problem, Long Felt But Unresolved Need, and Failure of Others	17
2. Industry Praise.....	19
III. CONCLUSION.....	20

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Belden Inc. v. Berk-Tek LLC</i> , 805 F.3d 1064 (Fed. Cir. 2015)	7, 13
<i>In re Cyclobenzaprine Hydrochloride Extended-Release Capsule Pat.</i> <i>Litig.</i> , 676 F.3d 1063 (Fed. Cir. 2012)	6, 19
<i>In re Gordon</i> , 733 F.2d 900 (Fed. Cir. 1984)	7
<i>KSR Int'l Co. v. Teleflex, Inc.</i> , 550 U.S. 398 (2007).....	5
<i>Novartis AG v. Torrent Pharms. Ltd.</i> , 853 F.3d 1316 (Fed. Cir. 2017)	18, 19
<i>Polaris Indus., Inc. v. Arctic Cat, Inc.</i> , 882 F. 3d 1056 (Fed. Cir. 2018)	5

I. INTRODUCTION

Centripetal Networks, LLC, (“Centripetal” or “Patent Owner”) requests that the Board find the Challenged Claims² patentable over Sourcefire and Emerging Threats because Petitioner has failed to demonstrate that it would have been obvious at the time the invention was made to modify Sourcefire (Ex. 1004) with Emerging Threats (Ex. 1020) to yield Centripetal’s claimed exfiltration prevention methods. The full trial record confirms what the Office and District Courts judges have consistently agreed: it would not have been obvious to modify the teachings of Sourcefire to prevent exfiltration operations. Ex. 1002 at 35-40 (allowing ‘343 Patent in view of Sourcefire); Ex. 1077 at 16-20 (denying *inter partes* review of the ‘343 Patent based on Sourcefire); Ex. 1070 (denying *inter partes* review of the related ‘193 Patent); Ex. 1085 at 3-7 (Notice of Intent to Issue *Ex Parte*

² Keysight Technologies, Inc., (“Petitioner”) petitioned for *inter partes* review (IPR) of U.S. Patent No. 10,567,343 (Ex. 1001, the “’343 Patent”), challenging claims 1-20 (“the Challenged Claims”). On September 5, 2023, Palo Alto Networks, Inc. filed its second petition against the ‘343 Patent, with a Motion for Joinder. See Exs. 2008, 2009. Palo Alto Networks’ Joinder Request was granted on March 13, 2024. See IPR2023-01353, Paper 10.

Reexamination Certificate of the '193 Patent); Ex. 2007 at 22-23 (district court finding the '193 Patent “valid and directly infringed”).

The latest spin on this tired argument, that Emerging Threats disclosed rules that would have been modified to prevent exfiltrations, fails for the same reasons that every other challenge to this patent family has failed to date: (1) the rules do not filter packets on the claimed criteria and (2) do not drop traffic. The evidence developed at trial—including unrebutted testimony from a former Emerging Threats contributor who wrote many of the Emerging Threats rules—establishes that the rules cited in the Petition (and the new rules discussed in the Reply) were not developed to drop traffic and that no POSITA would have found it “obvious” to employ them to prevent exfiltrations. Ex. 2031 at ¶¶ 7-21. On the contrary, enabling the identified Emerging Threats rules and modifying them to drop traffic would have made the network unusable for its intended purpose.

Centripetal has also submitted expert testimony from Dr. Goodrich (Ex. 2010, “Goodrich Decl.”) and contemporaneous documentation from Emerging Threats itself (Exs. 2015-2022) that demonstrate Emerging Threats does not teach what Petitioner claims it does—namely, that Rule 2003021, the linchpin of Petitioner's case, is not configured to detect, let alone, prevent exfiltration operations. That rule is designed to detect whether a computer is infected with a particular bot known to

communicate over non-standard port numbers, not to prevent exfiltration operations. Goodrich Decl., ¶¶ 76-80; Ex. 2018; Ex. 2019.

In its Reply, Petitioner mischaracterizes this rebuttal evidence and the cross-examination testimony of Centripetal's witnesses with mere attorney argument. Petitioner declined the opportunity to refute Centripetal's evidence with argument or other evidence, such as a reply declaration from its own expert Dr. Staniford. The rest of Petitioner's Reply is spent arguing the threshold issue of Emerging Threats, and mischaracterizing the objective indicia of non-obviousness showing that Centripetal's exfiltration prevention methods solved a long-felt need in the industry, received significant industry praise, and were brazenly copied by Centripetal's competitors.

II. THE CHALLENGED CLAIMS ARE PATENTABLE

A. Sourcefire in View of Emerging Threats Does Not Disclose rules "configured to prevent an exfiltration operation"

The full trial record establishes that the Emerging Threats rules cited in the Petition and Reply do not facially satisfy the packet-filtering rules in the Challenged Claims for various reasons. Foremost among those reasons is that the Emerging Threats rules were specifically designed as **alert** rules for use on an IDS device that cannot, as the parties agree, "prevent" an exfiltration operation as written. Ex. 1101 at 99:18-100:1. It was, therefore, incumbent on Petitioner to explain how and why a POSITA would have modified those rules to prevent exfiltrations. That

explanation is wholly lacking and cannot be reconciled with the record evidence or the Office's repeated determinations that it would not have been obvious to modify Sourcefire in order to prevent exfiltration operations. POR at 13-26; Pet. at 12-15 (recognizing numerous prior proceedings where it was found that Sourcefire does not disclose or suggest rules for preventing exfiltration operations).

The underlying problem with the Emerging Threats rules, and all previous rule-based attempts to solve the exfiltration problem, were that they were overbroad, and such rules to actively drop traffic in a network environment would have made the network unusable. '343 Patent at 7:24-40; Ex. 1085 at 112. That is why Emerging Threats wrote alert rules for use on an IDS device rather drop rules for use on an IPS device like the Sourcefire 3D Appliance: while useful for understanding and responding to intrusions, they would not have "preserv[ed] the flow of normal legitimate network traffic without disruption" if enabled to drop traffic in a network environment. See POR at 10-12; Ex. 1085 at 111, ¶ 9 and 112, ¶ 11.

1. Undisputed Evidence Contradicts Petitioner's Conclusory Motivation to Modify Emerging Threats' Rules to Drop Traffic

Petitioner acknowledges that the Emerging Threats rules are not anticipatory because, as **alert** rules, they are not configured to **prevent** exfiltration operations. See Pet. at 57-58. In view of this deficiency, Petitioner cited Sourcefire's disclosure of modifying a rule's action from alert to drop to show that an administrator **could**

change the rule's action from alert to drop "once the user observes that they operate as desired." *Id.* at 57. But the obviousness inquiry turns on what "a skilled artisan would have been motivated to do at the time of the invention," not what it could have done. *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F. 3d 1056, 1068-69 (Fed. Cir. 2018) (citation omitted).

Even by its own standards, Petitioner did not establish that any of the Emerging Threats rules identified in the Petition or Reply **would** have "operate[d] as desired" if the rule's action was switched from an alert rule to a drop rule. Pet. at 57-58. It did not test the identified rules in a network environment or even consider whether any aspects of the rules would have made them entirely inappropriate for use as drop rules for an IPS device. *See id.* Petitioner has not, therefore, established a *prima facie* case that a POSITA would have modified the disclosures of Emerging Threats (the identified "alert" rules) with Sourcefire's to reach a packet-filtering rule that prevents exfiltration operations because it did not explain or provide any motivation for modifying the teachings of the cited art. *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 418 (2007) ("[I]t can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to **combine the elements** in the way the claimed new invention does") (emphasis added).

Instead of meeting this burden, Petitioner blithely claimed that "[a] POSA would have understood the obvious desirable effect of setting Emerging Threats

rules imported into Sourcefire to drop traffic associated with detected exfiltration operations.” Pet. at 34-35. That unsupported, conclusory assertion is unrelated to the actual rules disclosed in Emerging Threats that would have to be modified and cannot withstand scrutiny on the weight of undisputed evidence developed over the course of the trial because it does not acknowledge, let alone address the evidence weighing against that conclusion. That approach invites legal error. *In re Cyclobenzaprine Hydrochloride Extended-Release Capsule Pat. Litig.*, 676 F.3d 1063, 1074 (Fed. Cir. 2012) (“[A] fact finder consider[s] all evidence relating to obviousness before finding a patent invalid on those grounds.”).

Undisputed testimony of a former Emerging Threats employee, and author of many rules in the Emerging Threats ruleset, testified that “rules that are written to alert” would not have been flipped to drop traffic. Ex. 1101 at 54:5-14 (testifying that “these kind of rules were never designed to drop traffic . . . These rules exist to give evidence that some network administrator can correlate an event on the network with other events with other systems in order to start an investigation”). Mr. Marinho also explained that that the rules that he and other contributors to the Emerging Threat project wrote were intrusion detection system (IDS) rules, not intrusion prevention system (IPS) rules. Ex. 2031 at ¶ 6 (confirming “there are no ‘drop’ rules in the Emerging Threats reference; all of the Snort rules use the ‘alert’ keyword”); *see also* Ex. 1101 at 28:19-30:21.

Mr. Marinho's unrebutted testimony about the nature of the Emerging Threats rules entirely undermines Petitioner's case because even Dr. Staniford admits that rules that generate too many "false positives" would have rendered the product unusable. Ex. 2011 ("Staniford Tr.") at 33:6-21 ("[I]f a product has a lot of false positives, you know, it becomes unusable"), 31:9-14 ("[I]f you block too broadly, then obviously you block a user trying to get to an asset that's not in fact compromised"), 27:23-28:8, 29:20-31:8 (describing challenges and lack of accuracy in the approach of "getting lists of IP addresses and the main names of botnet controllers and detecting [them]"); *see also id.* at 68:25-69:5, 69:13-71:14 (opining that certain Emerging Threat rules were commented out because they were an "expensive rule to run"). Claims are not obvious when the modification of the art renders the resulting device inoperable for its intended purpose. *In re Gordon*, 733 F.2d 900, 902 (Fed. Cir. 1984).

And while Petitioner elicited cross-examination testimony saying a rule **could** be changed from "alert" to "drop" (a point which Centripetal has never disputed), it neglected to inform the Board or rebut that Mr. Marinho's repeated testimony about why no person would make such a change. Reply at 4 (arguing "PO's declarants confirmed that commented-out rules could be enabled"). As discussed above, the obviousness inquiry does not turn on what a POSITA **could** have done, but what a POSITA would have done at the time of the invention. *Belden Inc. v. Berk-Tek LLC*,

805 F.3d 1064, 1073 (Fed. Cir. 2015) (“[O]bviousness concerns whether a skilled artisan not only could have made but would have been motivated to make the combinations or modifications of prior art to arrive at the claimed invention.”) (citation omitted).

The Challenged Claims are, therefore, patentable because—like the Board has already found—even if Sourcefire **could** have been modified to prevent exfiltrations, a POSITA would not have modified Sourcefire to do so at the time of the invention.

2. There is No Claim Construction Dispute

Unable to contest Mr. Marinho's clear testimony that the Emerging Threats rules were not designed for, or expected to be used in, an IPS environment, Petitioner attacks a strawman. Reply at 1-3 (suggesting that Centripetal raised a tacit claim construction argument in the POR). As should be clear from the previous sections, Centripetal's arguments about preventing exfiltrations “while still preserving the flow of normal legitimate network traffic without disruption” were made in the context of rebutting Petitioner's conclusory, unsupported attempts to transform Emerging Threats' alert rules into drop rules (POR at 10-12) or to help explain the benefits achieved by the claimed invention (POR at 30).

The point was (and remains) that it was known that overbroad rules could not be used to prevent exfiltrations at the time of the invention, and merely enabling an overbroad rule to drop traffic would render the network unusable. See Ex. 1085 at

112, ¶ 11 (“[P]rior attempts by others to prevent data exfiltration were often too coarse or overbroad because they would simply block all traffic to/from a given network, regardless of the actual threat, resulting in a negative impact to the subject computer network and ultimately to business operations.”). For example, a network administrator could write a rule that blocked all network traffic, and while that rule would prevent exfiltration operations, no network administrator would drop packets pursuant to such a rule because it would shut down the network, rendering it inoperable.

That is why the claimed rules did not exist before Centripetal’s innovations and why no POSITA would have considered modifying Emerging Threats’ rules to drop traffic (at least without first establishing a reasonable expectation of success, a burden that Petitioner did not attempt to meet with respect to **any** of the identified rules). Centripetal did not, therefore, “read additional vague requirements into the term,” it explained why it wouldn’t have been obvious to modify Emerging Threats’ rules to reach the Challenged Claims. Reply at 2.

Accordingly, Petitioner framed the problem recognized by the inventor too broadly and failed to consider the subject matter of the application as a whole by failing to consider the need to preserve the flow of legitimate network traffic without disruption.

B. Sourcefire in View of the Identified Emerging Threats Rules Does Not Disclose the Claimed Packet-Filtering Rule

1. Rule 2003021 Does Not Prevent Exfiltration Operations

As a preliminary matter, as with every other Emerging Threats rule cited in this case, Rule 2003021 cannot prevent exfiltration operations because it is an alert rule, and Petitioner has not even attempted to establish that a POSITA would have found it obvious to modify this rule's action to drop packets. *See* Section II.A, *supra*.

The evidence surfaced during trial establishes that Rule 2003021 was meant to detect a new bot that happened, idiosyncratically, to establish encrypted sessions on a high port. Goodrich Decl., ¶ 78; Ex. 2018 at 1 (e-mails from Emerging Threats indicating that “[t]he impetus to create [these rules] was a new bot that’s using standard ssl for a command and control session on a high port”); Ex. 2019 at 2; *see also* POR at 14-19. This idiosyncrasy gave network security experts a way to alert a network administrator that the known bot **might** be operating on a computer in a network. Goodrich Decl., ¶ 77-80. The administrator could then investigate the matter further and determine whether the computer was actually infected or whether the alert represented a false alarm. The purpose for this rule is consistent with the purpose of all of the Emerging Threats rules. Ex. 1101 at 54:5-14 (“These rules exist to give evidence that some network administrator can correlate an event on the network with other events with other systems in order to start an investigation.”); *id.*

at 36:11-21 (similar), 92:19-24 (similar), 109:18-22, 116:4-9, 117:13-24. They were not meant to, and are not suited for, dropping network traffic. Ex. 1101 at 54:5-8.

This evidence establishes that the rule was designed to help suss out a particular exploit and contradicts Dr. Staniford's unsupported opinion that "this rule was not directed to looking for instances of exploits or attacks." Ex. 1003 at ¶ 228. The rule would trigger (if it were enabled) any time a computer sent encrypted information on a high port number, whether or not it was infected with a bot. Ex. 2011 at 90:5-13, 92:13-15. Indeed, a companion rule would trigger during the handshake, and if modified to drop traffic, the session would not be initiated, and there would be no exfiltration operations to prevent. Ex. 1100 at 51:9-20. And confirming that no POSITA would have enabled this rule and modified it so that it drops packets, it was commented out for performance reasons. Ex. 1101 at 73:1-74:7. Such rules are overbroad and would render the network unusable. Consistent with this conclusion, the rule was commented out and eventually removed from the Emerging Threats ruleset entirely. Ex. 2020 at 3.

Petitioner is also incorrect to say that this rule is only for outdated versions of SSL that were known to be vulnerable. Several other similar rules in the same ruleset were written to target versions of TLS/SSL without the alleged vulnerabilities of SSLv3. Ex. 2010 at ¶¶ 78-79; Ex. 2018 (Emerging Threats rule author stating "It's set to get sslv2, sslv3, and most tls implementations."). These rules further support

the notion that they were meant to alert an administrator to the possibility that a computer was infected with a particular both, not to detect or prevent exfiltration operations.

2. The Other Rules Do Not Match Any Application Layer Header Field

The Board acknowledged that the Petitioner has not argued that any other rules are applicable to this limitation, and therefore are not part of Petitioner's case. Institution Decision at 31. In its Reply, Petitioner does not dispute that Rules 2002526, 2002034, 2001328 do not render obvious the claim limitations. Reply at 8-9; POR at 19-20.

Instead, Petitioner has now shifted their theory to argue that Rules 2005319, 2006409, 2010234, and 2003937 disclose rules that match on application layer header information. Reply at 8-9. However, the claims require that the packet transformation function be applied "responsive to" matching the application layer criteria, and each of these rules do not meet that criteria, a point that Petitioner glosses over. *See id.* at 8 ("PO mistakenly asserts that other Emerging Threats rules do not match application header field values.").

The issue raised in the POR was not only whether the identified rules **match** application header field values (they don't), but whether the packet transformation function that prevents the exfiltration operation is applied "**responsive to**" matching that information. Each of these newly identified rules fails to teach this aspect of the

Challenged Claims. Specifically, rules 2005319 and 2010234 do not trigger (let alone drop packets) responsive to detecting traffic containing a POST method. Reply at 8. Instead, both rules check “uricontent” (e.g., “/zuzu.php?&r”) before triggering the rule’s action. *Id.* at 8-9. Rule 2003937 similarly detects “additional content in a post going to a remote web server,” which means that it does not trigger responsive to detecting the application layer header information. *Id.* at 9; POR at 21-23. Rule 2006409 moreover, suffers from all of the same deficiencies as Rule 2003021 in that no POSITA would have enabled the rule to drop packets in view of the comment that this rule was not meant to be a “definite indication of hostile activity.” Ex. 1020 at 98. Such rules are written with the knowledge that they will generate too many false positives to give an administrator confidence that they could be used to drop live traffic, which requires a high degree of confidence. Ex. 1101 at 105:15-22, 112:14-113:2; Ex. 2011 68:19-23.

These arguments should also be rejected as untimely and improper. Rules 2005319 and 2010234 are only cited in the original Petition in the context of dependent claims (see Pet. at 61-62, 64-65) and the Board should reject this attempt to incorporate arguments by reference. Rules 2006409 and 2003937 are mentioned nowhere in the original Petition. These new rules were not introduced to rebut any of the arguments or evidence made in the POR. *Belden*, 805 F.3d at 1081-82 (“Rebuttal evidence is supposed to be limited to that which is responsive to the

adversary's evidence: the traditional principle [is] that evidence offered to rebut must accomplish the function of rebuttal; to explain, repel, counteract, or disprove the evidence of the adverse party.”) (internal quotations and citations omitted).

Because these new rules are evidence that could have been cited in the Petition, it is improper for the Petitioner to raise them now. As such, the Board should reject Petitioner's attempts to sandbag the proceeding by introducing new evidence so late into the proceeding, particularly because their relevance is supported only by attorney argument and it provides no opportunity for Centripetal to introduce expert or fact testimony demonstrating that the rules do not meet the elements of the claims.

In the end, these new rules add nothing to Petitioner's case at least because they are all alert rules, and Petitioner has not attempted to establish that a POSITA would have modified any of these rules to drop packets.

C. Claims 5 and 12

Claims 5 and 12 are patentable because Emerging Threats Rule 2010234 does not include an application layer header field that identifies specified resource data, and because a POSITA would not have been motivated to modify the rule to drop packets. POR at 26-27.

First, Petitioner has never attempted to explain with specificity why the URI content specified in the rule is “specified resource data,” and it made no effort to

cure that basic deficiency in the Reply. Pet. at 64-65; Reply at 13. The '343 Patent uses the term “resource” to refer the parties to a communication session, which are identified by 5-tuple data (*i.e.* IP addresses and port numbers). See '343 Patent at 8:45-52 (“Conceptually, the first stage may determine if the network policy allows any communications between the **resources** identified in the 5-tuple rule; if so, the second stage may determine if the policy allows the specific method or type of communication (e.g., file read, file write, encrypted communication, etc.) between the **resources**.”) (emphasis added).

The path specified in the “uricontent” in Rule 2010234 is missing this basic component of “specified resource data” because it does not include the identity of the resource hosting the file named “/senm.php ?data=.” That information would be found in the full URL, which is not specified in the rule. The exclusion of the “resource” from this information is consistent with Mr. Marinho’s unrebutted testimony establishing that IDS rule writers did not write rules to “match on the entire URL.” Ex. 1101 at 61:11-62:2.

Second, for all of the reasons specified above, a POSITA would not have transformed Rule 2010234 from an alert rule to a drop rule. Section II.A, *supra*. Indeed, Mr. Marinho’s unrebutted testimony establishes that this rule would have had far too high a rate of false positives to be implemented as a drop rule in a network environment. Ex. 2031 at ¶¶ 18-19; Ex. 1101 at 110:14-116:16.

D. Evidence of Secondary Considerations Demonstrate Non-Obviousness of the Challenged Claims

The Office has already confirmed that objective indicia of nonobviousness supports the conclusion that Centripetal's exfiltration technology is patentable. Ex. 1085 at 7. Although that case dealt with Centripetal's '193 Patent, much of the evidence and arguments the Examiner found persuasive is cited herein and directly applicable for the same reasons. See POR at 27-34 (citing Exs. 2023, 2024, 2025, 2026, 2027, 2028); Goodrich Decl., ¶ 104-116.

For example, the Examiner credited a wealth of evidence establishing that there was a long-felt need for a solution to the exfiltration problem and that Centripetal solved that problem. Ex. 1085 at 137-140, 144-145 ('193 Patent Response to Non-Final Office Action); *id.* at 5-7 (Patent Office's Notice of Intent to Issue Ex Parte Reexamination Certificate). The Examiner also credited evidence of industry praise, including evidence showing that Centripetal's Threat Intelligence Gateway can "deliver more than is possible with firewalls and IPS systems" like Sourcefire.

This evidence, along with evidence that a competitor copied the '193 Patent, led the Examiner to conclude, a POSITA would not have modified Sourcefire to meet the claims of the '193 Patent. Ex. 1085 at 7. The objective indicia of non-obviousness presented in this case compels the same conclusion with respect to the Challenged Claims of the '343 Patent.

1. Recognition of a Problem, Long Felt But Unresolved Need, and Failure of Others

The '343 Patent satisfied a long-felt need in the industry that others had failed to solve—namely, how to protect against “[a] category of cyber attack known as exfiltrations (e.g., stealing sensitive data or credentials via the Internet).” Goodrich Decl., ¶ 104 (citing '343 Patent at 1:28-51).

Undisputed evidence establishes a need for a solution to the exfiltration problem extending back to at least 2006. *Id.*, ¶ 105 (citing Ex. 1081, ¶ 6; Ex. 2023, Ex. 2024). The Examiner credited this argument and evidence when it was presented as evidence of a long-felt need for the invention recited in the '193 Patent. Ex. 1085 at 7. The Examiner also credited Centripetal's arguments and evidence establishing the nexus between its solution to the exfiltration problem and the claims of the '193 Patent. Ex. 1085 at 7.

Centripetal presented the same evidence in this proceeding. POR at 27-32. Petitioner does not acknowledge the Office's earlier consideration of this evidence, dispute its accuracy, or otherwise challenge Centripetal's demonstration of a long-felt need for to the exfiltration problem. Reply at 14-15. Instead, Petitioner asks the Board to turn a blind eye to all of this evidence because one small section of Dr. Goodrich's opinion analyzed the testimony and underlying evidence from the inventor (which Petitioner filed in this case and did not challenge). *Id.* at 15. Petitioner gives no legal basis for this request to ignore record evidence, and doing

so would violate the requirement that all evidence be considered before reaching an obviousness determination. Petitioner's failure to rebut Dr. Goodrich's testimony or the evidence underlying his opinions should be taken for what it is: an admission that Dr. Goodrich's testimony is accurate.

Petitioner's argument that Sourcefire and Emerging Threats already provided that solution fails because it misapplies *Novartis AG v. Torrent Pharms. Ltd.*, 853 F.3d 1316, 1331 (Fed. Cir. 2017). *Novartis* stands for the notion that "the identified objective indicia must be directed to what was *not* known in the prior art." *Id.* (emphasis added). There is no evidence of record that either Sourcefire or Emerging Threats disclosed a packet-filtering rule for "preventing exfiltration operations." See *generally* Petition and Reply. In order to reach this aspect of the challenged claims, Petitioner argues that a POSITA would have *modified* the rules disclosed in Emerging Threats in order to actively drop packets.³ Packet-filtering rules "configured to prevent exfiltration operations" were, therefore, not "known" in the art but only (allegedly) obvious over what was known.

Novartis cannot possibly stand for the proposition that objective indicia of non-obviousness is irrelevant when it is tied to an element that is only "known" is

³ As discussed throughout Centripetal's briefing, Petitioner has not attempted to establish that a POSITA would have modified any one of the Emerging Threats rules to drop traffic.

allegedly known based on a combination of teachings in the art. That approach commits the sin of assuming obviousness before considering the objective evidence. *In re Cyclobenzaprine Hydrochloride*, 676 F.3d at 1079 (“[F]act finders must withhold judgment on an obviousness challenge until it considers all relevant evidence, including that relating to the objective considerations.”).

Petitioner does not dispute that there was a long-felt need for a solution to the exfiltration problem or the evidence establishing that the '343 Patent satisfied that need. Its only argument, that the claims lack nexus to the objective evidence, relies on its misreading of *Novartis*. The Challenged Claims are nonobvious.

2. Industry Praise

Products embodying the invention claimed in the '343 Patent have received substantial industry praise. Goodrich Decl., ¶¶ 114-117. In a white paper entitled “Centripetal Networks Threat Intelligence Gateway: Designed to Enable Continuous Prevention Through Intelligence-Led Enforcement,” an industry research firm named ESG Research praised Centripetal’s Threat Intelligence Gateway as having “the highest performance network filter that ESG has tested or seen in action to date.” Ex. 2025 at 8; Goodrich Decl., ¶ 114. The ESG Paper further lauded Centripetal’s Threat Intelligence Gateway’s ability to “deliver[] more than is possible with firewalls and IPS systems,” pointing to Centripetal’s RuleGATE and CleanINTERNET products. Ex. 2025 at 7.

The evidence of industry praise discussed above is reasonably commensurate with the scope of the claims of the '343 Patent and that there is a nexus between the merits of the claimed invention and the evidence of secondary considerations, as the praise is directed at Centripetal's products which embody the claimed features of the '343 Patent. Therefore, the praise that Centripetal's products and technology have received from others further demonstrates that the claimed invention of the '343 Patent is not obvious.

III. CONCLUSION

For all of these reasons, Patent Owner accordingly requests that the Board confirm the patentability of the Challenged Claims of the '343 Patent.

Respectfully submitted,

Dated: March 13, 2024

/James Hannah/
James Hannah (Reg. No. 56,369)
Jenna Fuller (Reg. No. 74,212)
KRAMER LEVIN NAFTALIS & FRANKEL LLP
Twin Dolphin Drive, Suite 700
Redwood Shores, CA 94065
Tel: 650.752.1700 Fax: 650.752.1800
jhannah@kramerlevin.com
jfuller@kramerlevin.com

Jeffrey H. Price (Reg. No. 69,141)
KRAMER LEVIN NAFTALIS & FRANKEL LLP
1177 Avenue of the Americas
New York, NY 10036
Tel: 212.715.7502 Fax: 212.715.8302
jprice@kramerlevin.com

Scott M. Kelly (Reg. No. 65,121)
Bradley C. Wright (Reg. No. 38,061)
John. R. Hutchins (Reg. No 43,686)
BANNER & WITCOFF, LTD.
1100 13th Street, NW, Suite 1200
Washington, DC 20005
Tel: (202) 824-3000 Fax: (202) 824-3001
skelly@bannerwitcoff.com
bwright@bannerwitcoff.com
jhutchins@bannerwitcoff.com

(Case No. IPR2023-00446)

Attorneys for Patent Owner
Centripetal Networks, LLC

CERTIFICATE OF COMPLIANCE WITH 37 C.F.R. § 42.24

The undersigned hereby certifies that the foregoing PATENT OWNER'S SUR-REPLY has 4,620 words in compliance with the word limit set forth in 37 C.F.R. § 42.24(c)(4). This word count was prepared using the Microsoft Word word-processing system used to prepare this paper.

Dated: March 13, 2024

/James Hannah/

James Hannah (Reg. No. 56,369)
Jenna Fuller (Reg. No. 74,212)
KRAMER LEVIN NAFTALIS & FRANKEL LLP
333 Twin Dolphin Drive, Suite 700
Redwood Shores, CA 94065
Tel: 650.752.1700 Fax: 650.752.1800
jhannah@kramerlevin.com
jfuller@kramerlevin.com
Jeffrey H. Price (Reg. No. 69,141)
KRAMER LEVIN NAFTALIS & FRANKEL LLP
1177 Avenue of the Americas
New York, NY 10036
Tel: 212.715.7502 Fax: 212.715.8302
jprice@kramerlevin.com

Scott M. Kelly (Reg. No. 65,121)
Bradley C. Wright (Reg. No. 38,061)
John. R. Hutchins (Reg. No 43,686)
BANNER & WITCOFF, LTD.
1100 13th Street, NW, Suite 1200
Washington, DC 20005
Tel: (202) 824-3000 Fax: (202) 824-3001
skelly@bannerwitcoff.com
bwright@bannerwitcoff.com
jhutchins@bannerwitcoff.com

(Case No. IPR2023-00446)

Attorneys for Patent Owner
Centripetal Networks, LLC

CERTIFICATE OF SERVICE

The undersigned certifies, in accordance with 37 C.F.R. § 42.6(e), and pursuant to agreement by the parties that filing with the Board through the Patent Trial and Appeal Case Tracking System (P-TACTS) constitutes electronic service, that service was made on Petitioner as detailed below.

<i>Date of service</i>	March 13, 2024
<i>Manner of service</i>	Electronic Filing with the Board
<i>Documents served</i>	PATENT OWNER'S SUR-REPLY
<i>Persons Served</i>	REED SMITH LLP Gerard M. Donovan Peter J. Chassman Walter M. Egbert Jonathan I. Detrixhe Sidharth Kapoor gdonovan@reedsmith.com pchassman@reedsmith.com wegbert@reedsmith.com jdetrixhe@reedsmith.com skapoor@reedsmith.com ROPES & GRAY LLP James L. Davis, Jr. Andrew Radsch james.l.davis@ropesgray.com andrew.radsch@ropesgray.com

By: /James Hannah/
James Hannah (Reg. No. 56,369)