No. 2021-1888

United States Court of Appeals for the Federal Circuit

CENTRIPETAL NETWORKS, INC.,
Plaintiff-Appellee,

v.

CISCO SYSTEMS, INC.,
Defendant-Appellant.

Appeal from the United States District Court for the Eastern District of Virginia, Case No. 2:18-cv-00094-HCM-LRL, Judge Henry C. Morgan Jr.

CENTRIPETAL NETWORKS, INC.'S RESPONSE BRIEF [NON-CONFIDENTIAL]

Paul J. Andre
Lisa Kobialka
James Hannah
Hannah Lee
KRAMER LEVIN NAFTALIS & FRANKEL LLP
990 Marsh Road
Menlo Park, California 94025
Telephone: (650) 752-1700

Blair A. Silver
BANNER & WITCOFF, LTD.
1100 13th Street NW, Suite 1200
Washington, DC 20005
Telephone: (202) 824-3000

Andrei Iancu
Alan J. Heinrich
IRELL & MANELLA LLP
1800 Avenue of the Stars
Los Angeles, CA 90067
Telephone: (310) 203-7537

Philip J. Warrick
IRELL & MANELLA LLP
750 17th Street NW, Suite 850
Washington, DC 20006
Telephone: (202) 831-6238

Christopher Cotropia
BEY & COTROPIA PLLC
213 Bayly Court
Richmond, Virginia 23229
Telephone: (804) 404-2367

ATTORNEYS FOR CENTRIPETAL NETWORKS, INC.

REPRESENTATIVE CLAIMS

U.S. Patent No. 9,686,193 ("'193 Patent")

19. One or more non-transitory computer-readable media comprising instructions that when executed by one or more computing devices cause the one or more computing devices to:

receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;

responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:

apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

drop each packet in the first portion of packets; and

responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network:

apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator, configured to forward packets not associated with the particular type of data transfer toward the third network; and

forward each packet in the second portion of packets toward the third network.

U.S. Patent No. 9,203,806 ("'806 Patent")

17. One or more non-transitory computer-readable media comprising instructions that when executed by a computing system cause the computing system to:

receive a first rule set and a second rule set;

preprocess the first rule set and the second rule set to optimize performance of the computing system for processing packets in accordance with at least one of the first rule set or the second rule set;

configure at least two processors of the computing system to process packets in accordance with the first rule set;

after preprocessing the first rule set and the second rule set and configuring the at least two processors to process packets in accordance with the first rule set, receive a plurality of packets;
process, in accordance with the first rule set, a portion of the plurality of packets;
signal, each processor of the at least two processors, to process packets in accordance with the second rule set; and
configure, each processor of the at least two processors to, responsive to being signaled to process packets in accordance with the second rule set:
cease processing of one or more packets;
cache the one or more packets;
reconfigure to process packets in accordance with the second rule set;
signal completion of reconfiguration to process packets in accordance with the second rule set; and
responsive to receiving signaling that each other processor of the at least two processors has completed reconfiguration to process packets in accordance with the second rule set, process, in accordance with the second rule set, the one or more packets.

U.S. Patent No. 9,560,176 ("'176 Patent")

21. One or more non-transitory computer-readable media comprising instructions that when executed by a computing system cause the computing system to:
identify a plurality of packets received by a network device from a host located in a first network;
generate a plurality of log entries corresponding to the plurality of packets received by the network device;
identify a plurality of packets transmitted by the network device to a host located in a second network;
generate a plurality of log entries corresponding to the plurality of packets transmitted by the network device;
correlate, based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device, the plurality of packets transmitted by the network device with the plurality of packets received by the network device; and
responsive to correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device:
generate, based on the correlating, one or more rules configured to identify packets received from the host located in the first network; and

provision a device located in the first network with the one or more rules configured to identify packets received from the host located in the first network.

U.S. Patent No. 9,917,856 ("'856 Patent")

24. A packet-filtering system comprising:
at least one hardware processor; and
memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to:
receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;
identify packets comprising unencrypted data;
identify packets comprising encrypted data;
determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;
filter, based on at least one of a uniform resource identifier (URI) specified by a plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:
packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and
the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and
route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

CERTIFICATE OF INTEREST

Counsel for Centripetal Networks, Inc. certifies the following:

1. The full name of every entity represented by us is:

   Centripetal Networks, Inc.

2. The name of the real party in interest for the entity. Do not list the real party if it is the same as the entity:

   Not applicable.

3. All parent corporations and any other publicly held companies that own 10 percent or more of the stock of the party or amicus curia represented by me are listed below:

   None.

4. The names of all law firms, and the partners or associates that have not entered an appearance in the appeal, and (a) appeared for the entity in the lower tribunal; or (b) are expected to appear for the entity in this court:

   Yuridia Caire, Melissa Brenner, Kristopher Kastens, Hien Lien, Gregory Proctor, Michael Lee, Julian Pymento, Jeffrey Eng, Shannon Hedvat, Cristina Martinez, Eileen Patt, Jonathan Caplan and Aaron Frankel of Kramer Levin Naftalis & Frankel LLP;

   Jeffrey Thomas Martin, Jr. of Henry & O'Donnell, P.C. and Kevin Martin O'Donnell of Henry & O'Donnell, P.C.; and

   Stephen Edward Noona of Kaufman & Canoles, P.C.

5. Other than the originating case number(s), the title and number of any case known to counsel to be pending in this or any other court or agency that will directly affect or be directly affected by this court's decision in the pending appeal

   - *Palo Alto Networks, Inc. v. Centripetal Networks, Inc.*, No. IPR2021-01520 (P.T.A.B.)

- *Palo Alto Networks, Inc. v. Centripetal Networks, Inc.*, No. IPR2021-01521 (P.T.A.B.)

- *Palo Alto Networks, Inc. v. Centripetal Networks, Inc.*, No. IPR2022-00182 (P.T.A.B.)

6. All information required by Fed. R. App. P. 26.1(b) and (c) in criminal cases and bankruptcy cases.

   None.

Respectfully submitted,

Dated: December 6, 2021

By: */s/ Paul J. Andre*

Paul J. Andre
Kramer Levin Naftalis
& Frankel LLP
990 Marsh Road
Menlo Park, CA 94025
Tel: 650.752.1700
Fax: 650.752.1810
pandre@kramerlevin.com

Attorneys for Plaintiff-Appellee,
Centripetal Networks, Inc.

TABLE OF CONTENTS

CONFIDENTIAL MATERIAL OMITTED

The material omitted from pages 43-46 contains a description of a confidential license agreement between Centripetal and a third party that was sealed in the district court.

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Legislative Material

Other Authorities

STATEMENT OF RELATED CASES

Pursuant to Federal Circuit Rule 47.5, Centripetal Networks, Inc. states that:

No appeal in this case was previously before this Court or any other court.

The following cases are pending before the U.S. Patent Trial and Appeal Board regarding the '176, '193 and '856 Patents:

- *Palo Alto Networks, Inc. v. Centripetal Networks, Inc.*, No. IPR2021-01521 (U.S. Patent No. 9,560,176) (P.T.A.B.)
- *Palo Alto Networks, Inc. v. Centripetal Networks, Inc.*, No. IPR2021-01520 (U.S. Patent No. 9,686,193) (P.T.A.B.)
- *Palo Alto Networks, Inc. v. Centripetal Networks, Inc.*, No. IPR2022-00182 (U.S. Patent No. 9,917,856) (P.T.A.B.)

INTRODUCTION

Cisco gives no deference to the district court's extensive findings of fact and credibility determinations, and asks this Court to do the same. Presiding over a twenty-two-day bench trial and a damages hearing, Judge Henry Coke Morgan, Jr. observed thirty-five witnesses and testimonial evidence concerning hundreds of trial exhibits. He "had the opportunity to observe the demeanor and hear the live testimony of witnesses by video/audio and by deposition at trial [and] made certain credibility determinations, as well as determinations relating to the appropriate weight to accord the testimony." Appx51. He subsequently issued two orders totaling 217 pages based on the extensive record and his credibility determinations. Cisco disregards or mischaracterizes most of the Judge's detailed findings of facts and conclusions of law.

Cisco launched its "network of the future" featuring Centripetal's patented technology after Centripetal and Cisco had multiple meetings covered by a nondisclosure agreement ("NDA") where Centripetal disclosed its protected algorithms and patented technology. Centripetal's patented technology transformed traditional network devices—like Cisco's traditional routers, switches and firewalls—into integrated security solutions. The launch of Cisco's infringing products was wildly successful, grossing over $21 billion in less than three years. Centripetal received neither credit nor compensation.

Adding insult to injury, Cisco argued at trial that Centripetal's innovations were actually old Cisco technology. Undeterred by its own documents heralding revolutionary advances in network security, Cisco claimed the new solutions already existed in legacy products, which it characterized as invalidating prior art. This strategy led Cisco to focus on its old technology at trial, advancing invalidity arguments that it has abandoned on appeal while simultaneously failing to acknowledge the accused functionality. The court expressed frustration with Cisco's tactics and ultimately determined that Cisco directly and willfully infringed four of Centripetal's patents.

On appeal, Cisco again fails to ground its arguments in the factual record, attempting to sow confusion regarding the functionality of its accused products, the value of the infringing technology and the history of how Centripetal's solutions ended up in Cisco's products. Judge Morgan issued detailed findings of fact based on Cisco's own documents and his credibility determinations. His work is thorough; it is correct; and it is entitled to significant deference by this Court.

STATEMENT OF ISSUES

1. Whether, after weighing the witnesses' credibility and Cisco's documents to provide detailed factual findings, the court committed clear error or abuse of discretion in finding Cisco directly infringed Centripetal's patents by making, using, offering to sell or selling Cisco's products.

2. Whether the court committed clear error or abuse of discretion in following this Court's precedent regarding apportionment and relying upon the only comparable license in the record as a starting point for the royalty rate.

3. Whether the court committed reversible error in finding this was an "egregious case of willful misconduct beyond typical infringement" and enhancing damages based on Cisco's blatant copying of Centripetal's patented technologies.

4. Whether the judge abused his discretion in determining that recusal under 28 U.S.C. § 455(b) was unnecessary.

STATEMENT OF THE CASE

A. Centripetal Operationalized Threat Intelligence and Patented Its Inventions

In 2009, decorated veteran Steven Rogers founded Centripetal to develop a new solution that leveraged threat intelligence to detect and proactively stop cybersecurity threats. Appx1235-1236; Appx1308-1309. Following a $65 million investment in research and development, Centripetal launched its patent-practicing RuleGATE system and CleanINTERNET service marked with its patents that collect, process and implement threat intelligence. Appx192; Appx1242-1243; Appx2204-2205.

'193 Patent: Cybercriminals use dangerous security breaches called exfiltration attacks to hijack computers on a network and steal ("exfiltrate") data. Appx128-129. Protecting against these attacks had proven difficult, and

counter-measures were crude. Cisco's previous technology identified potentially compromised computers and completely shut down any network traffic to or from those machines (Appx4017-4018), resulting in significant productivity costs. The '193 Patent prevents potentially compromised computers from making a particular type of data transfer, *e.g.*, accessing a company's sensitive data, while allowing other types of data transfers, *e.g.*, accessing the internet.

'806 Patent: Network devices may include rules to monitor and filter network traffic. Because cyber threats evolve rapidly, these rules require frequent updates. Appx142. Centripetal recognized that "[a]s rule sets increase in complexity, the time required for switching between them presents obstacles for effective implementation" and often results in dropping packets. Appx283 (1:20-22). The '806 Patent preprocesses rules and performs rule swaps between the processing of packets to ensure none are dropped. Appx284 (4:60-64); Appx288 (11:40-53).

'176 Patent: Centripetal recognized that it could identify malware-infected computers on a network through "correlation" techniques. Appx112; Appx1340-1341. Centripetal's technology analyzes and correlates logs corresponding to network traffic to identify and remediate unusual activity using network security rules. Appx1973-1975. The '176 Patent transforms traditional switches and routers into a system that can sense and react to network threats.

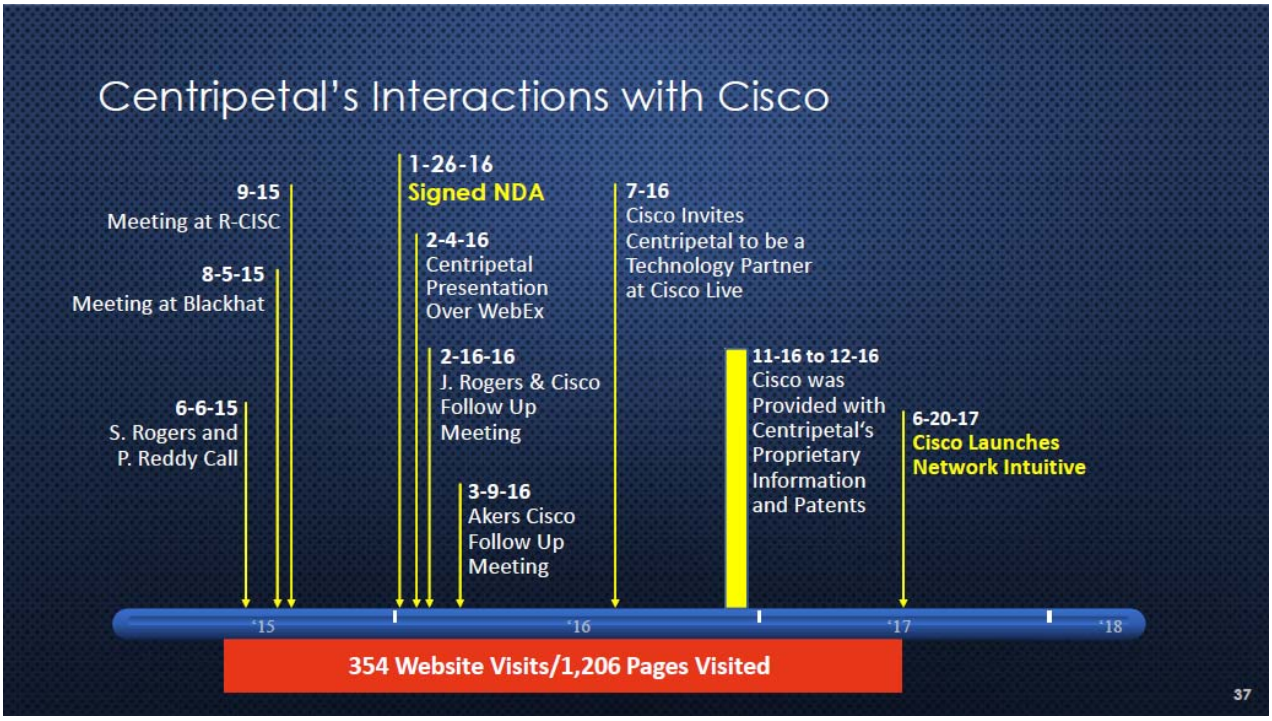
'856 Patent: Encryption plays an important role in online security, but hackers can encrypt traffic to obfuscate dangerous malware and evade detection. Appx344 (1:17-20). Centripetal invented a system that detects and blocks threats in encrypted network traffic without using the traditional, slow and computationally expensive process of decrypting, inspecting and re-encrypting packets. Appx75.

B. Cisco Needed Centripetal's Solution and Entered into an NDA to Access It

Facing commoditization of its network devices, Cisco needed a differentiator. Appx2455 (2016 10-K describing "increased competition . . . based on commoditized hardware"). In 2015, Cisco contacted Mr. Rogers because Centripetal's technology "fit into the types of solutions [Cisco] needed for customers . . . that went beyond the offerings that Cisco had at the time." Appx192 (citing Appx1256-1257).

Thereafter, Centripetal and Cisco signed an NDA to explore jointly selling Centripetal technologies in Cisco products. Appx2216. Centripetal had at least six meetings with Cisco's technical and corporate development teams and provided multiple demonstrations of RuleGATE and its patented functionalities. Appx192-195. At Cisco's invitation, Centripetal presented its patented solution at the Cisco Live conference as Cisco's technology partner. Appx2300. While Cisco purported to be interested in a partnership or investment, Cisco's employees accessed over

1,200 pages on Centripetal's website during the course of over 350 visits (Appx195; Appx2024 (1024:16-25)), as summarized in the timeline from the court's opinion:



Appx195.

After signing the NDA, Centripetal disclosed substantial confidential information to Cisco. At a February 2016 meeting, Centripetal presented "detailed, highly sensitive, confidential and proprietary information about its patented technology and products," including its patented filter algorithms to prevent exfiltration ('193 Patent), correlation algorithms ('176 Patent) and Centripetal's patented technologies for detecting threats in encrypted traffic ('856 Patent) and rule swapping ('806 Patent). Appx193; Appx2222-2225; Appx5127-5129. After

that meeting, a Cisco engineer told his team to "look at [Centripetal's] algorithms" and "study their [patent] claims." Appx193 (citing Appx5055).

Cisco continued to receive additional Centripetal confidential information through late 2016, including a list of Centripetal's issued patents, patent-practicing products and highly sensitive technical disclosures detailing RuleGATE's core patented functionalities. Appx193-194 (citing Appx5813-5818); Appx2244-2245.

C. Cisco Incorporated Centripetal's Patented Technologies into Its Products

In June 2017, Cisco unveiled its "network of the future" that "stops security threats in their tracks." Appx194-195 (citing Appx5247). Cisco's new line of network products integrated security into its switches, routers and firewalls with corresponding management software to generate, process and enforce rules that protect against network threats. *See, e.g.*, Appx5180.

Switches: Cisco's Catalyst 9000 series switches ("Switches") infringe. After learning of Centripetal's threat-intelligence-based security, Cisco reengineered them to be "built for security" and "designed to enable customers to detect threats, for instance, in encrypted traffic" as part of "a critical part of an end-to-end integrated security solution, one that detects and stops threats." Appx5381; Appx5450. They can enforce a variety of security rules to forward or drop packets.

Routers: Cisco's Integrated Services Routers ("ISR") and Aggregation Services Routers ("ASR") (collectively "Routers") infringe. Cisco redesigned

them to enforce network security rules that forward or drop packets. Appx1443-1444.

Firewalls: Cisco designed a new architecture for its Firepower and Adaptive Security Appliance firewalls ("Firewalls"), integrating them with management software called Firepower Management Center ("FMC"). Appx144; Appx1558. Cisco's Firewalls provide a new level of network security based on threat indicators with new types of rules that FMC processes and that can be swapped efficiently in the devices. Appx144; Appx1694-1695.

DNA: Cisco embeds Digital Network Architecture ("DNA") management software in Switches and Routers. Appx143; Appx5415. DNA processes rule sets, which Switches and Routers swap without packet loss. Appx143-144. DNA's "primary function is to interact and operate routers and switches" providing the infringing capabilities. Appx61-62.

Stealthwatch: Cisco's Stealthwatch software analyzes traffic flowing through Switches and Routers to "detect and respond to threats in real-time." Appx5143; Appx5172; Appx5199. This analysis involves correlating traffic that enters and leaves devices in the network to determine whether the traffic contains a threat. Appx1994-1995; Appx5222. Detected malicious traffic can be "blocked or quarantined by Stealthwatch," which involves sending rules to Switches and

Routers. Appx5178. Cisco touts Stealthwatch as a "feature" of Routers, selling Stealthwatch with Switches and Routers "as one product." Appx2467; Appx5457.

ETA: Cisco embeds Encrypted Traffic Analytics ("ETA") into Stealthwatch, Switches and Routers. Appx62; Appx1887-1888; Appx1890 (testimony regarding Appx5143); Appx5034 (functionality "built in to the system"); Appx5523 (55:25-56:9). Cisco touts ETA as a "feature" of and "benefit of upgrading to" its redesigned Switches and Routers. Appx5381; Appx5143; Appx5378-5379; Appx5457.

ISE: Identity Services Engine ("ISE") software provides "[c]entral network device management" and "granular control of who can access which network device." Appx5097. Stealthwatch and ISE "work together" as "an integrated solution." Appx5215-5216; Appx5513 (68:07-69:22); Appx5191. ISE can generate rules enforced by Switches and Routers to protect networks from threats, even in encrypted traffic.

D. The District Court Made Detailed Findings of Fact after a Lengthy Trial

After expending significant effort to arrive at its judgment, the court found four of Centripetal's patents valid and infringed, and found no infringement of a fifth patent. Appx65-66. Over a 22-day trial and damages hearing (Appx46), the court heard thirty-five witnesses and reviewed over 300 exhibits, producing a record of over 3,500 pages. Appx29-30; Appx47-51. The court spent months

preparing a detailed 167-page order explaining its judgment. Later, it denied Cisco's post-trial motions in another detailed 50-page order.

The court found Centripetal's experts credible, accurate and persuasive because they relied on Cisco's documents and fact witnesses. Cisco's experts, however, advanced "objectively unreasonable" positions that were "unpersuasive and in many instances not credible." Appx227-229. The court found that "[m]ost of Cisco's challenges amounted to no more than conclusory statements by its experts without evidentiary support" (Appx72) and Cisco's demonstratives "***contradicted*** Cisco's employee witnesses" and "***conflict[ed]*** with Cisco's own technical documents." Appx202 (emphases added). These credibility determinations were integral to the court's decisions.

The court found Cisco's contentions about the value of the infringing technologies similarly "unsupportable" based on Cisco's own documents and data. Appx105-108. Cisco contended they were identical to its previous products and of minimal value. But the court found none of Cisco's older products offered the patented functionalities. Appx108; Appx125; Appx140; Appx155-156. The patented technologies "added very significant value" and Cisco enjoyed increased revenues and strong profits for the infringing products and repeatedly stressed the importance and success of the technologies. Appx180-185.

The court conducted a detailed *Georgia-Pacific* analysis, using the only comparable license in the record (the Centripetal-Keysight agreement) as a "baseline." Appx171-192. Although this agreement applied a royalty rate to unapportioned revenues of licensed products, the court conservatively apportioned Cisco's infringing revenues and applied a royalty rate based on credible evidence. *Id.* It enhanced the award based on Cisco's "egregious case of willful misconduct beyond typical infringement." Appx204.

E. Judge Morgan Discovered His Wife's Interest in Cisco after Deciding the Case

After trial and "a full draft of [the court's] opinion had been prepared" with "virtually every issue decided," Judge Morgan discovered his wife owned 100 shares of Cisco stock valued at less than $4,700. Appx30. Because he had no knowledge of the shares throughout the entirety of the case and his decision-making process, the shares "did not and could not have influenced [his] opinion on any of the issues in this case." *Id*.

Cisco moved for recusal, arguing that divestment was not an option. After Judge Morgan determined that recusal would be improper, his wife divested her stock into a blind trust because selling the stock could create the appearance of using insider information to avoid a loss in advance of the judgment against Cisco. Appx18593; Appx42-43.

SUMMARY OF ARGUMENT

The court did not clearly err in its factual findings that Cisco makes, uses, markets (offers for sale) and sells its hardware and software network security products as integrated solutions; and that Cisco embeds its infringing software, including ISE, FMC, DNA and Stealthwatch in Switches, Routers and Firewalls. Cisco's attempt to transform direct infringement into a legal issue depends on a misinterpretation of *Deepsouth Packing Co. v. Laitram Corp*., 406 U.S. 518 (1972), that this Court has repeatedly rejected. Cisco cannot escape infringement liability simply by splitting its infringing system into separate invoice line items, particularly in view of its infringing manufacturing and use.

Cisco identifies no clear error in the court's infringement findings and credibility determinations, which flowed from Cisco's numerous attempts to advance arguments in conflict with its own documents and fact witnesses. The court correctly determined that Switches and Routers practice every limitation of the '193 Patent by applying network security rules to forward or drop packets, ensuring that potentially compromised computers can remain online without accessing sensitive information. These same Switches and Routers, in combination with software embedded as part of Cisco's integrated security solutions, practice every limitation of the '176 Patent by generating new rules based on threats identified by correlating network traffic and the '856 Patent by

detecting and blocking threats in encrypted network traffic without requiring decryption. These products, as well as Firewalls and related embedded software, likewise practice every limitation of the '806 Patent by swapping network security rules without dropping packets.

Cisco also fails to identify any clear error or abuse of discretion in the court's damages award. The court found each Switch and Router individually practices every limitation of the '193 Patent, which Cisco wrongly characterizes as being combined with other products to infringe. As such, the court properly included revenues from those products in the royalty base based solely on Cisco's infringement of the '193 Patent. And because Switches, Routers, Firewalls and related software are designed, made, used, marketed and sold as integrated solutions that directly infringe the '806, '176 and '856 Patents, the court properly included their revenues in the royalty base. The court then appropriately considered and adjusted the only comparable license in the record as part of its detailed *Georgia-Pacific* analysis and conservatively apportioned Cisco's revenue base.

Cisco fails to establish reversible error in the court's careful analysis and specific factual findings regarding Cisco's unabated and deliberate copying of Centripetal's patented technology, which the court accurately described as an "egregious case of willful misconduct beyond typical infringement." Appx204.

The court did not abuse its discretion when it enhanced damages against this factual backdrop and determined that Cisco's non-infringement and invalidity arguments were not a close call, particularly in view of the infirmities of Cisco's defenses and its misleading and contradictory trial evidence.

Finally, Cisco strains credulity in arguing that Judge Morgan abused his discretion by declining to recuse himself after his wife promptly divested less than $4,700 of Cisco stock once he learned of the shares after already deciding the case's outcome. He promptly disclosed the issue to the parties and his wife divested into a blind trust, curing any potential appearance of bias.

ARGUMENT

I. STANDARD OF REVIEW

Cisco's appeal seeks to relitigate the court's factual findings, which "must not be set aside unless clearly erroneous." Fed. R. Civ. P. 52(a)(6). This Court may not supplant the court's findings with its own simply if "it would have weighed the evidence differently." *Anderson v. City of Bessemer City*, 470 U.S. 564, 573-74 (1985); *Inwood Labs., Inc. v. Ives Labs., Inc.*, 456 U.S. 844, 856 n.16 (1982) (reasonable inference is not clear error even if evidence potentially supports other inferences). All such factual findings—including those underlying any ultimate legal conclusions—are entitled to deferential clear error review. *Endo Pharms. Sols., Inc. v. Custopharm Inc.*, 894 F.3d 1374, 1379 (Fed. Cir. 2018).

Here, even "greater deference" is required because the court supported its findings with credibility determinations, detailing the persuasive evidence corroborated by Cisco's documents and fact witnesses. *Anderson*, 470 U.S. at 575 (crediting one witness over another "can virtually never be clear error"); *see, e.g.*, Appx66-67, Appx203-204. It is not for the appellate court to reverse a trier of fact "on a question of credibility" or "second-guess" these determinations. *Equinor USA Onshore Props. Inc. v. Pine Res., LLC*, 917 F.3d 807, 815 (4th Cir. 2019).

Abuse of discretion applies to the court's decisions to enhance damages, admit expert testimony, choose damages-related methodologies and not recuse. *Whitserve, LLC v. Comput. Packages, Inc.*, 694 F.3d 10, 26, 35 (Fed. Cir. 2012).

II. BASED ON THE EVIDENCE PRESENTED AT TRIAL AND CREDIBILITY DETERMINATIONS, THE DISTRICT COURT PROPERLY FOUND DIRECT INFRINGEMENT AND THE CORRESPONDING ROYALTY BASE

A. Cisco Makes, Uses, Offers for Sale and Sells Infringing Products

Cisco's allegation of ***legal*** errors in the court's direct infringement analysis (Cisco's Opening Brief ("Br.") 16-21), depends on misapplications of law and incorrect factual premises.

1. Each Switch and Router Individually Infringes the '193 Patent

Contrary to Cisco's statement (Br. 18), the court did not find that Switches and Routers must be combined with Stealthwatch or ISE to infringe the '193 Patent. It found that each Switch and Router ***alone*** infringes:

- "Cisco's Catalyst 9000 series ***switches***, the Aggregation Services Router 1000 series ***routers*** and the Integration Services Router 1000 and 4000 series ***routers*** literally INFRINGE Claims 18 and 19 of the '193 Patent." (Appx132) (emphases added);
- Switches and Routers satisfy all claim elements. (Appx127-137);
- "[T]he accused products perform all the functionality required to infringe the claims." (Appx137);
- Cisco presentation shows "switches and routers perform" infringing process, and do not require combination with ISE. (Appx257-260) (citing Appx5438-5439); and
- "Cisco technical documents . . . demonstrate that Stealthwatch is not involved in the two stages of the infringing functionality." "[A]ny evidence regarding Stealthwatch has no bearing on infringement for the '193 Patent." (Appx138).

Cisco challenges non-existent accused combinations by citing the court's description of Switches and Routers in the context of Cisco's integrated security system. Br. 18 (citing Appx133). As the court explained, ISE and Stealthwatch may generate network security rules used by Switches and Routers. Appx133. But the claims do not require rule generation or transmission. *See* Appx325-326. The court correctly found that each Switch and Router ***alone*** infringes the '193 Patent by ***enforcing*** rules, which does not require ISE or Stealthwatch. Appx129;

Appx133-138 (Switches and Routers "are the specific network devices used to institute this packet filtering system"). Specifically, the court found that the packet filtering process that each Switch and Router performs independently "meets the functionality required by the asserted claims." Appx133. Thus, Cisco's "combination" arguments have no relevance to the '193 Patent.

2. Cisco's Integrated Systems Infringe the '806, '176 and '856 Patents

Relying principally on *Deepsouth*, Cisco contends that it cannot be liable for direct infringement of Centripetal patents that require combinations of Cisco's allegedly separately sold hardware and software. Br. 16-21. However, "*Deepsouth* was intended to be narrowly construed as applicable only to the issue of the extraterritorial effect of the American patent law," *Paper Converting v. Magna-Graphics Corp*., 745 F.2d 11, 17 (Fed. Cir. 1984), which is absent here. Appx242; *see also Deepsouth*, 406 U.S. at 531.

Rotec Industries, Inc. v. Mitsubishi Corp. also involved extraterritoriality and a defendant who sold only ***some*** infringing components. 215 F.3d 1246, 1252 (Fed. Cir. 2000). Cisco cites *Rotec*'s statement that "one may not be held liable . . . for 'making' or 'selling' less than a complete invention" (Br. 17), but Cisco does not deny that it makes, uses, offers for sale and sells ***all*** the infringing components. As described below, it makes, uses and sells them as integrated systems providing comprehensive security solutions.

a. Cisco Offers for Sale and Sells Infringing Integrated Systems

The court correctly found that Cisco markets and sells combinations of Switches, Routers, Firewalls and other products, such as Stealthwatch, DNA, ISE and FMC, as integrated systems designed to work together. *See*, *e.g.*, Appx228 ("The evidence demonstrates that the accused products were made and sold to be used in the United States embedded with and in combination with the infringing technology."); Appx243 (Cisco never offered rebuttal evidence to establish that its "infringing software was not embedded in its traditional hardware and sold in combination with it"). These integrated systems provide network security functionality "of critical importance" to Cisco and its customers. Appx234; Appx235-236 (quoting testimony that Switches and Routers "come with" infringing software "even though they might have a separate charge, . . . ***they're selling it as one product***") (emphasis added). The evidence included:

- Cisco's expert testimony that "good network administration" requires "a layered defense" "where you have ***firewalls . . .*** and ***Stealthwatch*** . . . [for] a ***comprehensive technique***. Comprehensive ***set of products***." Only "customers [who] are extremely looking forward to having their networks hacked" would forego deploying Cisco's security technologies together as designed. (Appx232) (emphases added);
- Cisco presentation identifying how the infringing products work together as a security solution (Appx5198);
- Cisco's webpage showing security benefits of Firewalls with FMC as a package (Appx5060-5061);

- Cisco's SEC statements that Cisco delivers an integrated "cybersecurity architecture." (Appx2456-2457); (Appx5140) ("By combining a number of security technologies, we are delivering an end-to-end zero trust architecture."); and
- Cisco whitepaper stating Switches and DNA are "a critical part of an end-to-end integrated security solution" (Appx5381).

The court also cited extensive evidence supporting its finding that Cisco Switches, Routers and Firewalls embedded with infringing software directly infringe. Appx228-229 (infringing software embedded in Switches, Routers and Firewalls); Appx230-232 (Cisco's expert explaining press release (Appx5189) showing ETA embedded in Switches); *see also* Appx5076-5077 (Cisco marketing Stealthwatch as part of Switches and Routers).

The court also relied on Cisco's marketing materials, finding Cisco sells DNA, Stealthwatch and ETA as "features" of Switches and Routers, directly contradicting Cisco's claim it sells them without this functionality embedded. Appx234 (quoting testimony about internal Cisco presentation (Appx5038) regarding "embedding" ETA into Switches); Appx235-236 (quoting testimony regarding Cisco document (Appx5456-5457) showing DNA, Stealthwatch and ETA as Router features).

Cisco nonetheless argues it cannot directly infringe because customers must combine or "assemble" these components or activate embedded features. *See, e.g.*, Br. 19-20. But this Court has found direct infringement where users "must activate

the functions" when "the user is only activating means that are ***already present in the underlying software***." *Fantasy Sports Props., Inc. v. SportsLine.com, Inc.*, 287 F.3d 1108, 1118 (Fed. Cir. 2002) (emphasis added). Similarly, "if a device [here, an integrated system] is designed to be altered or assembled before operation, the manufacturer may be held liable for infringement if the device, as altered or assembled, infringes a valid patent." *High Tech Med. Instrumentation, Inc. v. New Image Indus., Inc.*, 49 F.3d 1551, 1556 (Fed. Cir. 1995).

At bottom, while Cisco argues it cannot directly infringe because it charges separately for components of these integrated systems, it fails to explain why splitting an otherwise infringing system into separate line items should preclude liability.

Courts have held others liable in similar circumstances. For example, in *Immersion Corp. v. Sony Computer Entertainment America, Inc.*, No. C 02-0710 CW, 2005 U.S. Dist. LEXIS 4777 (N.D. Cal. Jan. 10, 2005), Sony directly infringed where it separately sold consoles, controllers and computer games because it designed them to be interoperable and "advertises and sells" them as a system. *Id.* at *16. Likewise, Cisco designed Switches, Routers, Firewalls and related products to work together, and advertises and sells them as integrated systems. Another court found direct infringement for selling separate fluid tanks that customers assembled into an infringing structure. *EBS Auto. Servs. v. Ill. Tool*

Works, Inc., No. 09-CV-996 JLS (MDD), 2011 WL 4021323, at *5-6 (S.D. Cal. Sept. 12, 2011) (citing *High Tech* and noting "the patent laws do not allow a manufacturer to avoid infringement simply by selling a disassembled device that would infringe on assembly").

b. Cisco Makes Infringing Integrated Systems

Regardless of Cisco's arguments about customer choices, Cisco directly infringes the system and computer-readable media claims of the '806, '176 and '856 Patents because it makes the infringing systems and software. There are no asserted method claims, so all that is required is the existence of the claimed functionality, even if customers must activate particular features. *Finjan, Inc. v. Secure Computing Corp.*, 626 F.3d 1197, 1204-05 (Fed. Cir. 2010) (holding that the need to activate functions "by purchasing keys does not detract from or somehow nullify the existence of the claimed structure in the accused software"). System and storage medium claims do not require the performance of any method steps. *Id.* at 1203-06 (code for performing claimed functionality infringed computer-readable medium claim). Cisco directly infringes once it makes all components of the system that can perform the claimed functions, regardless of whether a customer subsequently puts the system into use.

c. Cisco Itself Uses Infringing Integrated Systems

Cisco did not dispute that it uses and tests DNA, Stealthwatch and ISE with Switches and Routers, and FMC with Firewalls. *See, e.g.*, Appx5524; Appx2664-2665; Appx2701. Cisco's use directly infringes Centripetal's patents and alone compels affirmance. *NTP, Inc. v. Research in Motion, Ltd.*, 418 F.3d 1282, 1317 (Fed. Cir. 2005) (system claim infringed when system put into service); *Segan LLC v. Zynga Inc.*, No. 11-670-GMS, 2013 WL 12156529, at *1 n.1 (D. Del. May 2, 2013) (internal use of accused product infringes system claims).

B. The District Court Did Not Clearly Err by Including All Infringing Sales in the Royalty Base

There was a factual dispute regarding the revenues to include in the royalty base. Centripetal contended Cisco sells its products as infringing integrated systems. Cisco contended it sometimes sells components separately. There is no legal error. The court resolved this dispute in Centripetal's favor, finding Centripetal's evidence to be "credible and persuasive" and rooted in Cisco's confidential documents, public representations and testimony. Appx227-236.

As discussed above, Centripetal demonstrated that Cisco sells the infringing products as integrated systems and that Cisco makes, uses and sells Switches, Routers and Firewalls "embedded with and sold in combination with the infringing technology." Appx243; *see also* Appx230-236; Appx2502-2503; *supra* § II(A)(2). Based on that factual finding, the royalty base only includes revenues of infringing

systems, and does not include product revenues that were not infringing combinations, as Cisco contends.[1]

Cisco offered no credible rebuttal evidence. Appx229-243. Cisco never identified in the royalty base any sales of products other than in the infringing combinations. Instead, Cisco excluded from its proposed royalty base ***all*** revenues from Switches, Routers and Firewalls. Appx3945-3946. The court rejected Cisco's proposal as a "deeply flawed" position that was "completely unrealistic . . . compared to the reality of the marketplace," where Cisco offered for sale and sold its infringing products as integrated systems. Appx203-204.

Critically, noting the "tremendous" disparity between the parties' damages calculations and Centripetal's unrebutted evidence, the court gave Cisco yet another opportunity ***after the close of all evidence*** to provide rebuttal evidence that its products were not sold as integrated systems. Appx236-239; Appx3976-3987. The court requested that Cisco provide "sales figures based upon [Cisco's] damages theory," reflecting "what [Cisco] considered to be the relevant products." Appx238. It even invited Cisco to provide anything "you think would be helpful" because "you're not limited by what I ask for." Appx239. Despite the court's extraordinary request and having several weeks to compile such evidence, Cisco

[1] This distinguishes cases like *Omega Patents, LLC v. CalAmp Corp.*, 920 F.3d 1337, 1350-51 (Fed. Cir. 2019), which addressed a royalty base with non-infringing products. Br. 23.

"did not produce any compilation of sales figures to support [its] theory of damages." Appx238-239 (Cisco's "sales data . . . was not furnished").

Cisco also argues that damages "must be" correlated to customer use (Br. 21), but the court considered "the great extent [to] which Cisco . . . made use of the patented invention" in its detailed *Georgia-Pacific* analysis. Appx182-185. It considered Cisco's "technical documents, marketing representations, and the sales data" and found they warranted "a substantially increased royalty figure" because the patented technology added "very significant value." Appx185. As Centripetal explained, the scope of Cisco's infringement includes all infringing products Cisco made and used—not just sold—which should be included in the royalty base. Appx2502-2503.

III. INFRINGEMENT OF CENTRIPETAL'S PATENTS

A. Cisco Infringes Claims 18 and 19 of the '193 Patent

1. The District Court Specifically Found that Cisco's Infringing Switches and Routers "Prevent a Particular Type of Data Transfer"

Switches and Routers infringe the '193 Patent by preventing potentially compromised computers from exfiltrating sensitive data without the productivity costs of taking those machines completely offline.

Cisco wrongly argues that the court ignored the limitation, "prevent a particular type of data transfer." Br. 46, 50. The court correctly found that

Switches and Routers "operate[] by ***blocking packets*** affiliated with a ***particular type of data transfer*** to a protected resource, while allowing packets unaffiliated with a protected type of data transfer to be transmitted to their final destination." Appx135 (emphases added); Appx136 (Cisco's documents "show[] infected endpoints can be ***denied access to certain types of data*** while being ***allowed access to other types of data***") (emphases added). The court's findings are well-supported by the record.

Switches and Routers enforce what Cisco calls a "quarantine rule" by attaching Scalable/Secure Group Tags ("SGTs") to network packets and applying a set of rules known as Secure Group Access Control Lists ("SGACLs"), which apply operators to the packets, such as "permit" or "deny," that result in the packets being forwarded or dropped. Appx134-135. As in the '193 Patent, Switches and Routers attach SGTs to network packets based on information in the packet headers, including the source and destination IP addresses, the source and destination ports, and the protocol. Appx130; Appx134; Appx1782-1783; Appx3405.

These SGACLs prevent particular types of data transfers to or from potentially compromised computers—*e.g.*, transfers involving networks with sensitive information—but allow transfers involving other networks, such as the Internet. Appx130-136; Appx1541-1542 (testimony regarding Cisco document

(Appx5147) illustrating in color, blocking access (red) or allowing access (green) to certain types of data); Appx1547-1548 (Switches and Routers apply rules to drop or forward packets associated with a particular "type of data transfer"). As Cisco's documents state, "[d]evices that are suspected of being infected can be denied access to critical data while their users can keep working on less critical applications." Appx5431. Other traffic to or from the compromised computer's network is not affected.

2. Cisco Mischaracterizes How Its Products Function

The lynchpin of Cisco's argument on appeal—that Switches and Routers block or allow "***all*** packets, between a given source and destination" (Br. 49)—is factually incorrect. Contrary to Cisco's assertion (Br. 47), the court expressly found that—in addition to source and destination IP addresses—SGTs "can also be based on other information that is included in the 5-tuple [information in the packet header]," such as the port and protocol. Appx130. Both sides' experts support this finding. *See* Appx1782-1783; Appx3405-3406; Appx3409.

Because SGTs can be attached based on information other than source or destination IP addresses, Switches and Routers can ***selectively*** block network traffic between the same source and destination. Centripetal's expert testified that Switches and Routers "may also look at the port, which would specify whether it's HTTP [hypertext transfer protocol] or not." Appx1793; *see also* Appx1783

("typical port number for HTTP is 80"); Appx5401 (permitting/denying packets based on "protocol" like HTTP or FTP); Appx5399-5401 (rules also not limited to source and destination IP addresses but can include ports, etc.).

The '193 Patent teaches this precise functionality, explaining that filtering criteria "may take the form of a five-tuple, which may, for example, comprise one or more values selected from, packet header information, specifying a protocol type . . . , one or more source IP addresses, one or more . . . port values, one or more destination IP addresses . . . ." Appx321 (5:52-60); Appx317 (Fig. 3); Appx319 (2:11-15).

The court cited an example from a Cisco technical paper illustrating how Switches and Routers use SGTs and SGACLs to prevent a particular type of data transfer from a potentially compromised machine. In this example, Switches and Routers apply an SGACL (to packets with SGTs) to prevent a computer associated with a "supplier" from accessing sensitive data in a second network, such as data in a "shared server," while still allowing it to access data on the Internet. Appx134 (reproducing Appx5146); Appx5393 (explaining that SGTs can "limit the endpoint's network access"); Appx1496-1499.

3. Cisco Misstates the '193 Patent Claims

Cisco argues that the "particular type of data transfer" limitation requires inspecting packet contents for methods (used by a protocol) such as GET and PUT.

Br. 46-48. Claims 18 and 19 contain no such requirements, as highlighted by unasserted claims that do cover such embodiments. *See* Appx325 (PUT in Claim 11 and GET in Claim 15). Cisco cannot import these limitations.

Furthermore, Cisco is mistaken that "[i]nfringement would require a finding that Cisco's products block a computer from accessing 'sensitive data' from a 'protected' destination while allowing that same computer access to other data from the ***same*** destination." Br. 49. While Switches and Routers do just that, as discussed above, Claims 18 and 19 are not limited to blocking some, but not all, data between the "same computer" and the "same destination." Appx325-326.

Those claims recite "prevent[ing] a particular type of data transfer from the ***first network*** to a ***second network***" and forwarding other data transfers "toward the ***third network***." *Id.* (emphases added). Cisco ignores the claims' express reference to the third network and instead attempts to rewrite the claims more narrowly, as if they were directed to a two-network scenario. Applying the claims as drafted, Cisco concedes infringement: "If the court meant, consistent with its findings elsewhere, that Cisco's products block a computer [*i.e.*, in a "first network"] from accessing sensitive data in a protected network [*i.e.*, a "second network"], but allow that computer to access unsensitive data in a different network [*i.e.*, "a third network"], then [that] statement is accurate . . . ." Br. 49; Appx3428-3429 (Cisco's expert admitting same).

4. Centripetal Took Consistent Infringement and Validity Positions

Centripetal has not advanced inconsistent infringement and validity positions, as Cisco incorrectly contends. Br. 50-51. Cisco's IPR petition was denied because no operator was disclosed in its "Sourcefire" system. Appx4021; Appx5684. Centripetal's Preliminary Response highlights this omission in the prior art. Appx5680-5682 (patent teaches "detecting communications" and "using an operator," which Sourcefire does not disclose). Centripetal's arguments that Switches and Routers now practice the claimed process are consistent with distinguishing this prior art because the Switches and Routers do apply "an operator." Moreover, Centripetal's statements were not limited to Claims 18 and 19; they also addressed Claims 11 and 15, which—as mentioned above—recite additional limitations regarding PUT and GET methods. In any event, Cisco no longer challenges the validity of the patent.

B. Cisco Infringes Claims 9 and 17 of the '806 Patent

After learning about Centripetal's patented solution for swapping rules without dropping packets, Cisco adopted it in Switches, Routers and Firewalls. *See* Appx146-148; Appx1596; Appx5254-5256 ("Hitless ACL" in Switches and Routers); Appx5257-5260 ("Transactional Commit Model" in Firewalls). Cisco does not dispute that it preprocesses rules to perform swaps without dropping packets. Appx143-144; Appx5410-5413 (avoiding packet drops by "continuing to

use the old rules until the new rules are compiled and ready for use"); Appx5375-5377; Appx5256 ("no packets should drop"). The court found that Cisco's non-infringement arguments amounted to a "tangled web," noting "a number of factual conflicts in its presentation of evidence." Appx67. It found Cisco's expert Dr. Reddy, in particular, did "not accurately portray the current functionality of the accused products" and Cisco's own fact testimony and documents contradicted his opinions. Appx67; Appx150.

1. The Infringing Systems Cache and Cease Processing Packets "Responsive to Being Signaled to Process Packets in Accordance with the Second Rule Set"

On appeal, Cisco admits, as it must, that its infringing systems cache packets and cease processing them during rule swaps. Br. 26. Cisco now presents a narrow argument: because its devices cache and "cease processing packets during their normal packet processing operation," those operations somehow cannot be "responsive to being signaled" when swapping rule sets, as claimed. *Id*. Cisco even contends that the court "identified no evidence" that the infringing systems cache and cease processing packets "responsive to being signaled." Br. 24.

To the contrary, the court relied on Cisco engineer Peter Jones's testimony that Cisco's products cease processing packets ***in response to a signal*** for the second rule set (Appx152-153) and quoted his cross-examination on this issue at length. Appx253-254. As Mr. Jones admitted, "***a signal is sent to the processor*** to

stop processing packets with the old rule set and to start processing packets with the new rule set," and during a two- to four-clock cycle idle period "when there's no processing of packets, the rules are swapped." Appx254 (emphasis added); Appx3577-3579.

Further, the record supports the court's finding that Cisco's products cache packets in response to being signaled, as required by the claims. Centripetal's expert described how Cisco's infringing systems signal their processors to process packets in accordance with a second rule set, and ***in response to that initial signal***, packets are both cached and not processed. Appx1616-1618 (describing signal); Appx1619-1622 (describing "cease and cache"); Appx1633-1634 (summarizing engineer testimony); Appx1635-1640 (walking through source code and summarizing).

That the "cache and cease" operation also occurs during normal packet processing (Appx152) is no defense to infringement. Cisco specifically designed the infringing systems to signal the processor to stop processing packets with the old rule set, cache the packets and swap the rules. *See*, *e.g.*, Appx5254-5256; Appx5257-5260 (Firewall update stating "new rules will not take effect until compilation is done and stable" and a "reasonable amount of delay" is acceptable). The infringing systems control the processing of packets. They only swap rules in

response to an appropriate signal, and only after caching packets and ceasing processing, even if just momentarily. Appx1638.

2. The District Court Correctly and Specifically Found that Cisco's Firewalls Infringe the '806 Patent

Cisco's attempt to distinguish between Switches, Routers and Firewalls is a red herring. *See* Br. 24-25, n.7. Cisco's expert addressed them jointly, testifying that although "they all implement a different set of updates" with different names, "all of them work in a similar fashion." Appx3636-3637; *see also* Appx3617. Centripetal's expert likewise testified that Firewalls operate in a similar manner to Switches and Routers. Appx1647; Appx1680-1681.

Cisco nonetheless makes one Firewall-specific argument, contending that Firewalls do not "cease" processing packets at all. Br. 25. Centripetal's expert testified that Firewalls "have to cease" processing packets because it is undisputed that rule swaps occur between packets, and—even on a computer—nothing happens "instantaneously." Appx1705-1707; Appx1712 (describing cache used with Firewall); Appx1685; Appx1688-1693.

Cisco cites witness testimony about the Adaptive Security Device Manager, which is not accused of infringement. Br. 25; Appx3521; Appx150. The court asked this witness about packet processing, noting that "[t]here's got to be some kind of gap, however short it is," and eventually forcing a concession that some amount of time elapses between the processing of packets. Appx3526-3528.

C. Cisco Infringes Claims 11 and 21 of the '176 Patent

The claimed "correlation" invention of the '176 Patent: 1) "generate[s] . . . log entries corresponding . . . to packets received by" and "transmitted by the network device," 2) uses those logs to "correlate" the transmitted and received packets, and 3) uses the results to "generate" and "provision" appropriate network rules. Appx309-310. Cisco implemented infringing correlation technology in Switches and Routers with Stealthwatch.

Specifically, Switches and Routers generate ingress and egress NetFlow logs (or telemetry) of received and transmitted packets. Appx113; Appx5218-5220. They then send these records to Stealthwatch, where its artificial engine, called CTA, correlates them with each other. Appx113-114; Appx121; Appx248. Using these correlations, the system identifies abnormal traffic patterns in the network to detect threats. Appx114; Appx5150 ("Stealthwatch can collect NetFlow telemetry from network devices to analyze it for anomaly and threat detection.").

1. Cisco's Stealthwatch Performs the Claimed Correlation of Packets Using NetFlow Records

Cisco contends that Stealthwatch correlates NetFlow logs ***only*** with external global threat indicators, and not with other NetFlow logs from the internal network. Br. 37-39. The evidence contradicts that argument. Centripetal's expert testified that, having reviewed all the evidence, "NetFlow data is also correlated among

itself." Appx2109-2110; Appx2117 (testifying that "correlation can be performed just of the NetFlow data," including "the ingress and egress data").

As the court explained, Stealthwatch is not limited to using global threat indicators for correlation. It also "correlate[s] NetFlow within the network between multiple devices in order to recognize normal traffic patterns." Appx120-121 (citing Appx5148-5150). The court also referenced a Stealthwatch document explaining the system "will correlate flows from multiple devices and perform stitching and de-duplication action to provide a single bidirectional flow of the traffic end-to-end." Appx248. Likewise, the '176 Patent describes the need for correlating packets to track "flows of associated packets" communicated between network devices, which may be obfuscated by devices within the network. Appx301 (1:16-25). Cisco's engineer, Mr. Llewallyn, confirmed that Stealthwatch collects and correlates NetFlow records from multiple Switches and Routers within a network. Appx3152.

Cisco's Stealthwatch does not require both ingress and egress NetFlow logs from the same device to perform correlation. Stealthwatch can utilize ingress reports from multiple devices to correlate all of the packets transmitted and received by each individual device. *See* Appx5152 (Cisco's system "usually only needs ingress export from all interfaces on the exporter to create interface traffic data for inbound and outbound traffic"). This is possible because logs

corresponding to packets received by one device also correspond to packets transmitted by other devices. Correlating all of these logs necessarily results in the correlation of NetFlow logs corresponding to packets received by a network device with NetFlow logs corresponding to packets transmitted from that device, as claimed in the '176 Patent. Appx5219 ("NetFlow is a standard that defines data elements exported by network devices that describe the 'conversations' on the network.").

Nor do the claims require both "egress and ingress log entries," as Cisco contends. Br. 43. The claims require correlating packets based on "log entries corresponding to" packets transmitted and received by a network device, regardless of what the logs are called and which device(s) generated them.[2] As noted above, Stealthwatch correlates packets using NetFlow logs corresponding to packets transmitted and received by a given network device.

2. The '176 Patent Is Not Limited to a Single Network Device

Cisco appears to argue that the claims require correlating packets using log entries generated by a ***single*** device. Br. 43. As discussed above, the claims include no such limitation. Cisco's own expert admitted that the claimed device "could be more than one network device." Appx3282; *see also Baldwin Graphic*

[2] The court understood this distinction, stating that "the Cisco system correlates logs between multiple devices within the network on either ingress or egress." Appx118.

Sys., Inc. v. Siebert, Inc., 512 F.3d 1338, 1342-43 (Fed. Cir. 2008) ("a" means "one or more"). Cisco fails to address this admission, which the court justifiably relied upon as consistent with the teaching of the '176 Patent. Appx117-118 (quoting Appx304 (8:46-63) (correlation of packets transmitted and received "by network device(s)")); Appx262-263 (quoting Appx301 (2:58-63) ("Network device(s). . . may include one or more devices . . . .")). Cisco argues that Centripetal's expert limited his infringement theories to a single switch or router (Br. 43), but the court found that "Dr. Cole's cross examination testimony does not support Cisco's claim; indeed it may suggest exactly the opposite." Appx262; *see also* Appx2102 (infringement of "the entire system").

Although the claims are not limited to a single device, the court also found that a single Cisco network device can export both ingress and egress NetFlow. Appx116-117 ("accused switches and routers do identify and generate logs on ingress and egress"). Cisco technical documents support this finding, noting a Switch is capable of "384,000 Netflow entries . . . 192,000 ingress and 192,000 egress." Appx5220. Cisco's engineer confirmed (Appx3173), as did Cisco's expert while arguing an error condition would result when transmitted to Stealthwatch. Appx3290. As the court noted, however, Cisco's expert relied solely on source code from a previous version of Stealthwatch not accused of infringement. Appx116 (citing Appx3291).

3. The District Court Did Not Create New Infringement Theories

Nothing supports Cisco's assertion that the court "sua sponte" found infringement. Br. 41-43. The so-called "multiple-device theory" was endorsed by Cisco's own expert (Appx3282), so Cisco cannot credibly claim prejudice. As for the court's discussion of WebFlow/Syslog data, Cisco's specific concern is unclear, as the court's infringement findings should be affirmed based solely on the Netflow data. *See* Appx113-114. Nor do Cisco's systems require the use of such data (Appx5222), as Centripetal's expert confirmed. Appx2115-2118 ("correlation can be performed just of the NetFlow data," specifically "ingress and egress data"). Furthermore, Cisco cross-examined Centripetal's expert about WebFlow/Syslog. Appx2110 (testifying that Cisco's system "not only correlates the WebFlow and the NetFlow, but also the NetFlow data is also correlated among itself"). As Dr. Cole testified, Stealthwatch is "already performing correlation of NetFlow, and then it's using this information to perform some additional analysis." Appx2117.

D. Cisco Infringes Claims 24 and 25 of the '856 Patent

When hackers send malicious files through networks, they are broken into thousands or even millions of pieces, which are encrypted and transmitted in separate packets (collectively called a "packet flow"), all of which need to be decrypted and reassembled to access the file. Appx55-57; Appx1103-1106. The '856 Patent monitors encrypted traffic without decrypting the packets. The

claimed invention requires, among other things: 1) determining which packets "correspond[] to one or more network-threat indicators" based on the unencrypted information in otherwise encrypted packets; 2) filtering those packets; and 3) "rout[ing] . . . the filtered packets." Appx357-358.

Upon learning about Centripetal's patented technology, Cisco implemented it in ETA. As the court correctly found, Switches and Routers send NetFlow data to Stealthwatch, including information from the unencrypted portions of encrypted packets; Stealthwatch and ETA determine which packet flows correspond to threats; and Stealthwatch sends the results to ISE, which provisions rules to Switches and Routers to filter the relevant packets and route them to a proxy system, known as a null interface. Appx75-80; Appx1910-1912; Appx5195-5198.

Cisco's arguments hinge on the misleading premise that its products cannot filter or re-route packets because only NetFlow data—and not packets themselves—are sent to Stealthwatch. *See* Br. 28-31. The claims only require making a determination "based on a portion of the unencrypted data" of the packets identified as encrypted (Appx358 (29:3-7)), and Cisco's documents demonstrate that Stealthwatch analyzes several categories of such unencrypted data from the packets, including an initial data packet and the encryption "handshake," among others. Appx76-77; Appx5142-5143. That the packets themselves are not sent to Stealthwatch is not relevant to infringement.

Cisco contends that Stealthwatch itself cannot filter packets, but Centripetal's expert clarified that "the entirety of this system, the routers and switches, the StealthWatch and the Identity Service Engine" filters packets. Appx2120. He explained that once Stealthwatch identified a threat, "it would communicate with [ISE], it would then have the [Switches or Routers] send the additional packets as part of that session to that proxy, the null interface, and then that would contain or control the damage that was being caused by that session." Appx2120; Appx1910-1912; Appx5195-5198; Appx2124. It is undisputed that this process prevents packets from reaching their destination.

Cisco further argues that individual packets used to generate NetFlow data may reach their destination before filtering can begin, and thus the packets determined to correspond to network-threat indicators by Stealthwatch and ETA are not the same as those filtered or routed to the proxy system. Br. 32-36. But as Cisco's expert explained, malware threats in encrypted network traffic require an ***entire*** packet flow (*i.e.*, thousands or even millions of packets) to reach its destination for reassembly. Appx1103-1106. Stealthwatch and ETA analyze unencrypted information from individual packets to make a determination about that entire packet flow, and—according to a Cisco white paper quoted by the court—"[u]pon discovery, ***a malicious encrypted flow can be blocked or quarantined*** by Stealthwatch." Appx5176-5178 (emphasis added); Appx99.

Cisco's products make a determination based on unencrypted data from the encrypted packet flow—the same packet flow as the filtered and routed packets. And as a practical matter, even if some of the initial packets arrive at their destination, blocking the flow prevents those packets from being reassembled into a malicious file. *See* Appx2065-2066. For infringement, however, the packets in the packet flow are the claimed "packets comprising encrypted data" (Appx358 (29:2)) and packets within the packet flow are both used in the "determining" step and filtered and re-routed, as claimed.

Despite its statement that "a malicious encrypted flow can be blocked or quarantined," Cisco argues that ETA provides only an "after-the-fact" system that merely analyzes historical network activity. Br. 29-30; Appx5178. The court rightly found this argument not credible, citing Cisco's failure to cite any technical documents regarding accused versions of its products and the contradictions between Cisco's witness testimony and its documents. Appx87; *see also* Appx94 (Cisco's expert "solely" "limit[ed] his testimony to the forensic after the fact analysis feature in the old pre-2017 Stealthwatch.").

The court cited Cisco documents[3] that contradict its "after-the-fact" argument, confirming that the accused systems:

[3] While these documents are not solely marketing materials (Br. 35-56), "there is no prohibition" against using such admissions. *PharmaStem Therapeutics, Inc. v. ViaCell, Inc.*, 491 F.3d 1342, 1351 (Fed. Cir. 2007). Unlike this litigation, the

- "[c]atch them in the act" and "detect and respond to threats in real time," (Appx5112-5113) (Stealthwatch data sheet);
- work "proactively with threat detection," (Appx5190-5191) (Stealthwatch document);
- provide "[r]eal-time detection of attacks by immediately detecting malicious connections," (Appx5081-5082) (Stealthwatch document);
- "[d]etect and stop threat[s]," (Appx5397-5398) (internal technical presentation regarding Switches); and
- "[d]etect and stop threats, even with encrypted traffic," (Appx5062) (Switch document).

Appx90-94.

Despite the court dedicating pages of analysis to this evidence (Appx84-94), Cisco fails to explain the clear conflict between these documents and its non-infringement theory. And how could it? Apart from asking this Court to believe that Cisco fundamentally misled its customers, how can Cisco reconcile its white paper claim that "[u]pon discovery, a malicious encrypted flow can be blocked or quarantined by Stealthwatch" (Appx5176-5178), with its engineer's testimony that it would not be "physically possible to block those packets" (Appx3210)? Or Cisco's data sheet claim that Stealthwatch will catch cyber criminals "in the act" by detecting and responding to threats "in real time" (Appx5112-5113), with its

---

cases Cisco cited involve undisputed features. *MAG Aero. Indus., Inc. v. B/E Aerospace, Inc.*, 816 F.3d 1374, 1377 (Fed. Cir. 2016) (undisputed "typo"); *Regents of Univ. of Minn. v. AGA Med. Corp.,* 717 F.3d 929, 939 (Fed. Cir. 2013) (undisputed feature described differently in sales literature).

expert's testimony that the accused products "[d]on't block malware before it infects the host" (Appx2926)?

IV. THERE WAS NO ABUSE OF DISCRETION OR CLEAR ERROR IN THE DISTRICT COURT'S DAMAGES ANALYSIS

A. The District Court Properly Considered the Only Comparable License

The court conducted a thorough *Georgia-Pacific* analysis, employing a comparative-license approach based on the 2018 Keysight/Centripetal agreement, Centripetal's sole license to its patents and the only license agreement in evidence. Appx171-175; Appx234, n.2; Appx5245-5246. This comparable license covered the four patents Cisco infringes, was close in time to Centripetal's 2017 hypothetical negotiation with Cisco, and like here, was license details. Appx2492-2493 (comparing Keysight agreement to hypothetical negotiation); Appx2211-2212, Appx2248-2249, Appx2334-2335 and Appx2489 (evidence of competition). Keysight agreed to pay Centripetal a 10% royalty on the license details product revenues of competing products and 5% on the license details product revenues of noncompeting products. Appx5245.

Based on evidence that Cisco's software and Firewalls directly compete with Centripetal, and because Cisco's embedded "patented software functionality" in Switches and Routers provide the same functionality as [Centripetal's] RuleGATE product," the court correctly found that they "are more comparable to the 10%

royalty on competing products . . . in Keysight." Appx172; Appx2493; Appx2502-2503. Mr. Gunderson's testimony supports this finding. Appx2562-2563.

The court duly accounted for the fact that this license was a settlement agreement. Appx172-173. It further used the "*Georgia-Pacific* factors to account for the similarities and differences in the Keysight license and the facts present in this case." Appx173, Appx171 (citing Appx2488-2494) (testimony comparing hypothetical negotiation to Keysight license).

Cisco contends there is a categorical rule against using settlement licenses for patent damages, relying on the 132-year-old case *Rude v. Westcott*, 130 U.S. 152 (1889). Br. 56. But "the language of patent-damages law and the language of evidence law . . . have changed significantly since *Rude*," *Prism Technologies LLC v. Sprint Spectrum L.P.*, 849 F.3d 1360, 1372 (Fed. Cir. 2017), and there is no per se rule against using settlement agreements. *Id.*; *Elbit Sys. Land & C4I Ltd. v. Hughes Network Sys., LLC*, 927 F.3d 1292, 1299-1300 (Fed. Cir. 2019) (affirming damages award based on litigation settlement). As Centripetal's damages expert explained, the litigation circumstances where license details was license details (Br. 56) are comparable to the assumption of validity and infringement in the hypothetical negotiation. Appx2485-2486; Appx2490-2493.

Cisco also takes issue with the fact that the Keysight license covers license details patents, whereas the hypothetical negotiation covers four. Br. 56-57. But

Centripetal's litigation with Keysight involved five patents, including the '856 Patent and patents "in the same patent family and cover[ing] similar fields" as the '176, '193 and '806 Patents. Appx171. In any event, the court accounted for this difference (Appx173), which does not render the Keysight agreement per se non-comparable. *Vectura Ltd. v. GlaxoSmithKline LLC*, 981 F.3d 1030, 1040-41 (Fed. Cir. 2020) (affirming damages award for infringement of single patent based on comparable license to 400 patents).

B. There Is No Clear Error or Abuse of Discretion in the District Court's Apportionment

1. Further Apportionment Was Not Required

As a threshold matter, the court was under no legal obligation to reduce the base of Cisco's revenues in its damages calculation (although it did so in any event). The comparable Keysight license applies the specified rates to license details revenues of licensed products. Appx5245-5246; Appx2567. "[W]hen a sufficiently comparable license is used as the basis for determining the appropriate royalty, further apportionment may not necessarily be required," because in such circumstances, apportionment is "built-in." *Vectura Ltd.*, 981 F.3d at 1040. In *Vectura*, this Court affirmed a reasonable royalty of 3% applied to total (unapportioned) infringing revenues, holding that apportionment was "built-in" through the use of a comparable license that likewise applied a royalty rate to an unapportioned revenue base. *Id.*; *Elbit Sys.*, 927 F.3d at 1301 (affirming damages

award with built-in apportionment). Such is the case here, given the close comparability of the Keysight agreement, which applied the specified royalty rates to the [redacted] revenue base.

Comparing the Keysight license to the court's reasonable royalty award shows that the court's award can be calculated as approximately 3.3% of Cisco's unapportioned revenues—roughly a third of the 10% rate in the Keysight license. Appx2567 (Centripetal's expert comparing a 10% royalty on Cisco's apportioned revenues to the Keysight royalty on an apples-to-apples basis). Thus, if the base here is [redacted] as it was in the Keysight license, the court's rate fully accounts for the differences the court found between the Keysight agreement and the hypothetical license. Because further apportionment—and specifically, apportionment of the revenue base—was not required, Cisco's arguments regarding Dr. Striegel's analysis provide no basis for disturbing the judgment.

2. The District Court's Apportionment Analysis Was Not an Abuse of Discretion

As a conservative measure, the Court appropriately apportioned the revenues based on credible expert testimony. The court did not abuse its discretion in applying Dr. Striegel's technical apportionment, approved of in *Finjan, Inc. v. Blue Coat Systems, Inc.*, 879 F.3d 1299, 1313 (Fed. Cir. 2018). Dr. Striegel, a computer

scientist who was not offering any "economic analysis"[4] (Br. 55), first reviewed Cisco's technical documents, depositions, source code and discussed infringement with Centripetal's other technical experts. Appx188; Appx2340-2341. He then identified each product's top-level functions of equal technical value ("functions") based on this technical information and used technical data sheets and product overviews to guide his testimony of these "core" functions. Appx2341-2342; Appx2430-2432. He distilled Cisco's complex technology into generally-named functions (Br. 52) and used some terms that did not appear in these documents, such as "commodity components." Appx188; Appx2348; Appx2431.

Like the technical expert in *Blue Coat*, Dr. Striegel separated infringing and non-infringing functions[5] on a patent-by-patent and product-by-product basis for apportionment. Appx2378-2379, Appx2404-2405; Appx5546; *see* Appx2352. For example, he excluded non-infringing, commodity-type functions, such as life-cycle management, ports, power supplies, cables, maintenance and operating systems. Appx2379, Appx2410, Appx2433.

[4] Cisco misleadingly excerpts Dr. Striegel's testimony (Br. 52), omitting that he did not identify incremental value "from an economic perspective." Appx2406.

[5] Contrary to Cisco's argument (Br. 55, n.13), the court cited *Ericsson, Inc. v. D-Link Systems, Inc.*, 773 F.3d 1201 (Fed. Cir. 2014), for its holding that reliable and tangible evidence supports apportionment between patented and unpatented features. Appx185-186; Appx189.

The court apportioned the revenues ***and*** found apportionment warranted a downward influence on the rate in its *Georgia-Pacific* analysis. Appx175. It carefully tied the royalty to "the incremental value that the patented invention adds" through base and rate, and did not accept Dr. Striegel's analysis "in full." Br. 51, 54; *Exmark Mfg. Co. v. Briggs & Stratton Power Prods. Grp., LLC*, 879 F.3d 1332, 1348 (Fed. Cir. 2018).

3. Dr. Striegel Based His Apportionment on Significant Improvements to Network Security, as Claimed in the Patents

Cisco argues that Dr. Striegel should have removed from his apportionment what existed previously, like processors, unless there was a "patented improvement" to it. Br. 53-54. But it is "improper to assume" that use of "a conventional element [in an invention] cannot be rendered more valuable" as all inventions use "earlier knowledge." *AstraZeneca AB v. Apotex Corp.*, 782 F.3d 1324, 1338 (Fed. Cir. 2015); *see also* Appx2383-2384 (denying *Daubert* challenge to Dr. Striegel and observing that old functions can be improved). Dr. Striegel explained the importance of Cisco's specific processors, for example, "delivering" the patented technology and their role in infringement. Appx2418-2419.

Moreover, Dr. Striegel focused on the patent claims, determining that they were a "considerable improvement in technology" and "an altogether new capability" for network security. Appx2416. The court agreed, finding

Centripetal's Patents significantly improved existing technology that Cisco touted in its product offerings. Appx103 ("new advancement"); Appx153 ("greatly improve[d] security functionality"); Appx183 ("significantly improved existing hardware"); Appx180-182 (Cisco's "breakthrough" in security, solving challenges previously thought unsolvable); Appx5247-5248. Thus, Dr. Striegel's opinions reflect the footprint of the inventions as claimed.

4. Dr. Striegel Properly Focused on Core Functions

Cisco criticizes Dr. Striegel's analysis by pointing to allegedly non-infringing sub-features within the top-level functions he identified. Br. 52-53. As Dr. Striegel explained, doing so "misconstru[es]" his analysis (Appx2423-2424), which identified "core" functions, *i.e.*, the essential components of each product as perceived by a network and security expert with an extensive engineering background. Appx2429; Appx2431-2432; Appx2412. As in *Blue Coat*, where the expert relied on the infringer's own documentation to identify top-level functions, 879 F.3d at 1313, Dr. Striegel relied on Cisco documents providing "a representation of what Cisco viewed as being important" and "what Cisco represents to their customers." Appx2417; Appx2419.

Dr. Striegel considered and addressed the functions that Cisco raises on appeal, explaining how they related to Cisco's infringing functionality. Appx2426 and Appx2435 (sandboxing is part of AMP, which receives rules); Appx2435-2436

(ETA's relationship under "Advanced Security"). He also explained why the routing and switching capabilities play a role in infringement. Appx2379-2381. He specifically "considered whether further apportionment would be necessary" and concluded further parsing sub-features would "decrease" the integrity of his analysis, which focused on Cisco's representations of the core product functionality. Appx 2417.

Dr. Striegel's apportionment differs from a second damages methodology rejected in *Blue Coat* (Br. 55), where, unlike here, the expert failed to apportion a single software engine that included multiple non-infringing functions described in the infringer's documents as independently important to customers. *Blue Coat*, 879 F.3d at 1311. Dr. Striegel's approach also differs from the methodology rejected in *Finjan, Inc. v. SonicWall Inc.* (Br. 55), which involved grouping products together and then identifying functions of that product group, without accounting for any significant non-accused functions of individual products. *SonicWall* Order, No. 17-cv-04467, ECF 477 at 17, 19-20 (N.D. Cal. May 21, 2021). Dr. Striegel's more granular analysis here identified functions from each accused product. Appx189-190; Appx2408; Appx5546.

After weighing the evidence, the court found Dr. Striegel credible and accepted his analysis. Appx189-190. By contrast, Cisco's experts provided conclusory testimony disagreeing with Dr. Striegel and claiming that certain

functionality existed in the prior art, which the court did not find credible and did not abuse its discretion by rejecting. Appx66-67; Appx87; Appx180; *see*, *e.g.*, Appx3340-3343; Appx3478; *Blue Coat*, 879 F.3d at 1313 (fact-finder entitled to find patentee's expert more credible than defendant's witness testifying there were "many, many things" behind each top-level function); *Endo Pharms. Inc. v. Actavis LLC*, 922 F.3d 1365, 1374 n.10 (Fed. Cir. 2019) (credibility findings are not disturbed on appeal); *Conoco, Inc. v. Energy & Envtl. Int'l, L.C.*, 460 F.3d 1349, 1362-63 (Fed. Cir. 2006) (trial court has "broad discretion" in determining credibility because it saw the witnesses and heard their testimony).

C. A New Trial on Damages Is Not Required

A new damages trial is only warranted "where the jury rendered a single verdict on damages, without breaking down the damages attributable to each patent." *Verizon Servs. Corp. v. Vonage Holdings Corp.*, 503 F.3d 1295, 1310 (Fed. Cir. 2007); *accord Omega*, 920 F.3d at 1350. Those concerns are irrelevant here. There was no jury trial and no general verdict. The court's detailed apportionment for each patent ***and*** product, as shown below, provides sufficient information to recalculate the royalty base should this Court deem necessary.

Product	Patent	Infringing Functions	Court's Apportionment	Total Revenue
Switches	'193	6/13	31%	$11,839,742,927
	'806	4/13	31%	
	'856	6/13	31%	
	'176	5/13	31%	
ISR	'193	4/9	44%	$2,375,633,299
	'806	4/9	44%	
	'856	4/9	44%	
	'176	4/9	44%	
ASR	'193	2/8	25%	$3,456,557,172
	'806	2/8	25%	
	'856	2/8	25%	
	'176	2/8	25%	
Firepower	'806	7/13	54%	$2,283,221,005
ASA	'806	7/13	54%	$428,380,587
FMC	'806	7/13	54%	$67,635,757
DNA	'806	3/10	30%	$252,855,962
Stealthwatch	'856	4/5	80%	$266,052,460
	'176	4/5	80%	
ISE	'856	5/13	38%	$497,000,709

Appx189-191; Appx5546.[6]

Cisco does not (and cannot) show that the court abused its discretion by awarding a minimum and maximum ongoing royalty "[s]imilar to the Keysight license." Appx208. After declining Centripetal's request for an injunction against competitor Cisco, the court concluded limited future royalties were appropriate because it expected infringement to continue. Appx202; Appx207. Cisco's argument regarding the hypothetical discontinuance of the infringing devices is unsupported. Cisco reported months prior to trial that Switches are the "fastest-selling product ever," "propel[ling] the Company's Finances," (Appx178; Appx5114-5115), and its infringing products generated increased revenues and profits (Appx175-183), achieving the "top IT priority" of Cisco's customers—cybersecurity. Appx5140.

V. THERE IS NO CLEAR ERROR IN THE DISTRICT COURT'S FINDING OF WILLFULNESS OR ABUSE OF DISCRETION IN GRANTING ENHANCED DAMAGES

A. Cisco Stole Centripetal's Patented Technology

Cisco had pre-suit knowledge. Appx198-199. Centripetal gave Cisco "detailed presentations of the patents and their functionality," including numerous demonstrations of its marked RuleGATE product. Appx198-200; Appx192-194.

[6] Although Switches, Routers and Stealthwatch infringed multiple patents, Centripetal only counted their sales once. Appx2503-2504.

Centripetal observed that Cisco "hone[d] in on our filter technology and algorithms" and asked about "our patents." Appx5047. After learning of Centripetal's algorithms and internally stating it should undertake a "study [of Centripetal's] patent claims," "Cisco released products with Centripetal's functionality." Appx5055; Appx200.

"[T]he [court] was free to decide whose evidence it found more compelling on the question of willfulness and found in [Centripetal's] favor." *Georgetown Rail Equip. Co. v. Holland L.P.*, 867 F.3d 1229, 1245 (Fed. Cir. 2017). Cisco cites nothing to support its bare assertion that it is "legal error" to consider willfulness in the context of the *Read* factors. *Read Corp. v. Portec, Inc.*, 970 F.2d 816, 826-27 (Fed. Cir. 1992). Nothing in the court's decision suggests that it decided willfulness based on the closeness of the case, Cisco's size or its trial presentation—each of which expressly supported enhanced damages, not willfulness. Appx201-203.

B. Numerous Undisputed Factual Findings Support Enhancing Damages

Cisco makes no attempt to show that the court abused its discretion in enhancing damages after considering the *Read* factors based on Cisco's:

- failure to present evidence of investigating and forming a good faith belief of invalidity or non-infringement (Appx200);
- litigation conduct (including shielding Cisco engineers and executives "from answering to their own writings and statements") (Appx200-201);

- "immense size and commercial success with the infringing products" (Appx201-202);
- duration of misconduct and lack of remedial action (Appx202-203); and
- attempt to conceal its misconduct by "continually gather[ing] information from Centripetal as if it intended to buy the technology from Centripetal" to create infringing products (*id.*).

Cisco's incorporation of the patented technology "resulted in a dramatic increase in sales which Cisco touted in both technical and marketing documents." Appx203.

These findings are sufficient to sustain enhanced damages, even without a finding of copying or a close case. *SRI Int'l, Inc. v. Advanced Tech. Labs., Inc.*, 127 F.3d 1462, 1469 (Fed. Cir. 1997) (no *Read* factor required).

1. The District Court Correctly Found That Cisco Copied the Infringing Technologies

The court made numerous findings that Cisco copied Centripetal's patented technology. Appx200; Appx203 (Cisco "appropriated the information gained in these meetings . . . about Centripetal's patented functionality" and "embedded the copied [patented] software functionality" into Switches, Routers and Firewalls); *see also* Appx224; Appx268. Cisco's release of the infringing systems within a year was compelling evidence of copying. Appx199-200.

Centripetal's technical disclosures went well beyond purported "unclaimed" aspects of its RuleGATE product, "such as the ability to process millions of rules." Br. 59. The court found that Centripetal disclosed core patented algorithms to Cisco beginning in February 2016 (Appx193; Appx2222-2224; Appx5127-

5129) and showed Cisco how its patented technology worked, which Cisco described as "a pretty cool new approach to leveraging threat data." Appx192-193; Appx2303-2305; Appx5124. It also found that Centripetal assisted in preparing a subsequent presentation made to Cisco that "detailed the core RuleGATE functionalities covered by the Asserted Patents." Appx193-194; Appx2237; Appx2239-2240; Appx2244-2245; Appx5816-5818.

Thus, Cisco incorrectly claims that the court "made no finding about what" Cisco copied and its argument that embodiments of the claims must be copied is based upon inapposite law addressing secondary considerations of nonobviousness. Br. 59 (citing *Amazon.com, Inc. v. Barnesandnoble.com, Inc.*, 239 F.3d 1343, 1366 (Fed. Cir. 2001)).

Cisco urges this Court to accept Mr. McGrew's claim to have invented ETA, which the court implicitly rejected. *Romero by Romero v. United States*, No. 92-2617, 1993 WL 306114, at *4 (4th Cir. Aug. 11, 1993) (court need not "make findings on all facts presented," nor must it make findings "asserting the negative of each issue of fact raised"). But Mr. McGrew "did not directly contribute software to any of the products" and could not confirm whether his software was implemented into any products. Appx2784-2785. Further, he testified that Cisco senior management's description of ETA in Cisco's "network of the future" press release (Appx5104) "is wrong." Appx2790.

2. The District Court Detailed Why the Case Was Not Close and Supports Enhanced Damages

Cisco waived its argument that the court "failed to explain why its decisions were 'not a close call'" (Br. 62) by not raising it to the court. *See Consolidated Aluminum Corp. v. Foseco Int'l Ltd.*, 910 F.2d 804, 814 n.9 (Fed. Cir. 1990).

The court explained why the case was not close. It found Cisco's demonstratives and expert testimony in direct conflict with Cisco's witness testimony and its technical documents. Appx202; Appx229 (demonstratives "misrepresented the functionality of the infringing technology"); *see also* Appx85-94, Appx98 and Appx150-151 (Cisco's technical documents and engineer testimony refuted Cisco's non-infringement expert on the '856 Patent); Appx180. Cisco's expert testimony regarding the '806 Patent was just one example of how "Cisco's retained experts often contradicted Cisco's own documents as well as Cisco's own engineers." Appx67-72 (noting this "common thread weaved a very tangled web"). Even Cisco's non-infringement expert for the '193 Patent confirmed that Switches and Routers "perform all the functionality required to infringe" when confronted with Cisco's documents. Appx137. Further, the court found that Cisco "avoided calling the authors of its technical documents" as witnesses.[7] Appx200-202.

[7] Where appropriate, the court addressed Cisco's fact witness testimony that Cisco identified. Br. 63; *see, e.g.*, Appx94; Appx153; Appx250.

Cisco likewise ignores the court's findings that Cisco's defenses were objectively unreasonable because, *inter alia*, Cisco's:

- "non-infringement case was grounded upon [Cisco's unaccused] old technology" and contradicted its invalidity evidence (Appx203); and
- damages theory "lacked any precedential or evidentiary support . . . and was completely devoid of economic reality" and "damages evidence was deeply flawed" and "unrealistic." (Appx227; Appx203-204).

These findings and the determination that "Cisco's independent experts [were] unpersuasive and in many instances not credible" "result[ed] in a finding that Cisco's defenses were objectively unreasonable." Appx229; *SRI Int'l, Inc., v. Cisco Sys., Inc*., 14 F.4th 1323, 1328-29 (Fed. Cir. 2021) (evidence that Cisco's defenses were unreasonable—including that Cisco misrepresented how its accused products work, as shown by "Cisco's own technical witness"—supported a finding of willful infringement and enhanced damages).

Cisco ignores the court's finding that Cisco's accused products contained ***different*** technology from its previous products. Appx66-67; Appx104; Appx124-125; Appx140; Appx155-156. Cisco's assertion that the court erred in concluding that this defense was objectively unreasonable "is not a basis for concluding that the [court] abused its discretion in enhancing damages." *WBIP, LLC v. Kohler Co*., 829 F.3d 1317, 1341 (Fed. Cir. 2016).

In determining the closeness of the case, the court accounted for the fact that it found a fifth patent not infringed by reducing the multiplier. Appx204. Cisco argues that the court should have given more weight to the PTAB proceedings, but "[t]he trial judge is in the best position to weigh considerations such as the closeness of the case." *Amsted Indus. v. Buckeye Steel Castings Co.*, 24 F.3d 178, 184 (Fed. Cir. 1994) (affirming treble damages award and declining to reweigh *Read* factors based on allegation that court "failed to consider mitigating factors").

Cisco relies heavily on *Polara Engineering, Inc. v. Campbell Co.*, which is inapposite because that court concluded without explanation that the "close call" factor was neutral, despite having "failed to even mention" a key defense. 894 F.3d 1339, 1355 (Fed. Cir. 2018). Here, the court "made detailed factual findings" as to why the close call factor supported enhancement, including the impact of its credibility determinations. *See Georgetown Rail*, 867 F.3d at 1245-46 (affirming enhancement); *SRI Int'l*, 14 F.4th at 1330-31 (affirming enhanced damages where court "appropriately considered" the *Read* factors, including Cisco's "behavior as a party to the litigation," its "size and financial condition," its "motivation for harm," and the "closeness of the case").

VI. RECUSAL WAS NOT WARRANTED AND JUDGE MORGAN DID NOT ABUSE HIS DISCRETION

After presiding over a nearly six-week bench trial, spending months working and preparing "a full draft of [the court's] opinion" with "virtually every issue

decided," Judge Morgan learned while preparing annual financial disclosures that his wife had purchased Cisco stock worth less than $4,700, which "did not and could not have influenced [his] opinion on any of the issues in this case" given the timing. Appx30-31. He immediately notified the parties and his wife promptly divested her shares into a blind trust, eliminating any potential conflict, before he filed his opinion. Appx30.

Divestiture under "Section 455(f) was incorporated for exactly [this] type of situation[] where the Court discovers an interest after substantial time and resources have been devoted to the case." Appx42. No apposite authority supports Cisco's claim that Judge Morgan abused his discretion; vacatur under these circumstances is completely unwarranted.

A. Divestment into a Blind Trust under § 455(f) Cured Any Potential Conflict

Judge Morgan cured any potential conflict under 28 U.S.C. § 455(b) before he filed his already-drafted opinion when his wife divested her Cisco shares into a blind trust. Appx42-43. A blind trust is a valid divestment mechanism under § 455(f). *See, e.g.*, Marianne M. Jennings & Nim Razook, *Duck When a Conflict of Interest Blinds You: Judicial Conflicts of Interest in the Matters of Scalia and Ginsburg*, 39 U.S.F. L. Rev. 873, 904 (2005) ("A judge . . . can sell stocks or place them in a blind trust so that she can rule in cases involving the stock issuers without the existence or even appearance of a conflict of interest.").

Cisco cites no authority holding that a blind trust is inadequate ***under § 455(f)***. Cisco relies primarily on a non-binding advisory opinion of the Judicial Conference Committee on Codes of Conduct, which "is not authorized to interpret the statute" containing § 455. Jud. Conf. of U.S. Comm. on Codes of Conduct, Advisory Op. No. 20 (June 2009). And that opinion states only that blind trusts do not comply with the duty to "keep informed about financial interests" (under ***§ 455(c)***), saying nothing about a blind trust's sufficiency as a form of divestment under § 455(f). *Id.*, Advisory Op. No. 110 (Aug. 2013). The dictum from another circuit in *In re Cement Antitrust Litigation*, 688 F.2d 1297, 1314 n.18 (9th Cir. 1982), likewise states only that blind trusts cannot be used to evade § 455(c)'s keep-informed requirement; it predates and therefore says nothing about § 455(f). In fact, Congress added the divestiture provision of § 455(f) for the express purpose of abrogating *In re Cement.* H.R. Rep. No. 100-889, 100th Cong., § 2, at 68-69 (1988), *reprinted in* 1988 U.S.C.C.A.N. 5982, 6029-30.

Finally, the use of a blind trust cannot violate § 455(c). Br. 65-66. Judge Morgan was already "informed" of the Cisco stock prior to divesting it into a blind trust, which is what § 455(c) requires. Further, a blind trust was appropriate under the circumstances because "an outright sale of the stock would undermine the purpose of section 455" and "may be seen to benefit the Court" after issuing a decision "in Centripetal's favor." Appx42.

B. Vacatur Is Entirely Unwarranted

Judge Morgan's prompt disclosure and divestiture of his wife's *de minimis* interest in Cisco eliminated any basis for recusal. To the extent this Court finds any error in his approach (there was none), it would not justify the extreme remedy of vacatur, which is improper where a violation is "neither egregious nor clear cut." *United States v. Cerceda*, 172 F.3d 806, 815-16 (11th Cir. 1999) (explaining that vacatur in a close case would "increase[] rather than decrease that risk" of the public "los[ing] faith in the judicial system").

As Judge Morgan explained, the facts in *Liljeberg*, *Shell* and *Chase* bear no resemblance to this case because he did not learn of the issue until after he had decided the case, promptly and candidly disclosed it to the parties, and took good-faith steps to cure any conflict. Appx30, Appx36-38; *see Liljeberg v. Health Servs. Acquisition Corp.*, 486 U.S. 847, 855-56 (1988) (trustee of university at center of litigation); *Shell Oil Co. v. United States*, 672 F.3d 1283, 1286 (Fed. Cir. 2012) (over $250,000 of stock in prevailing party); *Chase Manhattan Bank v. Affiliated FM Ins. Co*, 343 F.3d 120, 127 (2d Cir. 2003) (no effort to divest).

Cisco makes no effort to show that vacatur is warranted under the three factors set forth in *Liljeberg*, 486 U.S. at 848. *See Polaroid Corp. v. Eastman Kodak Co.*, 867 F.2d 1415, 1420-21 (Fed. Cir. 1989). Not one is met. First, affirmance is not unjust to Cisco. Cisco "ultimately was able to fully and fairly

present its case before an impartial judge," *CEATS, Inc. v. Continental Airlines, Inc.*, 755 F.3d 1356, 1366 (Fed. Cir. 2014), as the court decided the case before learning of his wife's interest—well after the 22-day trial. Appx30. Furthermore, his wife's ownership interest was in Cisco, not Centripetal.

Second, affirmance will not produce injustice in other cases because the judge's denial of Cisco's motion "rest[ed] on the specific facts of this case." *Polaroid*, 867 F.2d at 1420.

Third, public confidence in the judicial process will not be undermined. To the contrary, "the public would lose confidence in the judicial process . . . because the parties and the courts would be forced to relitigate the case even though the proceedings leading to those judgments seemed completely fair." *Cerceda*, 172 F.3d at 816; *see also Polaroid*, 867 F.2d at 1420. Further, Judge Morgan's decision to utilize a blind trust "promote[s] public confidence in the integrity of the judicial process," *Kolon Industries Inc. v. E.I. DuPont de Nemours & Co.*, 748 F.3d 160, 169 (4th Cir. 2014), because the public could perceive selling the stock as "using inside information to potentially profit [his] wife's account." Appx18593; Appx42.

Vacatur under these circumstances would weaponize § 455 into an opportunistic tactic "to avoid the consequences of [a judge's] expected adverse decision." H.R. Rep. No. 93-1453, 93d Cong. § 2 (1974), *reprinted in* 1974

U.S.C.C.A.N. 6351, 6355; *Belue v. Leventhal*, 640 F.3d 567, 574 (4th Cir. 2011) ("[R]ecusal motions serve as an important safeguard against truly egregious conduct," but "they cannot become a form of brushback pitch for litigants to hurl at judges who do not rule in their favor."). With no "clear cut" violation of any kind, *Cerceda*, 172 F.3d at 816, vacatur would be a strike against reason and a miscarriage of justice.

CONCLUSION

The judgment should be affirmed.

Respectfully submitted,

Dated: December 6, 2021

By: */s/ Paul J. Andre*

Paul J. Andre
Lisa Kobialka
James Hannah
Hannah Lee
Kramer Levin Naftalis
& Frankel LLP
990 Marsh Road
Menlo Park, CA 94025
Tel: (650)752-1700
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com
hlee@kramerlevin.com

Andrei Iancu
Alan J. Heinrich
IRELL & MANELLA LLP
1800 Avenue of the Stars
Los Angeles, CA 90067
Telephone: (310) 203-7537

Philip J. Warrick
IRELL & MANELLA LLP
750 17th Street NW, Suite 850
Washington, DC 20006
Telephone: (202) 831-6238

Blair A. Silver
BANNER & WITCOFF, LTD.
1100 13th Street NW, Suite 1200
Washington, DC 20005
Telephone: (202) 824-3000

Christopher Cotropia
Bey & Cotropia PLLC
213 Bayly Court
Richmond, VA 23229
Tel: (804) 404-2367
chris@beycotropia.com

Attorneys for Plaintiff-Appellee,
Centripetal Networks, Inc.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on December 6, 2021, a copy of the foregoing document:

CENTRIPETAL NETWORKS, INC.'S RESPONSE BRIEF [NON-CONFIDENTIAL]

was filed electronically with the Clerk of the Court using the CM/ECF System, which will send a Notice of Docket Activity via electronic mail to all counsel of record.

Dated: December 6, 2021 By: */s/ Paul J. Andre*
Paul J. Andre

CERTIFICATE OF CONFIDENTIAL MATERIAL

The foregoing document contains 7 unique words (including any numbers) that are marked confidential as permitted by Fed. Cir. R. 25.1(d)(1)(A).

Dated: December 6, 2021 By: */s/ Paul J. Andre*
Paul J. Andre

CERTIFICATE OF COMPLIANCE WITH FED. CIR. R. 32

1. The foregoing filing complies with the type-volume limitation of Fed. Cir. R. 32(b)(1) because this brief contains 13,989 words exclusive of the parts of the filing as exempted by Fed. Cir. R. 32(b)(2).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2016 in Times New Roman 14 point font.

Dated: December 6, 2021 */s/ Paul J. Andre*
Paul J. Andre