



Barbara A. Murphy
bmurphy@fostermurphy.com

April 19, 2022

ELECTRONIC FILING

The Honorable Lisa R. Barton
Secretary
U.S. International Trade Commission
500 E Street, SW
Washington, D.C. 20436

Re: *Certain Computer Network Security Equipment and Systems,
Related Software, Components Thereof, and Products Containing Same*
Inv. No. 337-TA-

Dear Secretary Barton:

In accordance with the Commission's Temporary Change to the Filing Procedure, dated March 16, 2020, enclosed for filing on behalf of Centripetal Networks, Inc. ("Complainant" or "Centripetal"), please find the following documents in support of Complainant's request that the U.S. International Trade Commission commence an investigation pursuant to Section 337 of the Tariff Act of 1930, as amended. This submission includes:

1. One (1) electronic copy of the verified Complaint and the Public Interest Statement, pursuant to 19 C.F.R. §§ 210.8(a)(1)(i) and 201.8(b);
2. One (1) electronic copy of Centripetal's letter and certification requesting confidential treatment of the information contained in Confidential Exhibits Nos. 12C, 40C, 48C, 64C - 66C, 77C, and 79C (19 C.F.R. §§ 210.5(d) and 201.6(b));
3. One (1) electronic copy of the accompanying Non-Confidential Exhibits and public versions of the Confidential Exhibits (19 C.F.R. §§ 210.8(a)(1)(i));
4. One (1) electronic copy of the Confidential Exhibits Nos. 12C, 40C, 48C, 64C - 66C, 77C, and 79C to the Complaint, pursuant to Commission Rules 201.6(c) and 210.8(a)(1)(ii);
5. One (1) electronic copy of the certified versions of United States Patent No. 9,264,370 ("the '370 Patent"), United States Patent No. 10,193,917 ("the '917

Patent”), and United States Patent No. 10,284,526 (“the ’526 Patent”) (the “Asserted Patents”) cited in the Complaint as Exhibits 1-3 (19 C.F.R. §§ 210.12(a)(9)(i));

6. One (1) electronic copy of the certified versions of each of the assignments for the Asserted Patents cited in the Complaint as Exhibits 16-18 (19 C.F.R. §§ 210.12(a)(9)(ii));

7. One (1) electronic copy of the certified versions of the prosecution histories for the Asserted Patents, included as Appendices A, C, and E to the Complaint (19 C.F.R. §§ 210.12(c)(l)); and

8. One (1) electronic copy of the patent and technical reference documents identified in each of the prosecution histories of the Asserted Patents, included as Appendices B, D, and F to the Complaint (19 C.F.R. §§ 210.12(c)(2)).

Thank you for your attention to this matter. Please contact me if you have any questions regarding this submission.

Respectfully submitted,

/s/ Barbara A. Murphy

Barbara A. Murphy
Foster, Murphy, Altman & Nickel, PC
1150 18th Street, N.W., Suite 775
Washington, D.C. 20036
Telephone: 202-822-4100
Facsimile: 202-822-4199

Counsel to Complainant Centripetal Networks, Inc.



Barbara A. Murphy
bmurphy@fostermurphy.com

April 19, 2022

REQUEST FOR CONFIDENTIAL TREATMENT

ELECTRONIC FILING

The Honorable Lisa R. Barton
Secretary
U.S. International Trade Commission
500 E Street, SW
Washington, D.C. 20436

Re: *Certain Computer Network Security Equipment and Systems,
Related Software, Components Thereof, and Products Containing Same*
Inv. No. 337-TA-

Dear Secretary Barton:

Pursuant to Commission Rules 210.5(d) and 201.6(b)(1), Complainant Centripetal Networks, Inc. (“Centripetal” or “Complainant”), respectfully requests confidential treatment of the business information contained in the Confidential Exhibit Nos. 12C, 40C, 48C, 64C – 66C, 77C and 79C to the Verified Complaint.

The information contained in the Confidential Exhibits qualifies as confidential business information pursuant to Commission Rule 201.6(a) because:

1. It is not available to the general public;
2. The disclosure of such information would cause substantial harm to Centripetal and to the competitive position of Centripetal. Specifically, the Confidential Exhibits contain confidential proprietary information relating to Centripetal’s significant domestic investments in plant, equipment, labor, and capital relating to Centripetal’s domestic industry products, the exploitation of the asserted patents, proprietary information relating to Centripetal’s patented technology, and confidential information concerning licensing arrangements to the asserted patents; and
3. Unauthorized disclosure of the information could impair the Commission’s ability to obtain information necessary to perform its statutory functions.

The Honorable Lisa R. Barton
April 19, 2022
Page 2

Thank you for your attention to this matter. Please contact me if you have any questions regarding this submission.

Respectfully submitted,

/s/ Barbara A. Murphy

Barbara A. Murphy
Foster, Murphy, Altman & Nickel, PC
1150 18th Street, N.W., Suite 775
Washington, D.C. 20036
Telephone: 202-822-4100
Facsimile: 202-822-4199

Counsel to Complainant Centripetal Networks, Inc.

**UNITED STATES INTERNATIONAL TRADE COMMISSION
WASHINGTON, DC**

In the Matter of

CERTAIN COMPUTER NETWORK
SECURITY EQUIPMENT AND SYSTEMS,
RELATED SOFTWARE, COMPONENTS
THEREOF, AND PRODUCTS CONTAINING
SAME

)
)
)
)
)
)
)
)
)
)

Investigation No. 337-TA-_____

COMPLAINANT CENTRIPETAL NETWORKS, INC.’S
STATEMENT ON THE PUBLIC INTEREST

Complainant Centripetal Networks, Inc. (“Centripetal” or “Complainant”) hereby submits this Statement Regarding the Public Interest. 19 C.F.R. § 210.8(b). The proposed Respondent is Keysight Technologies, Inc. (“Keysight”). For purposes of the Complaint and this public interest statement, the relief that Centripetal seeks is a limited exclusion order and a cease and desist order directed to certain network traffic monitoring and security enforcement computer equipment, as well as related software components thereof, and products containing the same imported into the United States, sold for importation into the United States, and/or sold in the United States after importation by Keysight (collectively, the “Accused Products”). The Accused Products infringe one or more claims of three valid and enforceable patents owned by Centripetal: United States Patent Nos. 9,264,370 (the “’370 Patent”), 10,193,917 (the “’917 Patent”), and 10,284,526 (the “’526 Patent”) (collectively, the “Asserted Patents”).

The issuance of the requested relief will not have a negative impact on public health and welfare, on competitive conditions in the United States economy, the production of like or directly competitive articles in the United States or on consumers in the United States. Rather, the requested relief, if granted, would promote Centripetal’s domestic industry and protect

Centripetal's intellectual property rights. Indeed, the Commission has recognized that a strong public interest exists in enforcing intellectual property rights. *Certain Baseband Processor Chips and Chipsets, Transmitter and Receiver (Radio) Chips, Power Control Chips, and Products Containing Same, Including Cellular Telephone Handsets*, Inv. No. 337-TA-543, Comm'n Op., 2011 WL 6121182, at *68 (Oct. 1, 2011) ("We are also mindful that the very purpose of Section 337 is to enforce intellectual property rights against unfair acts."); *Certain Ink Cartridges and Components Thereof*, Inv. No. 337-TA-565, Comm'n Op. at *38 (Sept. 24, 2009) ("The public interest is not served if intellectual property rights are not respected, and the imposition of a penalty that is substantial enough to deter future violations is in the public interest."). Thus, the Commission should grant the requested relief as there is a strong interest in protecting intellectual property rights and the requested relief will not adversely affect public health and safety, the economy, or consumers.

I. Use of Accused Products in the United States

The Accused Products include certain network traffic monitoring and security enforcement computer equipment, as well as related software components thereof, and products containing the same, and include Keysight's Vision One, Vision X, Vision 7300, Vision 7303, Vision Edge 1S, Trade Vision, ThreatArmor 1G and ThreatArmor 10G. The Accused Products are typically used by commercial businesses and data centers in the United States to monitor, detect, and respond to network activities and cyber threats.

II. Requested Remedial Orders Will Not Raise Public Health, Safety, or Welfare Concerns

The exclusion of the Accused Products would not cause any public health, safety, or welfare concerns. There are available replacements if the Accused Products were removed from the U.S. market. Indeed, Centripetal already provides its CleanINTERNET® solutions

that directly compete with the infringing technology in the Accused Products. Furthermore, Cisco Systems, Inc. (“Cisco”), which has already been found to infringe some of Centripetal’s other patents, including a patent related to the asserted ‘370 Patent pursuant to a judgment under appeal, can also provide products that could be “substitutes” for the Accused Products. The Commission only denies exclusion orders in limited circumstances, such as when the articles are critical to United States health and welfare and would be unavailable in the United States market were an exclusion order granted. *See Spansion, Inc. v. Int’l Trade Comm’n*, 629 F.3d 1331, 1360 (Fed. Cir. 2010) (“The Commission has found public interest considerations to outweigh the need for injunctive relief in protecting intellectual property rights found to have been violated under Section 337 in only three investigations, all of which were decided prior to the 1988 legislative amendment discussed above, which removed the requirement that a patentee show irreparable harm.”). Contrary to technologies such as “energy efficient automobiles, basic scientific research, or hospital equipment” where public health and welfare are at issue, the technologies here are not critical to the health and welfare of consumers, at least because Centripetal is able to meet the demand for these products. *Id.* (noting that the rare few cases where an exclusion order was denied were “because inadequate supply within the United States—by both the patentee and domestic licensees—meant that an exclusion order would deprive the public of products necessary for some important health or welfare need: energy efficient automobiles, basic scientific research, or hospital equipment.”).

Centripetal has over 20,000 square feet of combined research and development, engineering, and testing facilities to research, develop, test, and load its software, with plans to add another 20,000 feet in 2022, all of which are in the United States. Centripetal has the capacity to meet more than its current share of demand, and continues to grow directly and

through partners. In addition to its own capacity, Centripetal has partnered with leading United States-based contract manufacturers and Fortune 100 technology platform providers for hardware components made to Centripetal's specifications, which makes it possible for the company to meet any level of demand. Centripetal has invested millions in material costs and developing the supply chain entirely in the United States. The security of the United States-based supply chain has been a critical requirement of the company and a key value proposition provided to its customers. Therefore, the exclusion of the Accused Products would cause little if any disruptions to the availability of similar technologies.

III. The Accused Products Could Be Replaced If the Requested Relief is Granted

Centripetal's requested relief would not adversely affect competitive conditions in the United States economy. In evaluating this factor, "the appropriate standard is not that no remedy should issue if every consumer cannot obtain the exact device desired that was found to infringe the patents at issue. Rather, the impact is assessed in the aggregate and consideration is given to whether there are reasonable substitutes for the devices subject to the exclusion order in terms of features, price points, and other pertinent factors." *Certain Elec. Digital Media Devices & Components Thereof*, Inv. No. 337-TA-796, Comm'n Op. at *80 (Sept. 6, 2013). Centripetal domestically researches, develops, engineers, and tests its CleanINTERNET solutions to customers, which are Threat Intelligence Gateway systems that practice the Asserted Patents ("the Domestic Industry Products"), and whose technologies are in direct competition with the technologies in the Accused Products. Centripetal's products are readily available to replace the Accused Products, when the Commission issues the requested relief. Centripetal can make these replacement products from its United States facilities.

In addition, the Accused Products are only a subset of Keysight's products in its computer network security equipment and systems offerings. For example, in Keysight's

Network Packet Brokers product category, Keysight offers additional, non-accused product models such as Vision E40, Vision E100, Vision 7816, Vision E10S, as alternatives to the accused Vision E1S, Vision One, Vision X, Vision 7300, and Vision 7303 products.

IV. There is the Capacity to Replace the Volume of the Accused Products in a Commercially Reasonable Time in the United States

Centripetal's CleanINTERNET® solutions are readily available and would be accessible in the United States in a commercial reasonable time. For example, the volume of ThreatArmor 1G and ThreatArmor 10G can be replaced by Centripetal's domestically developed and engineered CleanINTERNET solutions. The technologies in the Vision ONE, Vision X, Vision 7300, Vision 7303, Vision Edge 1S, and Trade Vision can also be replaced by CleanINTERNET solutions with sufficient volume. In addition, Keysight can replace any excluded Accused Products from its Vision series products with its other non-accused product models in the same product category.

V. The Relief Requested Will Have No Significant Negative Impact on United States Consumers

The requested relief will not adversely impact consumers. Since there is no unfilled demand, United States consumers will continue to have undelayed access to Centripetal's own domestically developed and patent protected products, Keysight's non-accused products, and other substitute products. To the extent Keysight could identify some minimal impact on United States consumers due to the exclusion of its Accused Products, that would not outweigh the strong public interest in enforcing intellectual property rights.

VI. Conclusion

For the foregoing reasons, there are no public interest concerns that would preclude the Commission from issuing the remedial orders requested by the Complainant.

Respectfully submitted,

Dated: April 19, 2022

By: /s/ Paul J. Andre

Paul J. Andre

Lisa Kobialka

James Hannah

Kris Kastens

Hannah Lee

KRAMER LEVIN NAFTALIS

& FRANKEL LLP

990 Marsh Road

Menlo Park, CA 94025

Telephone: (650) 752-1700

Facsimile: (650) 752-1800

pandre@kramerlevin.com

lkobialka@kramerlevin.com

jhannah@kramerlevin.com

kkastens@kramerlevin.com

hlee@kramerlevin.com

James B. Altman

Barbara A. Murphy

Susan Koegel

Matthew N. Duescher

FOSTER MURPHY ALTMAN

& NICKEL, PC

1150 18th Street NW, Suite 775

Washington, DC 20036

Telephone: (202) 822-4100

Facsimile: (202) 822-4199

FM-CNI@fostermurphy.com

Attorneys for Complainant

CENTRIPETAL NETWORKS, INC.

**UNITED STATES INTERNATIONAL TRADE COMMISSION
WASHINGTON, DC**

In the Matter of

CERTAIN COMPUTER NETWORK
SECURITY EQUIPMENT AND SYSTEMS,
RELATED SOFTWARE, COMPONENTS
THEREOF, AND PRODUCTS
CONTAINING SAME

)
)
) Investigation No. 337-TA-_____
)
)
)
)
)
)

**COMPLAINT OF CENTRIPETAL NETWORKS, INC.
UNDER SECTION 337 OF THE TARIFF ACT OF 1930, AS AMENDED**

COMPLAINANT

Centripetal Networks, Inc.
1875 Explorer Street, Suite 900
Reston, VA 20190

RESPONDENT

Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738
(800) 829-4444

COUNSEL FOR COMPLAINANT

Paul J. Andre
Lisa Kobialka
James Hannah
Kris Kastens
Hannah Lee
**KRAMER LEVIN NAFTALIS
& FRANKEL LLP**
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com
kkastens@kramerlevin.com

James B. Altman
Barbara A. Murphy
Susan Koegel
Matthew N. Duescher
**FOSTER MURPHY ALTMAN &
NICKEL, PC**

1150 18th Street NW, Suite 775
Washington, DC 20036
Telephone: (202) 822-4100
Fax: (202) 822-4199
FM-CNI@fostermurphy.com

Attorneys for Complainant
CENTRIPETAL NETWORKS, INC.

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. THE PARTIES.....	3
A. COMPLAINANT CENTRIPETAL.....	3
1. Centripetal's Products	4
B. PROPOSED RESPONDENT KEYSIGHT	8
1. The Accused Products.....	10
2. Keysight's Products	10
III. COMPLAINT BASED ON UNITED STATES PATENTS	15
A. Identification of Each United States Patent	15
B. Non-Technical Description of Asserted Patents	16
1. Non-Technical Description of United States Patent No. 9,264,370.....	16
2. Non-Technical Description of United States Patent No. 10,193,917.....	17
3. Non-Technical Description of United States Patent No. 10,284,526.....	18
C. Licensees under Each Asserted United States Patent	18
D. Foreign Patents and Applications	19
IV. UNFAIR ACTS OF PROPOSED RESPONDENT	20
A. Infringement of United States Patent No. 9,264,370	20
B. Infringement of United States Patent No. 10,193,917	24
C. Infringement of United States Patent No. 10,284,526	28
V. SPECIFIC INSTANCES OF UNFAIR IMPORTATION AND SALE	31
VI. BRIEF SUMMARY OF AGENCY OR COURT LITIGATION.....	38

VII.	DOMESTIC INDUSTRY	43
A.	Technical Prong	43
B.	Economic Prong.....	45
1.	Plant and Equipment	45
2.	Labor or Capital	46
3.	Exploitation of Patents.....	46
VIII.	REQUESTED RELIEF.....	47

LIST OF EXHIBITS

<u>Documentary Exhibits</u>	<u>Description</u>
1	Certified Copy of United States Patent No. 9,264,370
2	Certified Copy of United States Patent No. 10,193,917
3	Certified Copy of United States Patent No. 10,284,526
4	Press Release: Centripetal Named SINET 16 Innovator for 2017, dated October 31, 2017
5	Press Release: Centripetal Networks Named a 2017 Gartner “Cool Vendor” in Security, dated July 25, 2017
6	Press Release: Centripetal Ranked Number 93 of the Fastest Growing Companies in North America on Deloitte’s 2019 Technology Fast 500, dated December 2, 2019
7	Press Release: Centripetal Features in Deloitte’s 2020 Technology Fast 500, dated December 1, 2020
8	Deloitte 2021 Technology Fast 500 Rankings
9	SC Media Article: Finalists: Best Threat Intelligence Technology, dated March 29, 2021
10	Centripetal Data Sheet: RuleGATE 2000 Gateway, dated 2017
11	Centripetal Webpage: CleanINTERNET, dated February 8, 2022
12C	CONFIDENTIAL Declaration of Jonathan Rogers in Support of Complaint of Centripetal Networks, Inc., dated April 18, 2022
13	Centripetal Case Study: Financial Services Organization Sees Success with Smarter Threat Intelligence, dated 2018
14	Centripetal Case Study: Insurance Company Gains Real-Time Networks Enforcement, dated 2018
15	Centripetal Case Study: Retailer Safeguards Network with Advanced Security Solutions, dated 2018
16	Certified Assignments for United States Patent No. 9,264,370
17	Certified Assignments for United States Patent No. 10,193,917

18 Certified Assignments for United States Patent No. 10,284,526

19 Keysight Webpage: ThreatARMOR: Threat Intelligence Gateway, dated
January 5, 2022

20 Keysight Webpage: Application and Threat Intelligence (Subscription),
dated February 3, 2022

21 Infringement Chart for United States Patent No. 9, 264,370

22 Infringement Chart for United States Patent No. 10,193,917

23 Infringement Chart for United States Patent No. 10,284,526

24 IPWatchdog.com Article: Centripetal Networks Awarded \$1.9 Billion in
Infringement Suit Against Cisco, dated October 9, 2020

25 SC Media Article: Judge Denies Cisco New Trial, Upholds Judgment in
Patent Infringement Suit, dated March 29, 2021

26 Keysight Network Visibility Products Catalog, dated November 3, 2021

27 Keysight Webpage: Vision ONE, dated January 9, 2022

28 Keysight Webpage: Network Packet Brokers, dated December 31, 2021

29 Keysight Data Sheet: CloudLens Self-Hosted, dated August 21, 2020

30 Keysight Webpage: NetStack, dated December 31, 2021

31 Keysight Webpage: SecureStack, dated December 31, 2021

32 Keysight Webpage: AppStack, dated December 31, 2021

33 Keysight Webpage: AppStack, dated December 31, 2021

34 Keysight Webpage: MobileStack, dated December 31, 2021

35 Keysight Data Sheet: ThreatARMOR, dated April 28, 2021

36 Keysight Solution Brief: Threat Simulator: Proving You're Safer Than
You Were Yesterday, dated November 25, 2020

37 Keysight Webpage: Network Security Tools, dated December 31, 2021

38 Keysight Webpage: Application and Threat Intelligence (Subscription),
dated December 31, 2021

- 39 Keysight Webpage: ThreatArmor: Threat Intelligence Gateway, dated December 31, 2021
- 40C CONFIDENTIAL Mutual Non-Disclosure Agreement (NDA) between Centripetal Networks, Inc. and Ixia, dated November 4, 2014
- 41 Keysight Webpage: CloudLens, dated January 25, 2022
- 42 Keysight Data Sheet: Vision X Network Packet Broker, dated October 13, 2021
- 43 Keysight Webpage: Vision One, dated February 3, 2022
- 44 Keysight Webpage: Vision X Network Packet Broker, dated February 3, 2022
- 45 Keysight Investor Day 2020 Presentation, dated March 3, 2020
- 46 Keysight Press Release: Keysight Technologies' Corporate Headquarters Operational After Northern California Fires, dated November 6, 2017
- 47 Keysight/Ixia Vision One Product Label
- 48C CONFIDENTIAL Binding Term Sheet between Centripetal Networks, Inc. and Keysight Technologies, Inc. and Ixia, dated October 9, 2018
- 49 Keysight Webpage: Support, dated January 25, 2022
- 50 Keysight Webpage: Keysight Support, dated January 25, 2022
- 51 Ixia Webpage: Support, dated January 25, 2022
- 52 Keysight White Paper: Advanced Security Intelligence with Rap Sheet Analytics, dated November 10, 2021
- 53 Ixia Case Study: Financial Investment Firm Reduces Risk
- 54 Keysight Press Release: Keysight's New Security Operations Platform Enables Organizations to Measure and Improve Effectiveness of Operational Security, dated February 6, 2022
- 55 Keysight Form 10-K Annual Report for the fiscal year ended October 31, 2021
- 56 Keysight Webpage: TradeVision, dated January 25, 2022
- 57 Keysight Webpage: Network Security Tools, dated January 25, 2022

- 58 Keysight Webpage: Sales Request, dated February 4, 2022
- 59 CDW.com Webpage: Ixia Vision ONE with Fixed 48 Port SFP+ Security Appliance, dated February 4, 2022
- 60 Insight.com Webpage: Ixia Vision ONE SYS-Va-48PX-AC Security Appliance, dated 2022
- 61 Shi.com Webpage: Ixia ThreatARMOR 1G Security Appliance, dated February 4, 2022
- 62 Deltatechsol.com Webpage: Ixia ThreatARMOR-1G – ThreatArmor 1GBE Security Appliance with 4 1GB SFP Ports, Requires Active ATI, dated February 4, 2022
- 63 Caegis Solutions Ebay Invoice: Ixia Vision ONE Security Appliance 48-Ports + 48 SFP-10G SR 2x PSU, dated December 16, 2021
- 64C CONFIDENTIAL Domestic Industry Chart for United States Patent No. 9,264,370
- 65C CONFIDENTIAL Domestic Industry Chart for United States Patent No. 10,193,917
- 66C CONFIDENTIAL Domestic Industry Chart for United States Patent No. 10,284,526
- 67 Ixia Press Release: Ixia Leverages the Cloud to Streamline Network Threat Intelligence, dated November 9, 2016
- 68 Ixia White Paper: Application and Threat Intelligence Research Center, dated 2019
- 69 Ixia Feature Brief: SecureStack – Optimized Handling of Secure Traffic, dated 2018
- 70 Keysight Data Sheet: Vision ONE Security Without Sacrifice, dated July 23, 2021
- 71 Ixia Technical Overview: Ixia’s Inline Security Architecture, dated January 7, 2020
- 72 Keysight White Paper: Inspecting SSL Traffic: Achieving the Right Balance of Visibility and Security, dated May 22, 2020
- 73 Keysight Solution Brief: Security: In An Encrypted World, dated February 25, 2020

74	Centripetal Service Brief: CleanINTERNET, dated 2018
75	Centripetal Product Brief: CleanINTERNET, dated 2018
76	Centripetal: CleanINTERNET Managed Security Services, dated
77C	CONFIDENTIAL Centripetal Presentation: Active Network Defense
78	Centripetal White Paper: Far Beyond The Firewall: Centripetal CleanINTERNET Service, dated 2019
79C	CONFIDENTIAL Centripetal Presentation: Efficient SSL/TLS Threat Proxy aka “Decryption”: H/L Requirements PM Considerations Etc., dated March 22, 2019
80	Keysight Software Entitlement Certificate
81	Keysight Shipping Point Labels
82	Guidepoint Security, LLC Invoice, dated February 24, 2022

LIST OF APPENDICES

<u>Appendix</u>	<u>Description</u>
A	Certified Copy of Prosecution History for United States Patent No. 9,264,370
B	Copies of References Cited in Prosecution History of United States Patent No. 9,264,370
C	Certified Copy of Prosecution History for United States Patent No. 10,193,917
D	Copies of References Cited in Prosecution History of United States Patent No. 10,193,917
E	Certified Copy of Prosecution History for United States Patent No. 10,284,526
F	Copies of References Cited in Prosecution History of United States Patent No. 10,284,526

I. INTRODUCTION

1. Centripetal Networks, Inc. (“Centripetal”) requests that the United States International Trade Commission (“ITC”) institute an investigation pursuant to Section 337 of the Tariff Act of 1930, as amended, 19 U.S.C. § 1337 (“Section 337”), to remedy the unlawful importation, sale for importation, and/or sale within the United States after importation by Keysight Technologies, Inc. (“Keysight”) of certain computer network security equipment and systems, related software technologies, components thereof, and products containing same (collectively, “the Accused Products”) that infringe, directly or indirectly, literally or under the doctrine of equivalents, certain claims of United States Patent Nos. 9,264,370 (the “’370 Patent”), 10,193,917 (the “’917 Patent”), and 10,284,526 (the “’526 Patent”) (collectively “the Asserted Patents”) (Exs. 1-3).

2. A domestic industry, as required by 19 U.S.C. § 1337(a)(3)(A), (B), and/or (C) exists in the United States relating to the technology protected by the Asserted Patents. This industry is supported by Centripetal’s significant and substantial domestic investments in plant, equipment, labor, and capital in connection with Centripetal’s computer network security equipment and systems, related software technologies, and components thereof, and Centripetal’s exploitation of the technologies protected by the Asserted Patents.

3. Centripetal seeks, as relief, a permanent limited exclusion order pursuant to 19 U.S.C. § 1337(d), barring from entry into the United States certain computer network security equipment and systems, related software technologies, components thereof, and products containing same that infringe one or more claims of the Asserted Patents and are imported by or on behalf of Keysight. Centripetal also seeks a cease and desist order, pursuant to 19 U.S.C. § 1337(f), against Keysight and its parent entities, subsidiaries, affiliates, related entities, agents, distributors, importers, or consignees (or agents thereof) from engaging in activities

including, but not limited to, importing, marketing, advertising, demonstrating, warehousing inventory for distribution, offering for sale, selling, distributing, licensing, or using certain computer network security equipment and systems, related software technologies, components thereof, and products that infringe one or more claims of the Asserted Patents. Additionally, Centripetal requests the imposition of a bond pursuant to 19 U.S.C. § 1337(j), for any activities otherwise covered by the limited exclusion order and/or permanent cease and desist order, during the period of Presidential review of the Commission’s remedial orders.

4. Computer network security (also referred to as “Cybersecurity”) that is at issue in this Complaint relates to the protection of organizations from the myriad of bad actors that want to steal their information or otherwise compromise their computer systems. These bad actors are sophisticated and may be run by organized crime syndicates or foreign nations. Cutting edge technology that generates and uses cyber threat intelligence is at the forefront of defending from these attacks. Cyber threat intelligence includes gathering threat intelligence, performing rapid correlation of this threat intelligence, and using the resulting intelligence gained to protect an organization from the threat of these bad actors.

5. Keysight has engaged in unlawful and unfair acts including the importation into the United States, sale for importation into the United States, and/or sale within the United States after importation of Accused Products that infringe the Asserted Patents. A complete listing of the claims asserted by Centripetal in this investigation (collectively, “the Asserted Claims”) is shown below with the independent claims shown in **bold**:

Patent	Asserted Claims	Accused Products
9,264,370	22 , 23, 24, 25, 26, 27, 42, 43 , 44, 45, 46, 47, 48, 63	Vision One, Vision X, Vision 7300, Vision 7303, Vision Edge 1S, and Trade Vision

10,193,917	1, 5, 11, 15, 20	ThreatArmor 1G, ThreatArmor 10G
10,284,526	1, 2, 3, 6, 11, 12, 13, 16	Vision One, Vision X, Vision 7300, Vision 7303, and Trade Vision

II. THE PARTIES

A. COMPLAINANT CENTRIPETAL

6. Centripetal is a Delaware corporation with its principal place of business at 1875 Explorer Street, Suite 900, Reston, VA 20190. Centripetal also has facilities in Portsmouth, New Hampshire, and formerly headquartered in Herndon, VA. Centripetal was founded in 2009 by Steven Rogers, who has over 40 years of experience in secure communications and works on various aspects of secure communications for the United States Government. Since its founding, Centripetal has invested extensively in cutting-edge solutions for protecting computer networks from advanced threats, including considerable investments in capital, labor, expertise and ingenuity in design, research and development (“R&D”), and engineering in the United States to deliver security solutions across public and private sectors.

7. For over 10 years, Centripetal has designed and developed innovative network security technologies. Centripetal became the first in the field to develop and invent specialized core networking technologies to operationalize threat intelligence from multiple sources at an unprecedented scale and speed that could address the rapid growth in cyber threats. Centripetal was also the first to use the term “Threat Intelligence Gateway” to describe its products that include this technology. Centripetal conducts industry-leading research in Cybersecurity and has over 40 patents.

8. Centripetal has been recognized by third-party security organizations as a result of its innovations. The Security Innovation Network (“SINET”) named Centripetal the SINET

16 Innovator for 2017 at the SINET Showcase in Washington D.C. Ex. 4

(<https://www.centripetal.ai/centripetal-named-sinet-16-innovator/>). A leading research and advisory company, Gartner Research, has also recognized Centripetal as a Cool Vendor in Security for Technology and Service Providers in 2017. Ex. 5

(<https://www.prnewswire.com/news-releases/centripetal-networks-named-a-2017-gartner-cool-vendor-in-security-300493655.html>). From 2019 to 2021, Centripetal was ranked as one of the fastest growing technology companies in North America on Deloitte's Technology Fast 500.

Ex. 6 (<https://www.prnewswire.com/news-releases/centripetal-ranked-number-93-of-the-fastest-growing-companies-in-north-america-on-deloittes-2019-technology-fast-500-300966367.html>); Ex. 7 (<https://www.centripetal.ai/deloittes-2020-technology-fast-500/>); Ex. 8 at 3. Centripetal was recognized by SC Media in 2021 as a finalist for best threat intelligence technology. Ex. 9 (<https://www.scmagazine.com/news/-/best-threat-intelligence-technology-finalists>).

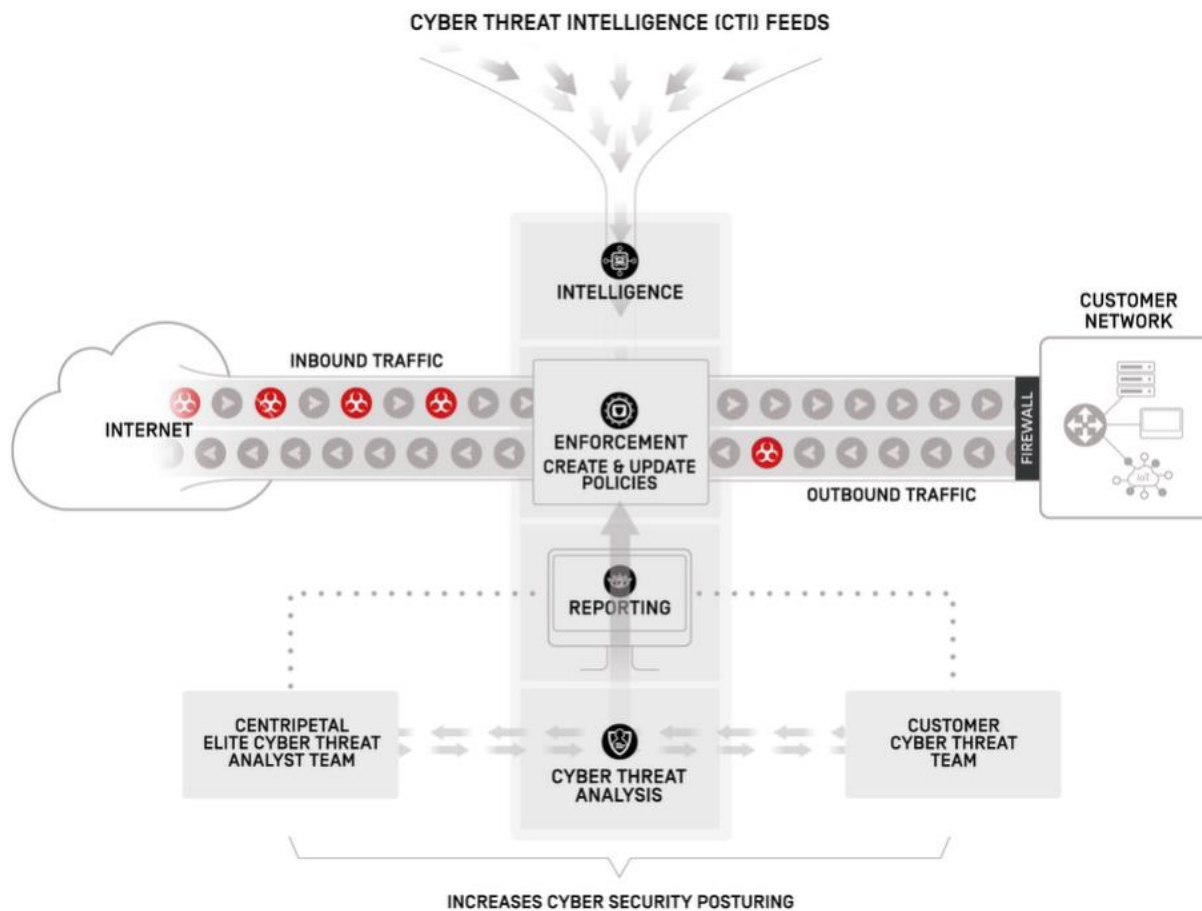
1. Centripetal's Products

9. Centripetal's CleanINTERNET® solutions practice the Asserted Patents ("the Domestic Industry Products"). An example of a CleanINTERNET® solution is Centripetal's "RuleGATE®" systems, which are specialized rack mounted computer systems that practice the Asserted Patents. There are several different models of the RuleGATE® systems, including the model number RG-100, RG-2000, and RG-2200. These systems differ in the processing power of the computer system, with some being able to handle larger traffic loads. An example of the RuleGATE® systems is provided below:



Ex. 10.

10. The Domestic Industry Products all operate in the same fundamental manner. A high-level diagram of the operation of the Domestic Industry Products is reproduced below.



Ex. 11 (<https://www.centripetal.ai/cleaninternet>).

11. As shown in the diagram above, the Domestic Industry Products generate and

use cyber threat intelligence, or “CTI”, to catch and eradicate known and unknown threats. CTI is information about different threats on the Internet. CTI is processed by Intelligence and sent to Enforcement (*e.g.* the RuleGATE® system) as rules, where the rules can be used to allow, block, divert (for further inspections), and log network traffic. Enforcement receives and analyzes inbound traffic that is entering a customer’s network from the Internet and also outbound traffic that is leaving a customer’s network and going to an external computer on the Internet. Enforcement blocks or reports traffic that is known to be malicious based on comparing it to rules created from the CTI. For example, traffic that originates from a known malicious source can be blocked. Or, traffic that is being sent to a malicious destination can be blocked. Enforcement can operate on both unencrypted traffic and traffic that has been encrypted. When the traffic is encrypted, Enforcement can utilize threat intelligence based on rules to determine whether to block traffic (without decryption) or send the traffic to another engine for further analysis with decryption. Enforcement also generates logs of network traffic which can be used to correlate network traffic and to uncover a malicious host that might have otherwise been obfuscated. For example, with correlations, the Cyber Threat Analysis can determine if computers in the customer’s network have been compromised and are sending traffic to computers on the Internet that are known to be bad. As another example, Enforcement’s activities can be used for traffic flow analytics and displayed to a user. The Domestic Industry Products provide its users with visibility into cyber threats with real-time attack visualization and analytics used by threat response teams.

12. The Domestic Industry Products are made by Centripetal in facilities located in Portsmouth, NH and Reston, VA. Ex. 12C (Declaration of Jonathan Rogers (“Rogers Decl.”)) at ¶ 11. Within these Centripetal facilities, employees conduct activities including product

development and engineering, testing, and sales operations. *Id.* at ¶ 14. The software for the Domestic Industry Products is also developed in Portsmouth, NH and Reston, VA. *Id.* at ¶ 11. The Domestic Industry Products also have been researched, developed, and engineered by numerous technologists working at Centripetal's Portsmouth, NH and Reston, VA facilities. *Id.* at ¶¶ 14-15. This R&D includes ongoing improvements to the Domestic Industry Products and software upgrades as well as testing and ongoing support and maintenance. In connection with the exploitation of the technologies covered by the Asserted Patents, Centripetal has made significant investments in the United States in plant, equipment (such as computers and testing equipment), labor, and capital. *Id.* at ¶¶ 13-17. Centripetal relies on its patents to protect its valuable technology and inventions underlying its investments.

13. Centripetal has made significant and substantial investments in plant, equipment, labor, capital, R&D, and engineering in the United States to develop and support the equipment and systems, related software, components thereof, and products protected by the Asserted Patents. For example, Centripetal maintains facilities and employs approximately 80 people in the United States to carry out R&D, production, maintenance, engineering, procurement and sourcing, sales and marketing, quality control, and distribution of the devices and systems, related software, components thereof, and products containing the technologies protected by the Asserted Patents. Ex. 12C (Rogers Decl.) at ¶ 19. Centripetal sources hardware components from domestic manufacturing facilities that are designed according to Centripetal's specifications. Ex. 12C (Rogers Decl.) at ¶ 11. Centripetal assembles the specially made hardware components and loads its software onto them. Ex. 12C (Rogers Decl.) at ¶ 11.

14. The Domestic Industry Products are used by a wide variety of entities across the

United States to provide network security. *See, e.g.*, Exs. 13-15. These entities include medium to large companies as well as high performance network environments such as global e-commerce retailers, critical infrastructure providers, and government applications.

15. Centripetal owns the entire rights, title, and interest in and to the Asserted Patents. Exs. 16-18.

B. PROPOSED RESPONDENT KEYSIGHT

16. Keysight is a Delaware corporation with its principal place of business at 1400 Fountaingrove Parkway, Santa Rosa, California 95403. Today, Keysight is a multi-billion dollar company that improperly provides computer network security equipment systems having Centripetal's patented threat intelligence technologies to customers. *See, e.g.*, Ex. 19 (<https://www.keysight.com/us/en/products/network-security/breach-defense/threat-armor.html>) (showing Keysight's ThreatArmor product uses threat intelligence technologies and Keysight advertises ThreatArmor as Threat Intelligence Gateway); Ex. 20 (<https://www.keysight.com/us/en/products/network-security/ati-application-threat-intelligence.html>) (showing Keysight's application threat intelligence subscription).

17. Centripetal sued Keysight for patent infringement on July 20, 2017 in the United States District Court for the Eastern District of Virginia. *Centripetal Networks, Inc. v. Keysight Technologies, Inc., and Ixia*, Case No. 2:17-cv-00383-HCM-LRL (E.D. Va.) ("*Keysight I*"). In *Keysight I*, Centripetal alleged Keysight infringed five Centripetal patents, including the '370 Patent which is also asserted in this Complaint and the '722 Patent, which is in the same family as the asserted '917 Patent in this Complaint. *See Centripetal Networks, Inc. v. Keysight Technologies, Inc., and Ixia*, Case No. 2:17-cv-00383-HCM-LRL, Dkt. No. 192 (Amended Complaint) (E.D. Va., Jul. 13, 2018). Trial commenced in October 2018. After Centripetal presented its case in chief, which included detailed evidence of Keysight's

infringement of Centripetal's patents and copying of Centripetal's products and technologies, Keysight settled with Centripetal by entering into a three-year patent license agreement for Centripetal's patents, including the Asserted Patents, to make, use, and sell Keysight's VisionONE, Vision 7300, Vision 7303, with AppStack and SecureStack on the infringing hardware, ThreatArmor, and BreakingPoint with Application and Threat Intelligence ("ATI") during the term. Ex. 48C.

18. After the license from Centripetal expired on December 31, 2021, Keysight has continued to make, use and sell the Accused Products incorporating Centripetal's patented technologies without a license or authorization. Exs. 21-23. As of the filing of this Complaint, Keysight has not attempted to re-license the Asserted Patents from Centripetal.

19. Prior to filing this Complaint, Keysight knew about the Asserted Patents because these patents were subject to the brief term license Keysight executed with and received from Centripetal in 2018 as set forth immediately above. In addition to the license, the technologies related to the '370 and '917 Patents were available to Keysight through other publicly available information, including the patent litigation filed by Centripetal against Keysight's competitors, Cisco Systems, Inc. ("Cisco"), and Palo Alto Networks ("PAN") in 2018 and 2021 respectively. In its litigation against Cisco in October of 2020, Centripetal obtained a judgment of validity and infringement against Cisco and damages of \$2.6 to \$3.2 billion based on a 5-10% royalty rate. This judgement was well publicized in the relevant industry providing further notice to Keysight of Centripetal's patents and patented technologies. *See, e.g.*, Ex. 24 (<https://www.ipwatchdog.com/2020/10/09/centripetal-networks-awarded-1-9-billion-infringement-suit-cisco/id=126094/>); Ex. 25 (<https://www.scmagazine.com/news/security-news/legal-security-news/judge-denies-cisco->

new-trial-upholds-judgement-in-patent-infringement-suit).

1. The Accused Products

20. In accordance with Commission Rule 210.12(a)(12), the products at issue are certain network traffic monitoring and security enforcement computer equipment, as well as related network analysis software components thereof, and products containing the same.

2. Keysight's Products

21. Keysight sells a number of products that are used for securing the networks of its customers. Keysight's Vision One, Vision X, Vision 7300, Vision Edge 1S, and Trade Vision, as well as the infringing software and components used by and with those devices ("Network Visibility Products") provide network security by detecting network threats and filtering network traffic with threat intelligence. *See, e.g.*, Ex. 26. Similar to Centripetal's Domestic Industry Products, the Keysight Network Visibility Products are computer systems, which can be rack mounted, an example of which is shown below:



Ex. 27.

22. The infringing Keysight Network Visibility products also monitor and log network traffic, which can be used by data analytics tools to discover network vulnerabilities. *See, e.g.*, Ex. 28. The infringing Network Visibility Products include products from the same families of products, but which include capacity differences. As discussed below, the

infringing Keysight Network Visibility Products are imported into the United States, sold for importation into the United States, and/or sold in the United States after importation.

23. By way of example, the infringing Network Visibility Products may be deployed by customers to leverage network threat intelligence to monitor, detect, and respond to network activities and threats. The infringing Network Visibility products include Keysight's underlying infringing technologies that are marketed as NetStack, PacketStack, SecureStack, AppStack, and MobileStack technologies. *See e.g.*, Exs. 26, 28. As described in greater detail below, NetStack, PacketStack, SecureStack, AppStack, and MobileStack software technologies provide Keysight's Network Visibility products with increased security, control, and/or visibility into packets traversing a network.

24. NetStack operates on network packets with a three-stage filtering process. Ex. 30. NetStack has features such as "robust filtering, load balancing, aggregation, replication, three stages of filtering, and dynamic filter compiler." Ex. 26 at 6. Keysight also advertises NetStack as being able to make "hitless changes – no packets dropped when you re-configure." Ex. 30.

25. PacketStack "[p]rovides intelligent packet filtering, manipulation, and transport with deduplication that removes duplicate packets at full line rate with no loss. Other capabilities include header (protocol) stripping, packet trimming, time stamping, data masking, and burst protection." Ex. 26 at 6.

26. SecureStack "optimizes handling for secure traffic. Supports inline and out-of-band SSL / TLS decryption and threat intelligence." Ex. 26 at 6. SecureStack has the threat insight feature which allows Network Visibility products to "[r]ecognize malware, botnet, exploits, hijacked IPs and phishing activity" and "[s]end threat information automatically via

NetFlow to existing security appliances.” Ex. 31

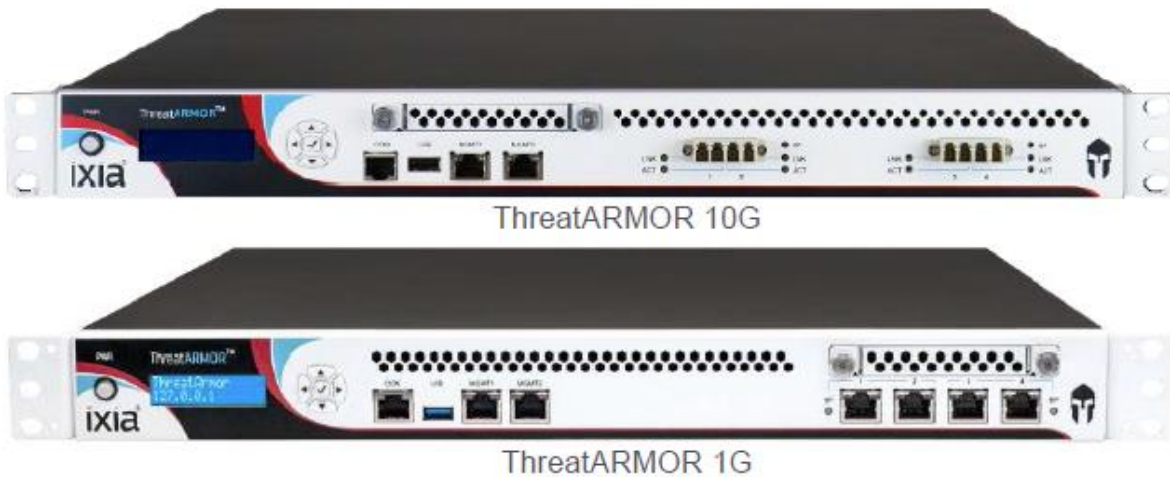
(<https://www.keysight.com/us/en/products/network-visibility/network-packet-brokers/securestack.html>).

27. AppStack, among other things, “[p]rovide[s] context-aware, signature-based application-layer filtering with accurate and fast application identification, geolocation and tagging.” Ex. 26 at 6. AppStack has Application and Threat Intelligence subscription that provides up-to-date application and geolocation information. Ex. 32

(<https://www.keysight.com/us/en/products/network-visibility/network-packet-brokers/appstack.html>); Ex. 33.

28. MobileStack “[o]ffers visibility intelligence for the mobile carrier.” Ex. 26 at 6. Among other things, MobileStack has features such as GTP/SIP Correlations (which “[offload] the correlation to Vision X, Vision One, GTP Session Controller (GSC) or Cloud Lens”) and Packet Core Filtering (which “[reduces] monitoring costs by selectively sending traffic to probes based on traffic type.”). Ex. 34.

29. Keysight’s infringing ThreatArmor 1G and 10G products, as well as the software and components used by and with those devices (“ThreatArmor Products”), are advertised as threat intelligence gateways that block malicious traffic. Ex. 19. The ThreatArmor Products are also rack mounted computer systems, example images of which are provided below:

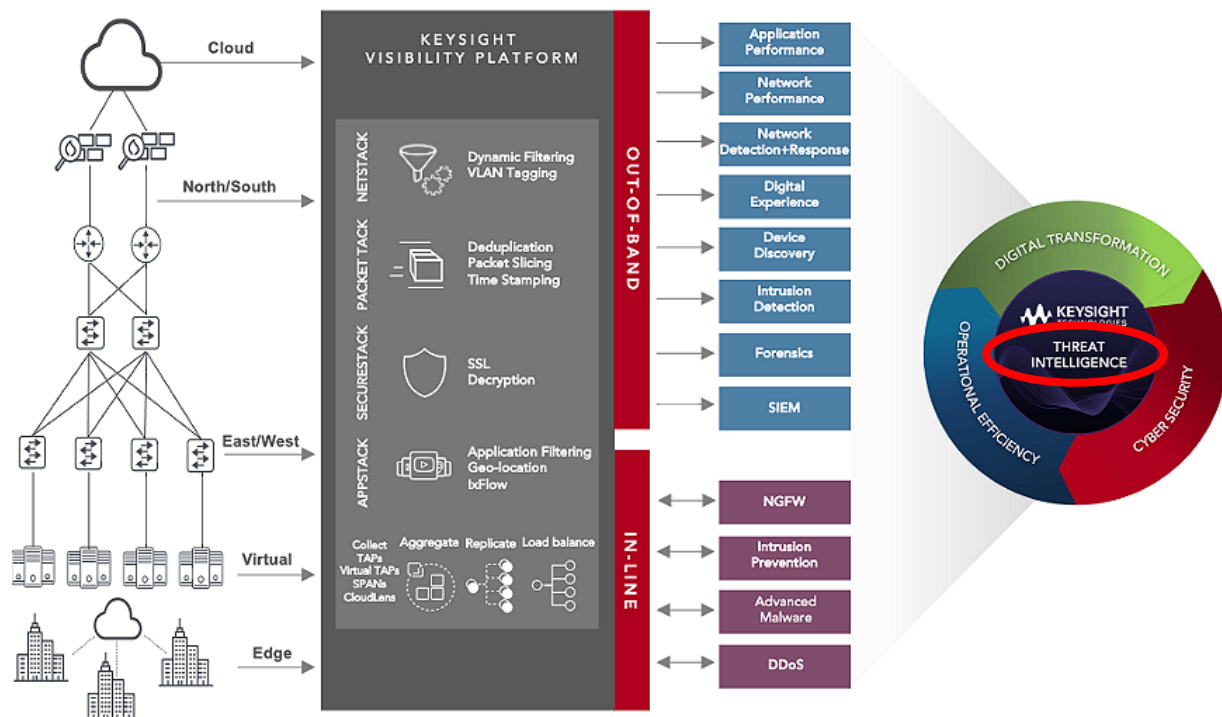


Ex. 35 (<https://www.keysight.com/us/en/assets/3119-1141/data-sheets/ThreatARMOR.pdf>).

30. Keysight sells its ThreatArmor Products in the United States. See Ex. 35 (<https://www.keysight.com/us/en/assets/3119-1141/data-sheets/ThreatARMOR.pdf>); Ex. 36. The ThreatArmor Products are imported into the United States, sold for importation into the United States, and/or sold in the United States after importation. The ThreatArmor Products “[block] bad traffic from entering your network” and “[reduce] alert fatigue by stemming the flood of notifications from your SIEM and security tools.” Ex. 37. The ThreatArmor Products use ATI technology, including ATI data feeds to carry out their functions. Exs. 38, 39; Ex. 36 at 4.

31. Keysight incorporated features and innovative technologies protected by Centripetal’s intellectual property after learning about Centripetal’s patented technology under a non-disclosure agreement (“NDA”) executed in 2014 with Ixia (now a division of Keysight acquired in 2017). Ex. 40C. Due to its infringement of the Asserted Patents, Keysight has updated its Network Visibility Products to provide network defense and protections, and centering on threat intelligence. An example of Keysight’s promotional description of its infringing systems is provided below, which illustrates that the infringing systems rely on the

infringing threat intelligence technology:



Ex. 41 (<https://www.keysight.com/us/en/products/network-visibility/cloud-visibility/cloudlens.html>); see also, e.g., Ex. 43

(<https://www.keysight.com/us/en/products/network-visibility/network-packet-brokers/visionone.html>) (“a single platform for a granular view of network security and troubleshooting”); Ex. 44 (<https://www.keysight.com/us/en/products/network-visibility/network-packet-brokers/vision-x.html>) (providing “inline security”).

32. Keysight markets its ThreatArmor Products as a threat intelligence gateway, similar to how Centripetal’s RuleGATE® Domestic Industry Product is marketed. See, e.g., Ex. 19 (<https://www.keysight.com/us/en/products/network-security/breach-defense/threat-armor.html>); Ex. 10 (https://www.centripetalnetworks.com/hubfs/Centripetal_Networks_September2017/PDF/CNI-RuleGATE2000.pdf).

33. Keysight's financial documents and website show that the Accused Products are developed abroad in Bucharest, Romania, manufactured abroad in Malaysia, and are imported into the United States by Keysight. Ex. 45 at 47 (Keysight's network test, visibility and security products are developed in Bucharest, Romania); Ex. 46 (<https://about.keysight.com/en/newsroom/pr/2017/06nov-nr17090.shtml>) ("Business continues as usual at Keysight's other 145 worldwide locations, including its primary manufacturing and order fulfillment location in Penang, Malaysia."); Ex. 42 (<https://www.keysight.com/us/en/assets/3120-1029/data-sheets/Vision-X-Network-Packet-Broker.pdf>) at 9 (Vision X's country of origin is Malaysia). Furthermore, Keysight marks at least some of the Accused Products as being assembled or made in Malaysia. Ex. 47 (picture showing Vision One with "assembled in Malaysia" sticker); Ex. 80 (ThreatArmor's Software Entitlement Certificate states "Made in MALAYSIA"); *see also* Ex. 81 (ThreatArmor's shipping box states "Shipping Point – Main Plant 56. Hilir Sg. Keluang 1 Penang").

III. COMPLAINT BASED ON UNITED STATES PATENTS

A. Identification of Each United States Patent

34. The '370 Patent, titled "Correlating Packets in Communication Networks" issued on February 16, 2016, is based on United States Patent Application No. 14/618,967, and was filed on February 10, 2015. The '370 Patent expires on February 10, 2035. Ex. 1.

35. The '917 Patent, titled "Rule-Based Network-Threat Detection" issued on January 29, 2019, is based on United States Patent Application No. 15/827,477, and was filed on November 30, 2017. The '917 Patent was previously published as United States Publication No. 2018/0159883 on June 7, 2018. The '917 Patent is a continuation of United States Patent No. 14/690,302, filed on April 17, 2015, now issued as United States Patent No. 9,866,576. The '917 Patent expires on April 17, 2035. Ex. 2.

36. The '526 Patent, titled "Efficient SSL/TLS Proxy" issued on May 7, 2019, is based on United States Patent Application No. 16/039,896, and was filed on July 19, 2018. The '526 Patent was previously published as United States Publication No. 2019/0028439 on January 24, 2019. The '526 Patent claims the benefit of United States Provisional Application No. 62/536,254, filed on July 24, 2017. The '526 Patent expires on July 19, 2038. Ex. 3.

37. Centripetal is the assignee of all rights, title, and interest in the inventions disclosed and claimed in the Asserted Patents. *See* Exs. 16-18. Pursuant to Commission Rule 210.12(c), certified copies of the prosecution histories of the Asserted Patents have been submitted with this Complaint as Appendices A, C, and E. Pursuant to Commission Rule 210.12(c), the technical references mentioned in the prosecution histories of the Asserted Patents have been submitted with this Complaint as Appendices B, D, and F.

B. Non-Technical Description of Asserted Patents¹

1. Non-Technical Description of United States Patent No. 9,264,370

38. The '370 Patent provides, among other things, improved techniques for discovering malicious endpoints and preventing malicious endpoints from damaging a network using a processor and memory to provision first and second devices with rules that causes the system to log packets, identify packets incoming and outgoing by a network device, generate log entries, correlate log entries, and perform certain actions in response to the correlation. For example, the '370 Patent describes a solution to the problem that occurs when network appliances alter data packets associated with a flow and obfuscate the flow in which a particular packet is associated. *See, e.g.*, Ex. 1 ('370 Patent) at 1:6-15, 1:41-49. This disassociation, and obfuscation of packet information, usually makes a network device unable

¹ The non-technical descriptions are provided solely for compliance with Commission rules and are not intended to limit, define, or otherwise affect the scope, construction and/or application of the Asserted Patents' claim language.

to know whether a packet posed a malicious threat to a network because it was coming from a malicious host. *See, e.g., id.; id.* at 9:52-54. However, the '370 Patent describes how to undertake an analysis to identify the true source of packets, despite any modification or obfuscation that may have occurred, based on information contained within the log entries. *See, e.g., id.* at 1:26-49. The '370 Patent also improves network security by generating rules or other identifying information based on the correlation so that network threat intelligence can be applied to recognize malicious packets. *See, e.g., id.* at 12:54-60. This can prevent other packets with the same threats from further damaging the network.

2. Non-Technical Description of United States Patent No. 10,193,917

39. The '917 Patent provides, among other things, improved techniques to combat constantly evolving threats in computer networks using a processor and memory of a packet-filtering device to receive packets, apply packet-filtering rules that either allow or block the packets to a destination, generate a packet log entry comprising a threat indicator, update the packet flow entry using the packet log entry and the packet flow analysis, communicate and display a portion of the packet flow analysis, such that the packet flow analysis data comprises at least on threat identifier, packet time data, and data whether the packet-filtering device blocked the packets. Ex. 2 ('917 Patent) at 1:28-33. The '917 Patent provides techniques for inspecting and monitoring network traffic information based on threat indicators. *See, e.g., id.* at 1:44-2:10. The threat indicators are based on network threat intelligence information received from various sources. The '917 Patent describes systems that are able to provide real-time monitoring and logging capacities based on network threat intelligence information and allow a user to observe the real-time traffic and customize the company's policy on the management tool in response to the real-time observations. *See, e.g., id.* at FIGs. 6A-6G, 1:64-

2:10, 8:1-32. The management tool can cause updates by the packet-filtering device, which automatically updates the rules for subsequent network traffic. *See, e.g., id.* at 13:29-43.

3. Non-Technical Description of United States Patent No. 10,284,526

40. The '526 Patent describes improvements to computer network security, particularly when dealing with encrypted network traffic, including a processor and memory for storing a list of identification data and corresponding action to perform on encrypted communication flows, receive packets that initiate at least one encrypted communication flow, identify flow identification data associated with packets initiating the encrypted packet flow, comparing the identified flow identification data with the list of identification data, decrypting the encrypted communication flows matching identification data to perform an action on each packet, and then re-encrypt the packets. Ex. 2 ('526 Patent) at 1:13-17. The '526 Patent describes that “[t]ypically, an SSL/TLS proxy decrypts all of the SSL/TLS-secured communications passing through it; but this may be undesirable and inefficient because of, for example, computational resource issues, network performance issues, management complexity issues, and/or privacy protection issues.” *Id.* at 1:35-40; 4:66-5:32. The '526 Patent addresses these issues by providing techniques for selectively decrypting encrypted communications, which for example, include the use of network threat intelligence information. *Id.* at 1:53-2:44, 5:33-43.

C. Licensees under Each Asserted United States Patent

41. Keysight licensed the Asserted Patents from Centripetal from October 9, 2018 through December 31, 2021 under a three-year term license. Ex. 48C. The license required Keysight to pay Centripetal a continuing royalty on hardware and software products, including VisionONE, Vision 7300, Vision 7303, with AppStack and SecureStack on the hardware, ThreatARMOR, and BreakingPoint with ATI. *Id.* However, the parties have been involved in

a still ongoing arbitration regarding Keysight's failure to pay royalties to Centripetal as required under the license. The license expired on January 1, 2022. *Id.*

42. Other than the expired license to Keysight as set forth immediately above, the Asserted Patents have not been licensed.

D. Foreign Patents and Applications

43. In accordance with Commission Rule 210.12(a)(9)(v), a listing of known foreign patents, foreign patent applications (not already issued as a patent) and foreign patent applications that have been denied, abandoned or withdrawn that may correspond to each Asserted Patent are provided below:

United States Asserted Patents	Foreign Patents or Publ./Appl. in the Same Family	Status	Litigation
9,264,370	EP 3257202 B1	Granted	Infringement case with Cisco was dismissed by Dusseldorf District Court in Germany and is on appeal at Dusseldorf Court of Appeal. Infringement cases with Palo Alto Networks and Keysight are pending before Munich District Court I in Germany. Nullity proceeding brought by Cisco and Palo Alto Networks is pending before the Federal Patent Court in Germany.
	AU2015382393	Granted	
	CA30141650	Pending	
10,193,917	EP 3557844 A1	Pending	
	EP 3284238 B1	Granted	Infringement case with Palo Alto Networks was withdrawn from the Dusseldorf District Court. Infringement case with Keysight is pending before Munich District Court I in Germany.
	DE202016009026	Pending	
	DE202016009028	Pending	
	DE202016009029	Pending	
	AU2016247760	Lapsed	

10,284,526	AU2020202148	Lapsed	
	CA3021054	Pending	
	EP 3659316 A1	Pending	
	AU2018307756	Pending	
	CN111034150	Pending	
	CA3069971	Pending	

44. Centripetal is not aware of any other foreign patents or applications corresponding to the Asserted Patents that remain pending or have been denied, abandoned, or withdrawn.

IV. UNFAIR ACTS OF PROPOSED RESPONDENT

45. Keysight has engaged in and will continue to engage in unlawful and unfair acts including the importation into the United States, sale for importation into the United States, and/or sale within the United States after importation of Accused Products that infringe the Asserted Claims.

46. On information and belief, Keysight maintains a significant inventory of the Network Visibility Products and ThreatArmor Products in the United States. On information and belief, Keysight has significant operations in the United States related to the Network Visibility Products and ThreatArmor Products.

47. Keysight is and will continue importing into the United States, selling for importation into the United States, and/or selling after importation into the United States network security products with threat intelligence technologies, related software, components thereof, and products containing same, as further described in Section V below.

A. Infringement of United States Patent No. 9,264,370

48. As described more fully in Section V, *infra*, Keysight imports into the United States, sells for importation into the United States, and/or sells within the United States after importation the Network Visibility Products that infringe the '370 Patent.

49. The Network Visibility Products infringe, directly and indirectly, at least claims 22, 23, 24, 25, 26, 27, 42, 43, 44, 45, 46, 47, 48, and 63 of the '370 Patent (the "'370 Asserted Claims"). Keysight directly and indirectly infringes these claims by importing into the United States, selling for importation into the United States, and/or selling after importation into the United States the Network Visibility Products. *See* Ex. 21 (infringement chart for the '370 Patent). The Network Visibility Products, at the time of importation, meet all limitations of the '370 Asserted Claims, are programmed to dictate the performance of and perform all steps of the method claims of the '370 Asserted Claims (claims 64, 73, and 75 are method claims), and/or are designed and programmed to comprise or be incorporated into the systems and devices and to be used in the methods in the '370 Asserted Claims. Keysight directly infringes these claims by importing the Network Visibility Products into the United States, selling the Network Visibility Products for importation into the United States, and/or selling the Network Visibility Products after importation into the United States.

50. Keysight has induced infringement of the '370 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring its customers, users, and/or vendors to perform one or more of the steps of the asserted method claims, or create all the elements of a system claim or computer readable medium claim, which infringe the '370 Asserted Claims, either literally or under the doctrine of equivalents. All elements of the claims are practiced by either Keysight, its customers, users, and vendors, or some combination thereof. As one example, Keysight instructs, directs and/or requires its customers, users, and vendors to configure a network security system as described above for direct infringement, including by using computing devices with processors and memory, to meet one or more elements of a '370 Asserted Claim. Keysight instructs, directs and/or requires its customers, users, and vendors,

or some combination thereof, to set up the network security system to identify packets and generate log entries. For example, the log entries may be provided to the Network Visibility Products for correlation and updates. As a further example, Keysight instructs, directs and/or requires its customers, users, and vendors, or some combination thereof, to obtain and activate subscriptions (such as Keysight's ATI subscription) and functions within the Network Visibility Products, to perform one or more steps in the asserted method claims of the '370 Patent. Keysight has known or has been willfully blind to the fact that it is inducing others to infringe one or more claims of the '370 Patent.

51. Keysight has knowingly and actively aided and abetted the direct infringement of the '370 Patent by instructing and encouraging its customers, users, and vendors to meet the elements of the '370 Patent with the Network Visibility Products. Such use is consistent with how the products are described to directly infringe the '370 Patent and how they are intended to be used, as described above and incorporated by reference here. Keysight's specific intent to encourage infringement includes, but is not limited to: advising its customers and users to use the Network Visibility Products in an infringing manner through direct communications via training, support services, or sales calls, thereby providing a mechanism through which third parties may infringe; by advertising and promoting the use of the Network Visibility Products in an infringing manner; and distributing guidelines and instructions on how to setup the Network Visibility Products in an infringing manner. To the extent Keysight's customers, users, and vendors direct and control the systems and methods in the claims, Keysight benefits by controlling the system as a whole.

52. Keysight updates and maintains a support website that includes technical documentation encouraging the use of the Network Visibility Products in an infringing manner.

See, e.g., Ex. 49 (<https://www.keysight.com/us/en/support.html>); Ex. 50 (https://support.keysight.com/s/?language=en_US); Ex. 51 (<https://support.ixiacom.com/>).

This technical documentation includes knowledge articles, videos, user guides, technical support articles, and knowledge center that cover the operation of the Network Visibility Products in-depth, including by advertising the Network Visibility Products' infringing security features and instructing customers, users, and vendors to configure and use the Network Visibility Products in an infringing manner. *Id.*

53. Keysight contributorily infringes the '370 Patent pursuant to 35 U.S.C. § 271(c) because it has provided its Network Visibility Products as software and computer systems with software installed, and these act as a material component of claims of the '370 Patent when combined with other components to create a complete network security system. As a former licensee of the '370 Patent, Keysight knows that the Network Visibility Products are especially made to be used in a manner that infringes the '370 Patent. The Network Visibility Products and their associated software are specialized security products, and, as such, are not staple articles or commodities of commerce. Keysight has known or has been willfully blind to the fact that it is contributing to the infringement of one or more claims of the '370 Patent.

54. Keysight has knowingly and actively contributed to the direct infringement of the '370 Patent by its manufacture, use, offer to sell, sale and importation of the Network Visibility Products that its customers, users, and vendors use to meet all the elements of the '370 Asserted Claims, as described above and incorporated by reference here. To the extent any of the Network Visibility Products are sold as software, this software is a material component that can be combined with other hardware components, such as processors and memory, to create an infringing system. Furthermore, Keysight's customers, users, and

vendors also directly infringe these claims jointly with Keysight, to the extent specific components are provided by those third parties. To the extent Keysight's customers, users, and vendors direct and control the infringing systems and methods in the claims, Keysight benefits from the control of the infringing system as a whole. For example, Keysight can use the information in the logs or the results of the correlations to identify hosts associated with a malicious entity. This information can be provided to other Keysight's products or to the ATI research center which will generate threat intelligence benefiting Keysight's other accused and unaccused products. Keysight and its customers, users, and vendors put the systems and methods described in the claims into service to the benefit of Keysight's ability to provide security and protection and identify threats across its customer base.

55. Keysight has known or, in the alternative, has been willfully blind to Centripetal's technology and the '370 Patent. At minimum, Keysight has become aware of its indirect infringement because of this Complaint. Centripetal is informed and believes that Keysight has undertaken no efforts to design these products or services around the '370 Patent to avoid infringement despite Keysight's knowledge and understanding that its products and services infringe the '370 Patent.

56. Exhibit 21 contains an exemplary claim chart mapping the Network Visibility Products to all asserted claims of the '370 Patent.

B. Infringement of United States Patent No. 10,193,917

57. As described more fully in Section V, *infra*, Keysight imports into the United States, sells for importation into the United States, and/or sells within the United States after importation the ThreatArmor Products that infringe the '917 Patent.

58. The ThreatArmor Products infringe, directly and indirectly, at least Claims 1, 5, 11, 15, and 20 of the '917 Patent (the "'917 Asserted Claims"). Keysight directly and

indirectly infringes these claims by importing into the United States, selling for importation into the United States, and/or selling after importation into the United States the ThreatArmor Products. *See* Ex. 22 (infringement chart for the '917 Patent). The ThreatArmor Products, at the time of importation, meet all limitations of '917 Asserted Claims, are programmed to dictate the performance of and perform all steps of the method claims of the '917 Asserted Claims (claims 1 and 5 are method claims), and/or are designed and programmed to comprise or be incorporated into the systems and devices and to be used in the methods in the '917 Asserted Claims. Keysight directly infringes these claims by importing the ThreatArmor Products into the United States, selling the ThreatArmor Products for importation into the United States, and/or selling the ThreatArmor Products after importation into the United States.

59. Keysight has induced infringement of the '917 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring its customers, users, and/or vendors to perform one or more of the steps of the method claims, or create all the elements of a system claim or computer readable medium claim, either literally or under the doctrine of equivalents. All the elements of the claims are used by either Keysight, its customers, users, and vendors, or some combination thereof. As one example, Keysight instructs, directs and/or requires its customers, users, and vendors to configure a system as described above for direct infringement, including by using computing devices with processors and memory to meet one or more elements of a '917 Asserted Claim. Keysight instructs, directs and/or requires its customers, users, and vendors to set up the system where ThreatArmor Products cause another device, such as a user device, a SIEM system, ThreatArmor Central Management to display packet analysis information. Keysight has known or has been willfully blind to the fact that it is inducing others to infringe one or more claims of the '917 Patent.

60. Keysight has knowingly and actively aided and abetted the direct infringement of the '917 Patent by instructing and encouraging its customers, users, and vendors to meet the elements of the '917 Patent with the ThreatArmor Products. Such use is consistent with how the products are described to directly infringe the '917 Patent and how they are intended to be used, as described above and incorporated by reference here. Keysight's specific intent to encourage infringement includes, but is not limited to: advising its customers and users to use the ThreatArmor Products in an infringing manner through direct communications via training, support services, or sales calls, thereby providing a mechanism through which third parties may infringe; by advertising and promoting the use of the ThreatArmor Products in an infringing manner; and distributing guidelines and instructions on how to setup the ThreatArmor Products in an infringing manner. To the extent Keysight's customers, users, and vendors direct and control the systems and methods in the claims, Keysight benefits from the control of the system as a whole.

61. Keysight updates and maintains a support website that includes technical documentation encouraging the use of the ThreatArmor Products in an infringing manner. This technical documentation includes knowledge articles, videos, user guides, technical support articles, and knowledge center that cover the operation of the ThreatArmor Products in-depth, including by advertising the ThreatArmor Products' infringing security features and instructing customers, users, and vendors to configure and use the ThreatArmor Products in an infringing manner. *See, e.g.*, Ex. 49 (<https://www.keysight.com/us/en/support.html>); Ex. 50 (https://support.keysight.com/s/?language=en_US); Ex. 51 (<https://support.ixiacom.com/>).

62. Keysight contributorily infringes the '917 Patent pursuant to 35 U.S.C. § 271(c) because it has provided its ThreatArmor Products as software and computer systems with

software installed, and these act as a material component of claims of the '917 Patent when combined with other components to create a complete network security system. Keysight knows that its ThreatArmor Products are especially made to be used in a manner that infringes the '917 Patent. The ThreatArmor Products and their associated software are specialized security products, and, as such, are not staple articles or commodities of commerce. Keysight has known or has been willfully blind to the fact that it is contributing to the infringement of one or more claims of the '917 Patent.

63. Keysight has knowingly and actively contributed to the direct infringement of the '917 Patent by its manufacture, use, offer to sell, sale and importation of the ThreatArmor Products that its customers, users, and vendors use to meet the elements of the '917 Patent, as described above and incorporated by reference here. To the extent any of the Network Visibility Products are sold as software, this software is a material component that can be combined with other hardware components, such as processors and memory, to create an infringing system. Furthermore, Keysight's customers, users, and vendors also directly infringe these claims jointly with Keysight, to the extent specific components are provided by those third parties. To the extent Keysight's customers, users, and vendors direct and control the systems and methods in the claims, Keysight benefits from the control of the system as a whole. Keysight and its customers, users, and vendors put the systems and methods described in the claims into service to the benefit of Keysight's ability to provide security and protection and identify threats across its customer base.

64. Keysight has known or, in the alternative, has been willfully blind to Centripetal's technology and the '917 Patent. At minimum, Keysight has become aware of its indirect infringement because of this Complaint. Centripetal is informed and believes that

Keysight has undertaken no efforts to design these products or services around the '917 Patent to avoid infringement despite Keysight's knowledge and understanding that its products and services infringe the '917 Patent.

65. Exhibit 22 contains an exemplary claim chart mapping the ThreatArmor Products to all asserted claims of the '917 Patent.

C. Infringement of United States Patent No. 10,284,526

66. As described more fully in Section V, *infra*, Keysight imports into the United States, sells for importation into the United States, and/or sells within the United States after importation the Network Visibility Products that infringe the '526 Patent.

67. The Network Visibility Products infringe, directly and indirectly, at least Claims 1, 2, 3, 6, 11, 12, 13, and 16 of the '526 Patent (the "'526 Asserted Claims"). Keysight directly and indirectly infringes these claims by importing into the United States, selling for importation into the United States, and/or selling after importation into the United States the Network Visibility Products. *See* Ex. 23 (infringement chart for the '526 Patent). The Network Visibility Products, at the time of importation, meet all limitations of '526 Asserted Claims, are programmed to dictate the performance of and perform all steps of the method claims of the '526 Asserted Claims (claims 1, 2, 3, and 6 are method claims), and/or are designed and programmed to comprise or be incorporated into the systems and devices and to be used in the methods in the '526 Asserted Claims. Keysight directly infringes these claims by importing the Network Visibility Products into the United States, selling the Network Visibility Products for importation into the United States, and/or selling the Network Visibility Products after importation into the United States.

68. Keysight has induced infringement of the '526 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring its customers, users, and/or vendors to perform

one or more of the steps of the method claims, or create all the elements of a system claim or computer readable medium claim, either literally or under the doctrine of equivalents. All the elements of the claims are used by either Keysight, its customers, users, and vendors, or some combination thereof. As one example, Keysight instructs, directs and/or requires its customers, users, and vendors to configure a system as described above for direct infringement, including by using computing devices with processors and memory to meet one or more elements of an '526 Asserted Claim. Keysight instructs, directs and/or requires its customers, users, and vendors to obtain and activate subscriptions (such as Keysight's ATI subscription) and functions (such as the inline decryption feature) to perform one or more steps in the claims of the '526 Patent. Keysight has known or has been willfully blind to the fact that it is inducing others to infringe one or more claims of the '526 Patent.

69. Keysight has knowingly and actively aided and abetted the direct infringement of the '526 Patent by instructing and encouraging its customers, users, and vendors to meet the elements of the '526 Patent with the Network Visibility Products. Such use is consistent with how the products are described to directly infringe the '526 Patent and how they are intended to be used, as described above and incorporated by reference here. Keysight's specific intent to encourage infringement includes, but is not limited to: advising its customers and users to use the Network Visibility Products in an infringing manner through direct communications via training, support services, or sales calls, thereby providing a mechanism through which third parties may infringe; by advertising and promoting the use of the Network Visibility Products in an infringing manner; and distributing guidelines and instructions on how to setup the Network Visibility Products in an infringing manner. To the extent Keysight's customers, users, and vendors direct and control the systems and methods in the claims, Keysight benefits

from the control of the system as a whole.

70. Keysight updates and maintains a support website that includes technical documentation encouraging the use of the Network Visibility Products in an infringing manner. This technical documentation includes knowledge articles, videos, user guides, technical support articles, and knowledge center that cover the operation of the Network Visibility Products in-depth, including by advertising the Network Visibility Products' infringing security features and instructing customers, users, and vendors to configure and use the Network Visibility Products in an infringing manner. *See, e.g.*, Ex. 49 (<https://www.keysight.com/us/en/support.html>); Ex. 50 (https://support.keysight.com/s/?language=en_US); Ex. 51 (<https://support.ixiacom.com/>).

71. Keysight contributorily infringes the '526 Patent pursuant to 35 U.S.C. § 271(c) because it has provided its Network Visibility Products as software and computer systems with software installed, and these act as a material component of claims of the '526 Patent when combined with other components to create a complete network security system. Keysight knows that its Network Visibility Products are especially made to be used in a manner that infringes the '526 Patent. The Network Visibility Products and their associated software are specialized security products, and, as such, are not staple articles or commodities of commerce. Keysight has known or has been willfully blind to the fact that it is contributing to the infringement of one or more claims of the '526 Patent.

72. Keysight has knowingly and actively contributed to the direct infringement of the '526 Patent by its manufacture, use, offer to sell, sale and importation of the Network Visibility Products that its customers, users, and vendors use to meet the elements of the '526 Patent, as described above and incorporated by reference here. To the extent any of the

Network Visibility Products are sold as software, this software is a material component that can be combined with other hardware components, such as processors and memory, to create an infringing system. Furthermore, Keysight's customers, users, and vendors also directly infringe these claims jointly with Keysight, to the extent specific components are provided by those third parties. For example, Keysight sold software and/or hardware for performing inline decryption (and re-encryption) and which is a material component that can be combined with other components, such as Keysight's Threat Insight to create an infringing system. To the extent Keysight's customers, users, and vendors direct and control the systems and methods in the claims, Keysight benefits from the control of the system as a whole. Keysight and its customers, users, and vendors put the systems and methods described in the claims into service to the benefit of Keysight's ability to provide security and protection and identify threats across its customer base.

73. Keysight has known or, in the alternative, has been willfully blind to Centripetal's technology and the '526 Patent. At minimum, Keysight has become aware of its indirect infringement because of this Complaint. Centripetal is informed and believes that Keysight has undertaken no efforts to design these products or services around the '526 Patent to avoid infringement despite Keysight's knowledge and understanding that its products and services infringe the '526 Patent.

74. Exhibit 23 contains an exemplary claim chart mapping the Network Visibility Products to all asserted claims of the '526 Patent.

V. SPECIFIC INSTANCES OF UNFAIR IMPORTATION AND SALE

75. Keysight, either itself or through affiliates or third parties acting on behalf of Keysight, is and will continue to engage in the importation into the United States, sale for importation into the United States, and/or sale after importation into the United States of the

Accused Products. The Accused Products are manufactured outside of the United States and imported for sale into the United States as described in detail below.

76. Keysight has disclosed public information regarding the manufacture and importation of the Accused Products, establishing that they are both developed and manufactured abroad and then imported into the United States for sale. The Accused Products are part of Keysight's network test, visibility and security products, which Keysight researches and develops abroad in Bucharest, Romania. Ex. 45 at 47. Keysight then manufactures these products in its facility in Penang, Malaysia which are intended for sale within the United States, as Keysight specific states that "Malaysia" is the country of origin for its Network Visibility Products in its product documentation.



Ex. 42 (<https://www.keysight.com/us/en/assets/3120-1029/data-sheets/Vision-X-Network-Packet-Broker.pdf>) at 9 (Keysight datasheet listing the Vision X's country of origin as Malaysia).

77. Keysight sells and has sold the Accused Products in the United States after importation from its manufacturing facilities in Malaysia as shown on its website, where Accused Products are available for sale to United States customers. For example, the website includes descriptions of the Keysight's Network Visibility Products that are for sale from Keysight. See, e.g., Ex. 24 (<https://www.keysight.com/us/en/products/network-visibility/network-packet-brokers.html>); Ex. 56 (<https://www.keysight.com/us/en/products/network-visibility/network-packet-brokers/tradevision.html>); Ex. 57 (<https://www.keysight.com/us/en/products/network-visibility/network-packet-brokers/tradevision.html>); Ex. 57 (<https://www.keysight.com/us/en/products/network-visibility/network-packet-brokers/tradevision.html>).

[security.html](#)). The website also includes descriptions of the ThreatArmor Products that are for sale from Keysight. *See, e.g.*, Ex. 19 (<https://www.keysight.com/us/en/products/network-security/breach-defense/threat-armor.html>). Keysight also sells to customers in the United States, as it includes on its United States website a sales form that allows a customer to request an Accused Products for purchase:

A screenshot of a web form element. At the top, the text "Country or Area *" is displayed in a small, dark font. Below this is a rectangular dropdown menu with a light gray border. Inside the menu, the text "United States" is visible in a dark font. To the right of the text, there is a small, dark downward-pointing arrow icon.

Ex. 58 (<https://www.keysight.com/us/en/contact/support/sales-request.html>).

78. Keysight has also established in numerous press releases that manufacturing and order fulfillment occurs from its Penang, Malaysia facility. *See*, Ex. 46 (<https://about.keysight.com/en/newsroom/pr/2017/06nov-nr17090.shtml>) (“Business continues as usual at Keysight's other 145 worldwide locations, including its primary manufacturing and order fulfillment location in Penang, Malaysia.”); *see also* Ex. 55 at 6 (“Keysight has a central order fulfillment organization that supplies solutions to customers across geographies. Our Penang, Malaysia site is our largest manufacturing facility, with a proven track record of operational excellence, technology capability and quality. We have an established network of suppliers and subcontractors, especially in Asia, that complements our in-house capabilities.”). The Accused Products are also available in the United States after importation from third party resellers. For example, the Network Visibility Products can be purchased directly from third-party reseller CDW Corporation. Ex. 59 (<https://www.cdw.com/product/ixia-vision-one-with-fixed-48-port-sfp/5071631>). As an additional example, Network Visibility Products can be purchased from third-party reseller Insight. Ex. 60 (https://www.insight.com/en_US/shop/product/SYS-V1-48PX-AC/IXIA/SYS-V1-48PX-

AC/Ixia-Vision-ONE-SYS-V1-48PX-AC---security-appliance/). Additionally, the ThreatArmor Products can be purchased from the United States website of SHI. Ex. 61 (<https://www.shi.com/Products/ProductDetail.aspx?SHISystemID=ShiCommodity&ProductId=entity=34887184>). In addition, the ThreatArmor Products are also available for purchase from the United States website of DeltaTech. Ex. 62 (<https://www.deltatechsol.com/ixia-threatarmor-1g-threatarmor-1gbe-security-appliance-with-4-1gb-sfp-ports-requires-active-ati/>).

79. A specific example of Keysight shipping the Accused Products from its facility in Penang, Malaysia to a customer in the United States, is when Complainant purchased a ThreatArmor device and the shipping label established that Keysight makes ThreatArmor in Malaysia and then ships it from this location to customers in the United States. This ThreatArmor product was purchased via GuidePoint Security, LLC in Herndon, Virginia. Ex. 82. As shown by the label in the photos below, ThreatArmor was made in Malaysia and shipped from Malaysia into the United States.



Keysight Order Number: 4243295
Keysight Certificate Number: YB64-RM48

Software Entitlement Certificate

This certificate is evidence of the entitlement for the products listed below. If you are receiving this certificate as part of a new instrument order, some or all of the licenses may have been pre-installed on the instrument.

Product	Description	Quantity
991-0111-02	IXIA ThreatARMOR 1G Security Appliance with 4 1Gb SFP ports Multi-Mode Activation Code: DD19-E5CA-4937-1160	1
909-4010	Ixia Annual Subscription for Application and Threat Intelligence (ATI) for 1G ThreatARMOR. Includes Essential Support	1
993-0083-03	IXIA Annual Subscription for Application and Threat Intelligence (ATI) for 1G ThreatARMOR Activation Code: 83FD-00D6-8262-E547	1
909-4010	Ixia Annual Subscription for Application and Threat Intelligence (ATI) for 1G ThreatARMOR. Includes Essential Support	1

INSTRUCTIONS:

- If your equipment on which the license is to be installed is online (can access the internet either directly or via proxy), please use the activation or entitlement code in your e-delivery email to activate and install your licenses using the Licensing utility for your application.
- If your equipment on which the license is to be installed is offline (cannot access the internet either directly or via proxy), a license file needs to be generated manually using the following steps:
 - Log into Keysight's licensing website at www.keysight.com/find/softwaremanager to redeem your license:
 - First time users will need to create a new account.
 - To create a new account, you will need your Keysight Order Number and Keysight Certificate number from the top of this certificate.
 - Returning users will need to login using their existing credentials.
 - A returning user can add new certificates.
 - To generate your license, you will:
 - Need to Request a new license file ("You can request new licenses")
 - Need Your 'Request File' which can be obtained from the Licensing utility for your application.

If you have any questions, please contact your local support representative, or visit the Support Website at www.ixiacom.com/support

Rights and restrictions on the use, transfer, and copying of the Software are set forth in Keysight Technologies' Software License agreement.

CID: 5797

Made in MALAYSIA

Page 1 of 1



5972-4004

Ex. 80.



Ex. 81.

80. Further showing that Keysight's products are imported for sale in the United States, Centripetal purchased a Vision One in the United States as a representative product of the Network Visibility Products. This Vision One was purchased from Caegis Solutions in Chantilly, Virginia. Ex. 63 (Invoice). As shown by the label in the photo below, Vision One was assembled in Malaysia. On information and belief, Keysight has not changed its supply chain between when the time this device was purchased and when Keysight's license of certain products expired on January 1, 2022. Furthermore, on information and belief the supply chain for all the Accused Products is the same.



Ex. 47.

81. These specific instances of importation and sale set forth above are representative examples of Keysight's unlawful importation, sale for importation, and/or sale

within the United States after importation of the Accused Products. Centripetal believes that discovery will reveal other specific acts of Keysight's sale for importation, importation, and/or sale after importation of Accused Products that infringe the Asserted Patents.

82. On information and belief, the Harmonized Tariff Schedule ("HTS") of the United States item number under which the Accused Products may be imported into the United States and classified under includes at least the following heading of HTS 8517. This HTS number is intended for illustration only and is not exhaustive of the products accused of infringement in this Complaint. The HTS number is not intended to limit the scope of this Investigation or any exclusion order or other remedy ordered by the Commission.

VI. BRIEF SUMMARY OF AGENCY OR COURT LITIGATION

83. The Asserted Patents have not been the subject of any ITC litigation.

84. The Asserted Patents are currently asserted against Keysight in a co-pending patent infringement suit filed on January 1, 2022, before the Eastern District of Virginia. *Centripetal Networks, Inc. v. Keysight Technologies, Inc.*, Case No. 2:22-cv-00002 (E.D. Va.) (*Keysight II*).

85. In addition to *Keysight II*, the '370 Patent was asserted against Keysight in *Centripetal Networks, Inc. v. Keysight Technologies, Inc. and IXIA*, Case No. 2:17-cv-00383 (E.D. Va.) ("*Keysight I*"). In *Keysight I*, Centripetal alleged that Keysight infringed the '370 Patent, among other patents which are not asserted here. Keysight denied infringement and asserted various defenses and counterclaims. The parties served their respective expert reports in *Keysight I* and the case went to trial. The parties then settled the case in the middle of trial, after Centripetal began its case in chief, but before Keysight presented its case. Subsequently, the parties submitted a joint stipulation of dismissal, which dismissed the *Keysight I* case without prejudice. *Centripetal Networks, Inc. v. Keysight Technologies, Inc. and IXIA*, Case

No. 2:17-cv-00383, Dkt. No. 589 (E.D. Va. October 11, 2018).

86. The '370 Patent is in the same patent family as United States Patent Nos. 9,560,176 (the "'176 Patent"), 10,530,903 (the "'903 Patent"), 10,659,573 (the "'573 Patent"), and 10,931,797 (the "'797 Patent"), which have been the subject of proceedings before United States District Court for the Eastern District of Virginia and the PTAB. Specifically, the '176 Patent was asserted against Cisco Systems, Inc. in the Eastern District of Virginia on February 13, 2018. *Centripetal Networks, Inc., v. Cisco Systems, Inc.*, Case No. 2:18-cv-00094-HCM-LRL (E.D. Va.) (the "*Cisco Case*"). Following a bench trial, the Court determined that the '176 Patent is infringed and valid. *Centripetal Networks, Inc., v. Cisco Systems, Inc.*, Case No. 2:18-cv-00094-HCM-LRL, Dkt. No. 621 (E.D. Va. Oct. 5, 2020); *Id.*, Dkt. No. 638 (E.D. Va. March 17, 2021). The *Cisco Case* is currently on appeal before the Federal Circuit. *Centripetal Networks, Inc. v. Cisco Systems, Inc.*, Case No. 2021-1888 (Fed. Cir.). Cisco also filed two IPRs on the '176 Patent on September 17, 2018, and the PTAB denied institution in both IPRs. *Cisco Systems, Inc. v. Centripetal Networks, Inc.*, IPR2018-01654, -01655 (P.T.A.B.) While Centripetal has not asserted the '176 Patent against Palo Alto Networks, Palo Alto Networks filed an IPR on the '176 Patent on September 15, 2021, which the PTAB denied institution. *Palo Alto Networks, Inc. v. Centripetal Networks, Inc.*, IPR2021-01521, Paper 23 (P.T.A.B. March 24, 2022). The '903, '573, and '797 Patents are currently in a patent infringement litigation against Palo Alto Networks in the Eastern District of Virginia. *Centripetal Networks, Inc. v. Palo Alto Networks, Inc.*, Case No. 2:21-cv-00137-RCY (E.D. Va.) (the "*PAN Case*"). The *PAN Case* was filed on March 12, 2021, and is currently stayed. Subsequent to the filing of the *PAN Case*, Palo Alto Networks filed IPRs on the '903 and '573 Patents on July 20, 2021, and filed a PGR on the '797 Patent on August 3, 2021. *Palo Alto*

Networks, Inc. v. Centripetal Networks, Inc., IPR2021-01150, -01151 (P.T.A.B.); *Id.*, PGR2021-00108 (P.T.A.B.). The PTAB denied institution for the '573 and '797 Patents and issued an institution decision for the '903 patent. The '573 Patent is also asserted in *Keysight II*.

87. The '917 Patent is in the same patent family as the following patents which have been the subject of proceedings before the PTAB or the United States District Court for the Eastern District of Virginia: United States Patent Nos. 9,413,722 (the "'722 Patent"), 10,542,028 (the "'028 Patent"), 10,567,413 (the "'413 Patent"), 10,609,062 (the "'062 Patent), and 10,757,126 (the "'126 Patent"). The '722 Patent was asserted in *Keysight I*, which settled during trial. *Centripetal Networks, Inc. v. Keysight Technologies, Inc. and IXIA*, Case No. 2:17-cv-00383 (E.D. Va.). The '722 Patent was also initially asserted in the *Cisco Case* on February 13, 2018, but was not part of the bench trial. *See Centripetal Networks, Inc., v. Cisco Systems, Inc.*, Case No. 2:18-cv-00094-HCM-LRL (E.D. Va.). Cisco filed an IPR on the '722 Patent on September 18, 2018, where the PTAB found that the '722 Patent is unpatentable. *Cisco Systems, Inc. v. Centripetal Networks, Inc.*, IPR2018-01760 (P.T.A.B.). The Federal Circuit affirmed the PTAB's decision. *Centripetal Networks, Inc. v. Cisco Sys., Inc.*, 847 F. App'x 881, 882 (Fed. Cir. Mar. 10, 2021), *cert. denied*, 142 S. Ct. 240 (2021). The '062 Patent is asserted in *Keysight II* and is not currently subject to any agency litigation. *Centripetal Networks, Inc. v. Keysight Technologies, Inc.*, Case No. 2:22-cv-00002 (E.D. Va.). The '028, '413, and '126 Patents are in the *PAN Case*, which is currently stayed. *Centripetal Networks, Inc. v. Palo Alto Networks, Inc.*, Case No. 2:21-cv-00137-RCY (E.D. Va.). PAN also filed IPRs on the '028, '126, and '413 Patents, where the PTAB has instituted the IPRs but has not issued final written decisions. *Palo Alto Networks, Inc. v. Centripetal Networks, Inc.*,

IPR2021-01147, -01148, -01149 (P.T.A.B.). The '028 and '126 Patents were also in litigation between Centripetal and Looking Glass filed on September 14, 2021 in the Eastern District of Virginia. *Centripetal Networks Inc., v. LookingGlass Cyber Solutions, Inc., et. al.*, Case No. 3:21-cv-00597-DJN (E.D. Va.). This action was voluntarily dismissed on December 13, 2021.

88. The table below summarizes litigation of the Asserted Patents.

Asserted Patent	Litigation	Status
The '370 Patent	<i>Centripetal Networks, Inc. v. Keysight Technologies, Inc. and IXIA</i> , Case No. 2:17-cv-00383 (E.D. Va.) (“Keysight I”)	Terminated
	<i>Centripetal Networks, Inc. v. Keysight Technologies, Inc.</i> , Case No. 2:22-cv-00002 (E.D. Va.) (“Keysight II”)	Pending
The '917 Patent	Keysight II	Pending
The '526 Patent	Keysight II	Pending

89. The table below summarizes litigation of the United States patents that are in the same patent family as the asserted '370 Patent.

United States Family Member	Litigation	Status
9,560,176	<i>Centripetal Networks, Inc., v. Cisco Systems, Inc.</i> , Case No. 2:18-cv-00094-HCM-LRL (E.D. Va.) (Cisco Case). <i>Centripetal Networks, Inc. v. Cisco Systems, Inc.</i> , Case No. 2021-1888 (Fed. Cir.). <i>Cisco Systems, Inc. v. Centripetal Networks, Inc.</i> , IPR2018-01654, -01655 (P.T.A.B.). <i>Palo Alto Networks, Inc. v. Centripetal Networks, Inc.</i> , IPR2021-01521 (P.T.A.B.).	Final judgment of infringement and validity in the Cisco Case, which is currently on appeal at the Federal Circuit. The IPRs have all been denied institution.
10,530,903	<i>Centripetal Networks, Inc. v. Palo Alto Networks, Inc.</i> , Case No. 2:21-cv-00137-RCY (E.D. Va.) (PAN Case).	The PAN Case is stayed. The IPR is instituted and is pending.

	<i>Palo Alto Networks, Inc. v. Centripetal Networks, Inc.</i> , IPR2021-01150 (P.T.A.B.).	
10,659,573	PAN Case Keysight II <i>Palo Alto Networks, Inc. v. Centripetal Networks, Inc.</i> , IPR2021-01151 (P.T.A.B.).	The PAN Case is stayed. Keysight II is pending. The IPR has been denied institution.
10,931,797	PAN Case <i>Palo Alto Networks, Inc. v. Centripetal Networks, Inc.</i> , PGR2021-00108 (P.T.A.B.).	The PAN Case is stayed. The PGR has been denied institution.

90. The table below summarizes litigation of the United States patents that are in the same patent family as the asserted '917 Patent.

United States Family Member	Litigation	Status
9,413,722	Keysight I Cisco Case <i>Cisco Systems, Inc. v. Centripetal Networks, Inc.</i> , IPR2018-01760 (P.T.A.B.). <i>Centripetal Networks, Inc. v. Cisco Sys., Inc.</i> , 847 F. App'x 881, 882 (Fed. Cir. Mar. 10, 2021), <i>cert. denied</i> , 142 S. Ct. 240 (2021).	Keysight I and Cisco Case are both terminated. The PTAB found the claims unpatentable which was affirmed by the Federal Circuit.
10,542,028	PAN Case <i>Palo Alto Networks, Inc. v. Centripetal Networks, Inc.</i> , IPR2021-01147 (P.T.A.B.). <i>Centripetal Networks Inc., v. LookingGlass Cyber Solutions, Inc., et. al.</i> , Case No. 3:21-cv-00597-DJN (E.D. Va.) (LookingGlass Case).	PAN Case is stayed. The IPR is instituted and is pending. LookingGlass Case is terminated.
10,567,413	PAN Case <i>Palo Alto Networks, Inc. v. Centripetal Networks, Inc.</i> , IPR2021-01149 (P.T.A.B.).	PAN Case is stayed. The IPR is instituted and is pending.

10,757,126	PAN Case <i>Palo Alto Networks, Inc. v. Centripetal Networks, Inc.</i> , IPR2021-01148 (P.T.A.B.). LookingGlass Case	PAN Case is stayed. The IPR is instituted and is pending. LookingGlass Case is terminated.
10,609,062	Keysight II	Pending

91. The '526 Patent does not have a patent family member that was or is in any United States litigation.

92. The unfair acts by Keysight and the subject matter thereof, as alleged in this Complaint, have not been the subject of any other litigation, except those set forth in this Complaint. The Asserted Patents have not been the subject of any other court or agency litigation, other than those set forth in the Complaint.

VII. DOMESTIC INDUSTRY

A. Technical Prong

93. There is a domestic industry, as defined under 19 U.S.C. § 1337(a)(3)(A), (B), and/or (C), comprising significant investments in plant and equipment and employment of labor and capital for manufacturing and production, maintenance, engineering, sales, testing, distribution, and R&D; and substantial investment in the exploitation of the Asserted Patents, including for engineering and R&D. Centripetal uses the inventions claimed in the Asserted Patents in its Domestic Industry Products and has made significant investments in domestic industry activities with respect to the CleanINTERNET® solutions, as set forth more fully in the accompanying Confidential Declaration of Jonathan Rogers (Exhibit 12C). The Domestic Industry Products that practice the Asserted Patents are the only products made or sold by Centripetal. Ex. 12C at ¶ 11.

94. Centripetal sells CleanINTERNET® solutions to customers, which are Threat

Intelligence Gateway systems that practice the Asserted Patents. *Id.* at ¶ 10. The Domestic Industry Products include Centripetal’s “RuleGATE®” systems, which are rack mounted computer systems that provide the most advanced strategy in network security today by practicing the technologies of the Asserted Patents. *Id.* The Domestic Industry Products generate and use cyber threat intelligence, or “CTI”, to catch and eradicate known and unknown threats. At a broad level, CTI is a collection of information about the myriad of different threats on the Internet. The Domestic Industry Products also report traffic information and perform cyber threat analysis on the traffic. *See id.* at ¶ 6.

95. Centripetal sells its Domestic Industry Products to customers, which practice the Asserted Patents. *See* Exs. 64C-66C (Domestic Industry Claim Charts).

96. The Domestic Industry Products practice at least Claim 43 of the ’370 Patent. The Domestic Industry Products have practiced claims of the ’370 Patent since before 2019 and still practice this patent. For example, the Domestic Industry Products receive updates to policies and rules, and generate log entries which can be used to perform correlations and rule updates. An exemplary claim chart comparing the Domestic Industry Products to Claim 43 of the ’370 Patent is attached as Exhibit 64C.

97. Centripetal’s Domestic Industry Products practice at least Claim 1 of the ’917 Patent. The Domestic Industry Products have practiced claims of the ’917 Patent when it was issued on January 29, 2019, and still practice this patent. For example, the Domestic Industry Products receive network packets, filter the packets with packet filtering rules, generate log entries, update packet flow entries, communicate and cause flow analysis data to be displayed. An exemplary claim chart comparing the Domestic Industry Products to Claim 1 of the ’917 Patent is attached as Exhibit 65C.

98. Centripetal's Domestic Industry Products practice at least Claim 1 of the '526 Patent. The Domestic Industry Products currently practice claims of the '526 Patent and practiced the '526 Patent since when the patent issued on May 7, 2019 and still practice the patent. For example, the Domestic Industry Products store a list of identification data and a corresponding action to be performed on encrypted network traffic, and filter the encrypted network traffic using such information. The Domestic Industry Products also decrypt packets in an encrypted flow if there is a match with the list of identification data and then re-encrypt the packets once an action is performed on those packets. An exemplary claim chart comparing the Domestic Industry Products to Claim 1 of the '526 Patent is attached as Exhibit 66C.

B. Economic Prong

99. Centripetal's investments and expenditures in a domestic industry for the Asserted Patents are significant, substantial, continuing, and on-going. Centripetal's United States R&D and engineering facilities are critical to their network security business.

1. Plant and Equipment

100. There is a domestic industry under Subsection (A) at least because Centripetal has made significant investments in equipment in the United States with respect to the Domestic Industry Products. Centripetal maintains extensive engineering and R&D facilities in the United States, including facilities in Reston, VA and Portsmouth, NH for the Domestic Industry Products. Ex. 12C (Rogers Decl.) at ¶ 11. The engineering and research and development facilities are used for all aspects of the operations necessary to make Centripetal's Domestic Industry Products, including, e.g., development, writing software, testing, and production activities to make the final Domestic Industry Products, and corporate overhead functions. See *id.* at ¶¶ 11, 14-15.

101. The R&D facilities are used for all aspects of engineering, research, and development, including design and testing of the Domestic Industry Products. *Id.* at ¶¶ 11, 14-15, 16. Centripetal has invested a significant amount of money in plant and equipment in order to undertake activities related to the Domestic Industry Products. *Id.* at ¶¶ 14-17.

2. Labor or Capital

102. There is a domestic industry under Subsection (B) at least because Centripetal has made significant investments in the employment of labor and capital in the United States with respect to the Domestic Industry Products. Centripetal has employed and continues to employ a workforce of 80 people in Reston, VA and Portsmouth, NH for the Domestic Industry Products. Ex. 12C (Rogers Decl.) at ¶19. These employees devote extensive time toward the production, maintenance, engineering, testing, customer support, sales and marketing, and R&D of the Domestic Industry Products. *Id.*. Centripetal has invested and continues to invest a significant amount of money in salaries, incentives, and other compensation and benefits for these employees and also make significant investments in operating expenses, capital expenditures, and material costs in the United States to support the work of these employees for the Domestic Industry Products. *Id.* at ¶¶ 17-19.

3. Exploitation of Patents

103. Centripetal makes extensive use of the inventions claimed in the Asserted Patents. The Domestic Industry Products are designed to practice the methods and incorporate the systems and devices claimed in the Asserted Patents. Centripetal has made substantial United States investments in the exploitation of the inventions of the Asserted Patents, including, by way of example, investments in engineering, research, and development. Ex. 12C (Rogers Decl.) at ¶¶ 17, 18, 20. At Centripetal's R&D facility, numerous engineers and

technologists work to engineer, research, and develop the technology of the Asserted Patents. *Id.* at ¶¶ 15-16. Centripetal's investments include salary and other compensation and benefits for these engineers and technicians, as well as investments in their training and recruitment. *Id.* at ¶ 18.

104. Centripetal is a leading innovator, provider, and designer of computer network security equipment and systems having threat intelligence technologies, related software, components thereof, and products containing same in the United States. Centripetal has invested and continues to invest significant and substantial resources in the United States to develop, produce, and support cutting-edge network security equipment and systems, related software, components thereof, and products containing same that exploit the patented technology. *Id.* at ¶¶ 7, 9, 20-21.

VIII. REQUESTED RELIEF

105. WHEREFORE, by reason of the foregoing, Centripetal respectfully requests that the United States International Trade Commission:

- a) Institute an investigation pursuant to Section 337 of the Tariff Act of 1930, as amended, 19 U.S.C. § 1337, with respect to violations based upon the unlawful importation into the United States, the sale for importation into the United States, and/or the sale within the United States after importation of certain computer network security equipment and systems, related software, components thereof, and products containing same that infringe the '370 Patent, the '917 Patent, and/or the '526 Patent;
- b) Conduct a hearing on said unlawful acts for the purposes of (i) receiving evidence and hearing argument concerning whether there has been a violation of Section 337, and (ii) determining that there has been a violation of Section 337;

c) Issue a permanent limited exclusion order pursuant to Section 337(d) directed to products that are manufactured, imported, sold for importation, or sold after importation by or on behalf of Keysight and its parents, subsidiaries, affiliates, related companies, agents, distributors, importers, or consignees (or agents thereof) excluding from entry into the United States certain computer network security equipment and systems, related software, components thereof, and products containing same that infringe, directly or indirectly, one or more of the Asserted Claims of the '370 Patent, the '917 Patent, and/or the '526 Patent;

d) Issue a permanent cease and desist order pursuant to Section 337(f) prohibiting Keysight, and its parents, affiliates, subsidiaries, related companies, distributors, and agents from engaging in unfair acts including, but not limited to, importing, selling for importation, marketing, advertising, testing, evaluating, demonstrating, warehousing inventory for distribution, offering for sale, selling, selling after importation, distributing, displaying, using, licensing, providing technical support for and/or otherwise transferring within the United States, certain computer network security equipment and systems, related software, components thereof, and products containing same that infringe, directly or indirectly, one or more of the Asserted Claims of the '370 Patent, the '917 Patent, and/or the '526 Patent, and engaging in any other commercial activity related to such products in the United States;

e) Impose a bond on importation and sales of infringing products during the 60-day Presidential review period pursuant to 19 U.S.C. § 1337(j); and

f) Grant such other and further relief as the Commission deems just and proper under the law, based on the facts determined by the investigation and the authority of the Commission.

Respectfully submitted,

Dated: April 19, 2022

By: /s/ Paul J. Andre
Paul J. Andre
Lisa Kobialka
James Hannah
Kris Kastens
Hannah Lee
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com
kkastens@kramerlevin.com
hlee@kramerlevin.com

James B. Altman
Barbara A. Murphy
Susan Koegel
Matthew N. Duescher
FOSTER MURPHY ALTMAN
& NICKEL, PC
1150 18th Street NW, Suite 775
Washington, DC 20036
Telephone: (202) 822-4100
Fax: (202) 822-4199
FM-CNI@fostermurphy.com

Attorneys for Complainant
CENTRIPETAL NETWORKS, INC.

**UNITED STATES INTERNATIONAL TRADE COMMISSION
WASHINGTON, DC**

In the Matter of

CERTAIN COMPUTER NETWORK
SECURITY EQUIPMENT AND SYSTEMS,
RELATED SOFTWARE, COMPONENTS
THEREOF, AND PRODUCTS CONTAINING
SAME

)
)
)
)
)
)
)
)
)
)

Investigation No. 337-TA-_____

VERIFICATION OF COMPLAINT

I, Jonathan Rogers, declare in accordance with 19 C.F.R. §§ 210.4 and 210.12(a), under penalty of perjury, that the following statements are true:

1. I am the Vice President of Operations & Chief Operating Officer at Centripetal Networks, Inc. and am duly authorized to sign this Complaint on behalf of Complainant;
2. I have read the foregoing Complaint;
3. To the best of my knowledge, information, and belief, based upon reasonable inquiry, the claims and other legal contentions set forth in the foregoing Complaint are warranted by existing law or by a good faith argument for the extension, modification, or reversal of existing law or the establishment of new law;
4. To the best of my knowledge, information, and belief, based upon reasonable inquiry, the allegations or other factual contentions set forth in the foregoing Complaint have evidentiary support or are likely to have evidentiary support after a reasonable opportunity for further investigation or discovery; and

5. The foregoing Complaint is not being submitted for an improper purpose, such as to harass or to cause unnecessary delay or needless increase in the cost of litigation.

Executed on April 18, 2022

/s/ Jonathan Rogers
Jonathan Rogers