IN THE UNITED STATES DISTRICT COURT FOR
THE EASTERN DISTRICT OF VIRGINIA
_____ DIVISION

CENTRIPETAL NETWORKS, INC.,	)	
	)	
Plaintiff,	)	No.
	)	
vs.	)	
	)	JURY TRIAL DEMANDED
KEYSIGHT TECHNOLOGIES, INC.,	)	
	)	
Defendant.	)	
	)	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Centripetal Networks, Inc. ("Centripetal") files this Complaint for Patent Infringement and Demand for Jury Trial against Keysight Technologies, Inc. ("Defendant" or "Keysight") and allege as follows:

THE PARTIES

1. Plaintiff Centripetal is a corporation organized under the laws of the state of Delaware with its principal place of business at 2251 Corporate Park Drive, Suite 150, Herndon, Virginia 20171.

2. Defendant Keysight is a Delaware corporation with its principal place of business at 1400 Fountain Grove Parkway, Santa Rosa, California 95403. Keysight acquired Ixia on April 18, 2017, and now calls Ixia a Keysight business.

3. Keysight regularly conducts and transacts business in Virginia, throughout the United States, and within the Eastern District of Virginia, and as set forth below, has committed and continues to commit tortious acts of patent infringement within Virginia, including the Eastern District of Virginia. Keysight maintains a regular and established place of business in this District through a permanent physical facility located at 43130

Amberwood Plaza #200, Chantilly, VA 20152. Further, the Keysight directly or indirectly uses, distributes, markets, sells, and/or offers to sell throughout the United States, including in this judicial district, various telecommunication products, including computing devices, associated equipment, and software.

JURISDICTION AND VENUE

4. This action for patent infringement arises under the patent laws of the United States, 35 U.S.C. § 101 *et seq.* This Court has original jurisdiction over this controversy pursuant to 28 U.S.C. §§ 1331 and 1338.

5. This Court has personal jurisdiction over Keysight. Keysight has conducted and continues to conduct business within the State of Virginia, and has engaged in continuous and systematic activities in the State of Virginia, including within this District. Keysight maintains a regular and established place of business in this District through offices located at 43130 Amberwood Plaza #200, Chantilly, VA 20152. Keysight, directly or through subsidiaries or intermediaries (including distributors, retailers, and others), ships, distributes, offers for sale, sells, and advertises (including by publishing an interactive web page in this District) its products and/or services in the Eastern District of Virginia, the State of Virginia, and the United States.

6. Keysight, directly and through subsidiaries or intermediaries including distributors, retailers, and others, has purposefully and voluntarily placed one or more of its infringing products and/or services, as described below, into the stream of commerce with the expectation that they will be purchased and used by consumers in the Eastern District of Virginia. These infringing products and/or services have been and continue to be purchased and used by consumers in the Eastern District of Virginia. Keysight has committed acts of

patent infringement within the State of Virginia and, more particularly, within the Eastern District of Virginia.

7. In addition, the Court has personal jurisdiction over Keysight because it has established minimum contacts with the forum such that the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice. For example, Keysight has recently advertised job listings in this District in the city of Chantilly, including job listings for developers and engineers, and makes, uses, offers for sale, and sells products or services that infringe the Asserted Patents in this District, as further described below.

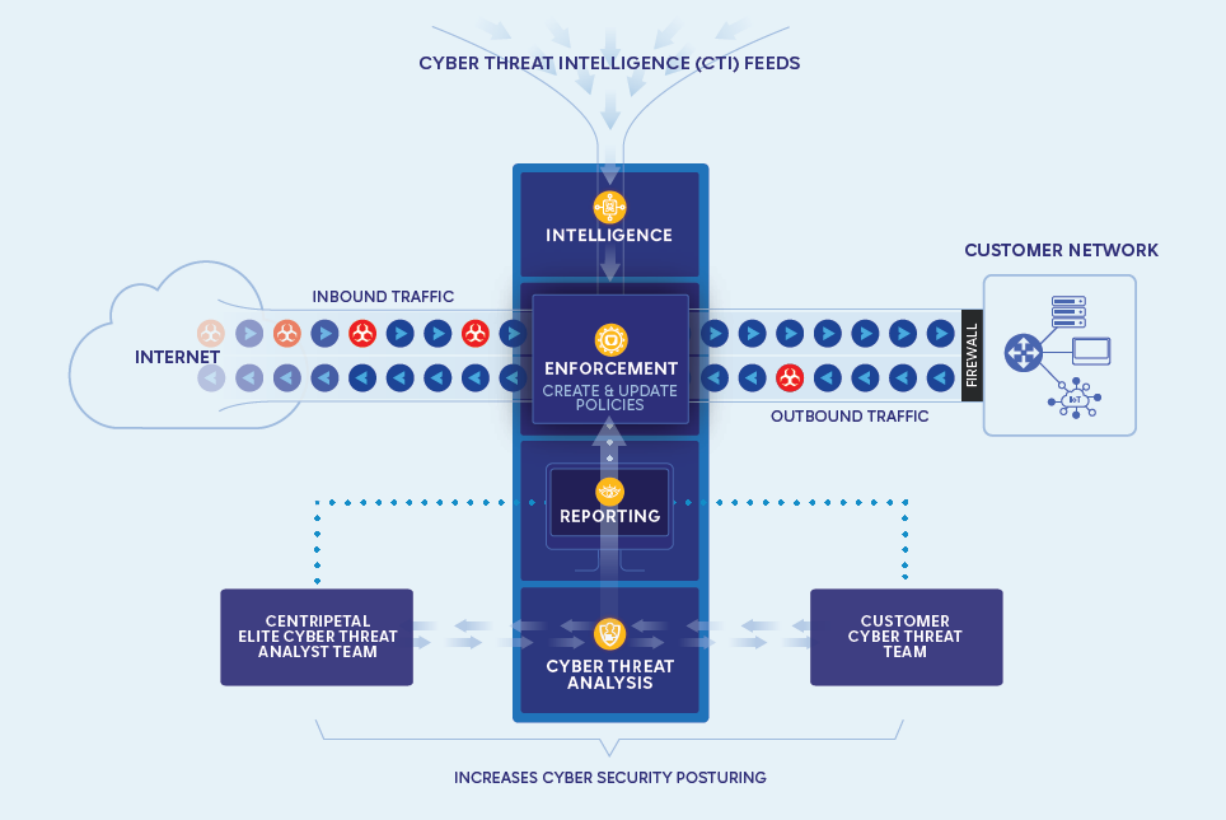
8. Venue is proper in the Eastern District of Virginia under 28 U.S.C. §§ 1391 (b) and (c) and/or 1400(b). Keysight has transacted business in this District, has a regular and established place of business in this District, and has infringed, induced infringement, and/or contributorily infringed in this District, and continues to do so. Keysight maintains a regular and established place of business in this District described above. Centripetal is informed and believes that Keysight employs a number of personnel in this District, including personnel involved in Keysight's infringement by at least through the testing, demonstration, support, use, offer for sale, and sale of the Accused Products and services within Virginia.

CENTRIPETAL AND ITS INNOVATIONS

9. Centripetal was founded in 2009 with a core mission to lead the field in innovating security technology to protect computer networks from advanced threats. Indeed, Centripetal became the first in the field to develop and invent specialized core networking technologies to operationalize threat intelligence from multiple sources at a scale and speed that could address the rapid growth in cyber threats. Centripetal has been the forerunner in developing cybersecurity technologies capable of fully operationalizing and automating threat

intelligence at scale. Centripetal's technologies protect organizations from advanced threats by extrapolating threat intelligence feeds and applying advanced packet filtering at the network edge to prevent unwanted traffic from hitting an organization's network and prevent compromised internal hosts from further damaging the organization's network. Today, Centripetal maintains one of the largest threat intelligence ecosystems, allowing it to provide community based solutions to defeat sophisticated cyberattacks.

10. Centripetal builds and sells software and appliances for network security using its patented technologies. Centripetal's CleanINTERNET® solutions utilize its patented Threat Intelligence Gateway, which allows organizations to catch and eradicate unknown threats based on threat intelligence enforcement.



Ex. 12. Centripetal's patented technologies also provide insight into an organization's security and gain visibility into threats. Centripetal's Threat Intelligence Gateway includes the

RuleGATE Gateway series of products, which are ultra-high performance threat intelligence gateways with real-time attack visualization and analytics. Ex. 13, CleanINTERNET® datasheet.

11. In recognition of its innovation and expertise, the U.S. Patent Office awarded Centripetal numerous patents that cover its key technological advances in the network security industry. Centripetal continues to apply for additional patents covering its innovations in the United States and around the world resulting directly from Centripetal's research and development efforts.

12. Centripetal has been recognized by third-party security organizations as an innovative technology company. For example, the Security Innovation Network ("SINET") named Centripetal the SINET 16 Innovator for 2017 at the SINET Showcase in Washington D.C. Ex. 14 (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. 15 (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. 16 (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. 17 (https://www.centripetal.ai/deloittes-2020-technology-fast-500/); Ex. 18 at 3.

CENTRIPETAL'S ASSERTED PATENTS

13. On February 16, 2016, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,264,370 (the "'370 Patent"), entitled "Correlating Packets in Communication Networks." A true and correct copy of the '370 Patent is attached hereto as Exhibit 1. The '370 Patent was filed on February 10, 2015. *Id.* at Cover.

14. On January 29, 2019, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,193,917 (the "'917 Patent"), entitled "Rule-Based Network-Threat Detection." A true and correct copy of the '917 Patent is attached hereto as Exhibit 2. The '917 Patent is a continuation of U.S. Patent No. 9,866,576 which was filed on April 17, 2015. *Id.* at Cover.

15. On May 7, 2019, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,284,526 (the "'526 Patent"), entitled "Efficient SSL/TLS Proxy." A true and correct copy of the '526 Patent is attached hereto as Exhibit 3. The '526 Patent claims and is entitled to the priority of provisional application No. 62/536,254 which was filed on July 24, 2017. *Id.* at Cover.

16. On December 17, 2019, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,511,572 (the "'572 Patent"), entitled "Rule Swapping in a Packet Network." A true and correct copy of the '572 Patent is attached hereto as Exhibit 4. The '572 Patent claims priority to U.S. Patent No. 9,203,806 (filed on January 11, 2013) via a series of continuation patents and/or applications. *Id.* at 1-2.

17. On February 18, 2020, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,567,343 (the "'343 Patent"), entitled "Filtering Network Data Transfers." A true and correct copy of the '343 Patent is attached hereto as Exhibit 5. The

’343 Patent is a continuation of U.S. Patent No. 9,686,193 which is a continuation of U.S. Patent No. 9,124,552 (filed on March 12, 2013). *Id.* at 1-2.

18. On March 31, 2020, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,609,062 (the “’062 Patent”), entitled “Rule-Based Network Threat Detection.” A true and correct copy of the ’062 Patent is attached hereto as Exhibit 6. The ’062 Patent is in the same family as the asserted ’917 Patent and claims priority to U.S. Patent No. 9,866,576 (filed on April 17, 2015). *Id.* at 1-2.

19. On May 19, 2020, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,659,573 (the “’573 Patent”), entitled “Correlating Packets in Communications Networks.” A true and correct copy of the ’573 Patent is attached hereto as Exhibit 7. The ’573 Patent is in the same family as the asserted ’370 Patent and claims priority to the ’370 Patent via a series of continuation patents. *Id.* at 1-2.

20. On June 9, 2020, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,681,009 (the “’009 Patent”), entitled “Rule Swapping in a Packet Network.” A true and correct copy of the ’009 Patent is attached hereto as Exhibit 8. The ’009 Patent claims priority to U.S. Patent No. 9,203,806 (filed on January 11, 2013) via a series of continuation patents. *Id.* at 1-2.

21. On February 16, 2021, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,924,456 (the “’456 Patent”), entitled “Methods and Systems for Efficient Encrypted SNI Filtering for Cybersecurity Applications.” A true and correct copy of the ’456 Patent is attached hereto as Exhibit 9. The ’456 Patent was filed on July 14, 2020. *Id.* at Cover.

22. On May 18, 2021, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 11,012,474 (the "'474 Patent"), entitled "Methods and Systems for Protecting a Secured Network." A true and correct copy of the '474 Patent is attached hereto as Exhibit 10. The '474 Patent claims priority to U.S. Patent Nos. 9,565,213 and 9,137,205 via a series of intermediate patents and applications. *Id.* at 1-2.

23. On September 22, 2020, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,785,266 (the "'266 Patent"), entitled "Methods and Systems for Protecting a Secured Network." A true and correct copy of the '266 Patent is attached hereto as Exhibit 11. The '266 Patent claims priority to U.S. Patent No. 9,137,205 via a series of intermediate patents. *Id.* at pgs. 1-2.

24. Centripetal owns by assignment the entire right, title, and interest in and to the '370 Patent, '917 Patent, '526 Patent, '572 Patent, '343 Patent, '062 Patent, '573 Patent, '009 Patent, '456 Patent, '474 Patent and '266 Patent (collectively, "the Asserted Patents").

25. All of the Asserted Patents are valid and enforceable.

THE ASSERTED PATENTS IMPROVE NETWORK SECURITY

26. Threats to computer network security have grown in number and in sophistication over time. Network security systems, in kind, have to continually improve and become more effective as hackers become increasingly more sophisticated and continue to identify and exploit newfound vulnerabilities. Prior to Centripetal's patented inventions, conventional solutions filtered network traffic in a static manner, and thus failed to adequately meet network security needs in the face of the ever-changing threat landscape. Centripetal's dynamic network security solutions allow network users to implement effective security systems that protect against the latest evolution of network threats.

27. The Asserted Patents are directed to solving problems existing in the field of computer network security. The Asserted Patents are concrete systems that provide specific improvements to the operation of network security systems.

28. A network packet is a fundamental means to transmit data over a computer network. Network packets are specifically formatted in a way that allows computers to communicate over networks by breaking larger messages into discrete chunks that are sent to a destination in the network and then reassembled back into original form at the destination.

29. The Asserted Patents provide benefits that are novel and superior to what was previously available.

30. The ’370 and ’573 Patents provide, 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 taps 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 and ’573 Patents provide a solution to the problem that occurs when network devices alter data packets associated with a flow and obfuscate the flow in which a particular packet is associated. *See, e.g.*, Ex. 1 at 1:6-15, 1:41-49; Ex. 7 at 1:23-32, 1:58-67. This disassociation and obfuscation of packet information would result in the network devices’ inability to know whether a packet posed a malicious threat to a network, including whether it was coming from a malicious host. *See, e.g.*, *id.*; Ex. 1 at 9:52-54; Ex. 7 at 10:14-16. The ’370 and ’573 Patents can 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.*, Ex. 1 at 1:26-49; Ex. 7 at 1:43-67. The ’370 and

’573 Patents also improve network security by generating rules or other identifying information based on the correlation. *See, e.g.*, Ex. 1 at 12:54-60; Ex. 7 at 13:19-26. This can prevent other packets with the same threats from further damaging the network.

31. The ’062 and ’917 Patents provide, 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. 6 at 1:32-37; Ex. 2 at 1:28-33. The ’062 and ’917 Patents provide techniques for inspecting and monitoring network traffic information based on threat indicators. *See, e.g.*, Ex. 6 at 1:48-2:14; Ex. 2 at 1:44-2:10. The threat indicators are based on threat intelligence information received from various sources. The ’062 and ’917 Patents describe systems that are able to provide real-time monitoring and logging capacities based on threat intelligence information and allow a user to observe real-time traffic and customize the company’s policy on the management tool in response to the real-time observations. *See, e.g.*, Ex. 6 at FIGs. 6A-6G, 2:1-14, 8:5-36; Ex. 2 at FIGs. 6A-6G, 1:64-2:10, 8:1-32. The management tool can cause the packet-filtering device to automatically receive updates to the rules for filtering subsequent network traffic. *See, e.g.*, Ex. 6 at 13:36-51; Ex. 2 at 13:29-43.

32. 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 an encrypted

communication flows, receive packets that initiates 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. 3 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.” Ex. 3 at 1:35-40; *see also id.*, 4:66-5:32. The ’526 Patent addresses these issues by providing techniques for selectively decrypting encrypted communications, which for example, may be based on threat intelligence information. Ex. 3 at 1:53-2:44, 5:33-43.

33. The ’572 and ’009 Patents describe improve network devices, including a processor and memory to cause a network device to receive a first rule set, modify a first rule set, configure a network device to process packets using the first rule set, receive a second rule set after the first rule set is implemented, modify a second rule set, modify a second rule set, based on signal to process packets with the second rule set, cease processing of packets, cache packet, reconfigure a processor to process under the second rule set, and process the second rule set. As described in the patents, “[n]etwork protection devices may require time to switch between rule sets. As rule sets increase in complexity, the time required for switching between them presents obstacles for effective implementation. For example, a network protection device may be unable to process network traffic while switching between rule sets due to the utilization of resources for implementing the new rule set. Additionally, while implementing a new rule set, a network protection device may continue processing packets in accordance with

an outdated rule set. In certain circumstances (e.g., in the event of a network attack), such processing may exacerbate rather than mitigate the impetus for the rule set switch (e.g., the effect of the network attack)." Ex. 4 at 1:38-50; Ex. 8 at 1:38-50. The '572 and '009 Patents include techniques that provide a significantly decreased downtime / decreased performance for the network whenever a major ruleset shift occurs from a first ruleset to a second ruleset that can be critical in the event of a major attack. Using the techniques described in the '572 and '009 Patents, a network device can swap large rule sets without needing to take the device offline and without packet loss.

34. According to the '343 Patent, conventional cyber defense systems fail to prevent advanced cyber-attacks, such as data exfiltration. Ex. 5 at 1:28-51. The '343 Patent describes improved techniques to address these types of advanced cyberattacks by offering granularity with regards to the mechanisms / configurations of the various network data transfer protocols, including by a processor and memory for receiving packets, determine, based on the packet header field value whether the packet complies with a packet-filtering rule, apply packet-filtering rules to matches to the packet, determine, based on the application header value, whether a packet-filtering rule matches a second criterion, and in response, perform a packet transformation function configured to prevent exfiltration. The '343 Patent describes techniques to inspect certain packet header information, and make a further determination based on application header field criteria. *See, e.g.*, Ex. 5 at 1:52-2:23. As a result, the network security devices are better tuned to significantly decrease the risk of network insider threats and at the same time, reduce the impact of a business's normal operation if a threat is detected.

35. The ’456 Patent provides improved techniques for detecting network threats, particularly in encrypted network traffic, including providing a method for receiving threat indicators, determining packet-filtering rules related to the threat indicator, receiving packets that include ciphertext comprising an encrypted server name (eSNI), determining whether the plaintext host name is resolvable from the cyphertext, based on the determination that the plaintext hostname matches at least one of threat indictors applying a packet-filtering operation. The ’456 Patent “generally relate to computer hardware and software for efficient packet filtering of Transport Layer Security (TLS) handshake messages containing ciphertext that corresponds to Server Name Indication (SNI) (e.g., encrypted SNI (eSNI)) values.” *See, e.g.*, Ex. 9 at 1:8-15. The ’456 Patent describes cybersecurity applications which can “detect an encrypted hostname” in packet information and use threat intelligence associated with the hostname to determine whether the packets relate to network threats. *See, e.g.*, Ex. 9 at 3:5-35.

36. The ’474 and ’266 Patents include methods and systems that providing a proactive and scalable network security solution, as opposed to the traditional, reactive approach, including a system that includes a packet security gateway with a processor and memory that receives from a security policy management server, dynamic security policy comprising packet-filtering rules that were modified or created by the security policy management server based on correlating malicious traffic information from various malicious host tracker services, the packet filtering rule including a packet matching criterion, packet transformation function, and an indication of the feed managed by the malicious host tracker services, and performing on the packet-filtering rules on the packets. Ex. 10 at 1:34-46; Ex. 11 at 1:36-48. Generally, they relate to scalable proactive security systems which protect networks using dynamically updated security policies. Ex. 10 at FIG. 5, 1:57-2:15, 14:66-

15:29; Ex. 11 at FIG. 5, 1:59-2:18, 14:9-39. The dynamic updates can be based on threat intelligence information gathered from various sources, causing rule or policy changes on network devices. *Id.* This process allows network devices to quickly and continually adapt to evolving cyber threats.

KEYSIGHT AND ITS PRODUCTS

37. Keysight is a multi-billion dollar company that offers network products to enterprise customers. Keysight Technologies, Inc. acquired Ixia in April 2017, who was making, using, selling, and offering for sale various packet brokers and network security products. Ex. 19. As a result of Keysight's acquisition of Ixia, Keysight added new products for "testing, visibility, and security solutions, strengthening applications across physical and virtual networks for enterprises, service providers, and network equipment manufacturers." *Id.* Keysight now develops and sells a range of different products and services that provide security and visibility into networks, including the ability to leverage threat intelligence.

38. Keysight makes, uses, sells and offers for sale Network Visibility products and services ("Network Visibility products"), which are currently marketed under the names of Vision X, Vision One, the Vision 7300 series of products, the Vision Edge series of products,[1] Vision 7816, TradeVision and CloudLens (including SaaS and Self-Hosted versions). *See e.g.*, Exs. 20-30. The Network Visibility products provide network security by detecting network threats and filtering network traffic with threat intelligence. *See, e.g.*, Ex. 21. The 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. 24.

[1] The Vision Edge series of products includes Vision E40, Vision E100, Vision E1S, Vision E10S, and Vision Edge OS.

39. The Network Visibility products have underlying technologies that are marketed as NetStack, PacketStack, SecureStack, AppStack, and MobileStack technologies. *See e.g.*, Ex. 21; Ex. 20; Ex. 30. NetStack, PacketStack, SecureStack, AppStack, and MobileStack technologies provide Keysight's products and services at issue with increased security, control and/or visibility into packets traversing a network.

40. NetStack operates on network packets with a three-stage filtering process. Ex. 31. NetStack has features such as "robust filtering, load balancing, aggregation, replication, … three stages of filtering, and dynamic filter compiler." Ex. 21 at 6. Keysight also advertises NetStack as being able to make "hitless changes – no packets dropped when you re-configure." Ex. 31.

41. 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. 21 at 6.

42. SecureStack "optimizes handling for secure traffic. Supports inline and out-of-band SSL / TLS decryption and threat intelligence." Ex. 21 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. 32.

43. AppStack, among other things, "provide[s] context-aware, signature-based application-layer filtering with accurate and fast application identification, geolocation and tagging." Ex. 21 at 6. AppStack has Application and Threat Intelligence subscription that provides up-to-date application and geolocation information. Exs. 34-35.

44. MobileStack "[o]ffers visibility intelligence for the mobile carrier." Ex. 21 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. 36.

45. The Network Visibility products contain one or more of these accused technologies described in Paragraphs 39-44. For example, CloudLens, a platform for public, private and hybrid clouds, contains technologies, such as Netstack, Packetstack, AppStack, and SecureStack, which also are in other Network Visibility products, like Vision One and the Vision 7300 family of products. *See, e.g.*, Ex. 37; Exs. 32-33. NetStack, PacketStack, and AppStack are also in other Network Visibility products, such as the Vision Edge 1S and 10S, Vision One, Vision X, and Vision 7300 family of products. Ex. 24. Vision X, Vision One, and the Vision 7300 family of products also include SecureStack. Exs. 32-33. MobileStack is in at least Vision One and Vision X. Ex. 24. TradeVision includes all technologies from Vision One and a technology marketed as TradeStack, which "[o]ffers the financial capital markets a simplified market feed data management tool that removes the hassle of configuring, analyzing, and managing market feed data." Ex. 38 at 1; Ex. 21 at 6.

46. The Network Visibility products also all have the accused Application and Threat Intelligence technologies ("ATI technology"). Ex. 39. The ATI technology provides updates in the form of data feeds (also referred to and marketed as Threat Insights, Application and Threat Intelligence, or Rap Sheets) from servers, which include information such as remote network attacks, remote application attacks, IP addresses, geolocation mapping, etc. The ATI technology provides dynamically updated data feeds which are actionable security intelligence

on application and network vulnerabilities, and include descriptions of threats across networks, endpoints, mobile devices, virtual systems, web, and email.

LEVERAGED ACROSS KEYSIGHT'S TEST, SECURITY, AND VISIBILITY PORTFOLIOS

Keysight's application and threat intelligence is harnessed by our test solutions including BreakingPoint, IxLoad, IxChariot, and IxNetwork, used by the world's largest network equipment vendors and service providers to test their networks and technology. ATI also provides data to Keysight's ThreatARMOR and AppStack, which is integrated into our award-winning Vision series of network packet brokers (NPBs).

- Real-time cloud threat intelligence that enables ThreatARMOR to provide continuous protection, filtering out untrusted countries, malicious sites, and harmful IP addresses (malware distribution, phishing sites, botnet C and C sites, spam distribution, bogons, hijacked domains, and unassigned IPs)
- Application insight enabling AppStack and our network-visibility products to provide complete network visibility extending beyond Layer 4 into granular application behaviors, including an always-on global IP geolocation database
- ATI delivers to BreakingPoint constant updates of the top applications critical in validating the legitimate application performance of security tools as well as validating the efficacy of lawful intercept (LI), data loss prevention (DLP), and deep packet inspection (DPI) solutions
- Daily malware update service enables nearer-real-time malware threat intelligence that helps differentiate the most agile security systems from the rest
- Real-world traffic that provides realistic, scalable application emulations to recreate network traffic profiles using 400+ applications, updated with the BreakingPoint ATI subscription
- Continually updated ATI application library, is used by the IxLoad, IxNetwork, and IxChariot test solutions, helps users validate the scale and performance capabilities of content-aware devices and networks
- Keysight's products, powered by ATI, improve your security performance, bring application-level visibility and context to your monitoring tools, and validate network devices with real-world threats and application conditions

Ex. 39. Keysight markets the ATI technology under several different marketing names, such as Threat Intelligence, Threat Insights, and Application and Threat Intelligence. *Id.*; Exs. 32-33; Ex. 39.

47. Keysight also makes, uses, sells and offers for sale Network Tap products and services ("Network Tap products") that are marketed under the names of Flex Tap, Flex Tap Secure+, Patch Tap, Copper Tap, Tap Aggregators, Copper Tough Taps, Copper Tough Tap Power Solution, Flex Tough Taps, and Vision T1000 Packet Aggregator. *See e.g.*, Exs. 40-44. The Network Tap products all capture network packet data and provide the captured network packet data to other network devices, like the Network Visibility products. *See* https://www.youtube.com/watch?v=r3-PBfmFMqA&t=39s.

48. Keysight makes, uses, sells and offers for sale Bypass Switch products and services ("Bypass Switch products") that are marketed under the names of iBypass 100G, iByPass 40G, iByPass Copper, iByPass Duo, iByPass HD, and iBypass VHD. *See e.g.*, Exs. 45-50. The Bypass Switch products can capture network packet data and provide them to other

tools, such as the Network Visibility products. Ex. 51 at 5. Additionally, the Bypass Switch products can route packets in a way to circumvent failed network devices. *Id.* at 3-4.

49. Keysight makes, uses, sells and offers for sale ThreatArmor and Security Operations Suite products and services ("ThreatArmor Suite"), including ThreatArmor and Threat Simulator. Exs. 52-53. Keysight advertises ThreatArmor as a threat intelligence gateway. Ex. 54. ThreatArmor "[blocks] bad traffic from entering your network" and "[reduces] alert fatigue by stemming the flood of notifications from your SIEM and security tools." Ex. 55. Threat Simulator "simulate attacks on your live network with breach and attack simulation. Validate your security tools, discover vulnerabilities in your security posture . . . ." *Id.* ThreatArmor and Threat Simulator use ATI technology, including ATI data feeds to carry out their functions. Ex. 39; Ex. 54; Ex. 53 at 4. ThreatArmor includes ThreatArmor Central Management service which manages one or more ThreatArmor devices. Ex. 56.

50. Keysight makes, uses, sells, and offers for sale testing products and services ("Testing products") marketed under the name BreakingPoint, which includes: (a) the accused technologies Keysight markets as CyPerf, IxLoad, IxNetwork, IxChariot, Hawkeye, and IOT Security Assessment Test Software and (b) related applications and security hardware platforms, such as APS-100/400GE series, PerfectStorm appliances (including, e.g., PerfectStorm 100GE 1-Port, 40/10GE, ONE 10/40GE, ONE 1/10GE, 10/1GE), CloudStorm appliances (including, e.g., CloudStorm 100GE 2-PORT, 25GE LoadModule, 10/40GE Load Module), NOVUS-NP 10G/1G/100M or on hardware in the cloud. *See e.g.*, Exs. 57-65. The BreakingPoint line of products have various marketing names, such as BreakingPoint, BreakingPoint VE, BreakingPoint QuickTest, and BreakingPoint Cloud.

51. The Testing products analyze packet information and discover security vulnerabilities in a network environment. *See, e.g.*, Ex. 55. The Testing products also have the accused technologies from Network Visibility products, such as those in Vision One. Among other things, the Testing products use the ATI technology, and receive ATI data feeds to carry out their functions. Ex. 39.

52. Keysight makes, uses, and sells Ixia Fabric Controller. *See e.g.*, Ex. 66. Ixia Fabric Controller manages at least Keysight's Network Visibility products, Taps products, and Bypass Switch products. Id.

KEYSIGHT'S INFRINGEMENT OF CENTRIPETAL'S PATENTS

53. Keysight has infringed and continues to infringe one or more claims of each of the Asserted Patents by engaging in acts that constitute infringement under 35 U.S.C. § 271, including but not necessarily limited to making, using, selling, and/or offering for sale, in this District and elsewhere in the United States, and/or importing into this District and elsewhere in the United States, the accused Network Visibility products, the Network Tap products, the Bypass Switch products, the ThreatArmor Suite, the Testing products, and Ixia Fabric Controller and the accused technologies identified above alone or in conjunction with one another (collectively, "the Accused Products").

54. In addition to directly infringing the Asserted Patents pursuant to 35 U.S.C. § 271(a), literally and/or under the doctrine of equivalents, Keysight indirectly infringes all the Asserted Patents under 35 U.S.C. §§ 271(b) and (c), literally and/or under the doctrine of equivalents. Keysight induces infringement of the Asserted Patents by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to meet claim elements, literally and/or under the doctrine of equivalents, of the Asserted Patents.

Keysight contributorily infringes the Asserted Patents by making and supplying products that are components of an infringing system with components from manufacturers, customers, purchasers, users, and developers that together meet all claim elements in the Asserted Patents, literally and/or under the doctrine of equivalents.

55. On information and belief, Keysight had knowledge of the Asserted Patents prior to this Complaint and of Centripetal. Keysight had knowledge of the Asserted Patents through several different avenues.

56. On information and belief, Keysight has long been acquainted with Centripetal's technology and has investigated Centripetal's products, technologies, and patents. Keysight has knowledge of the Asserted Patents based on Keysight's interactions with Centripetal through various other channels. For example, Keysight viewed information regarding Centripetal's patents and technology on Centripetal's website. Since 2014, Keysight (and its since acquired companies) visited Centripetal's numerous pages on Centripetal's website regarding business, products, and patents, and downloaded datasheets and white papers regarding Centripetal's patented products. Centripetal's datasheets indicate Centripetal's products are subject to one or more patents. Further, the downloaded technical "whitepapers" explained how Centripetal's technology worked, described its capabilities, and the new functionality in Centripetal's products. Further, Centripetal's products and services are marked with Centripetal's Asserted Patents, upon their issuance. In addition, Centripetal's public website and product datasheets identify that Centripetal has issued and pending patents, and its website includes a list of patent numbers, in compliance with 35 U.S.C. § 287. Ex. 67. On information and belief, Keysight used this information to incorporate infringing technologies into its products.

57. Keysight further should have knowledge of the Asserted Patents because of a previous patent litigation between the parties that commenced on July 20, 2017. In that litigation, Centripetal asserted the '370 Patent against Keysight. In the middle of trial, the parties entered into a limited term license agreement ("Centripetal Term License") to Centripetal's patent portfolio that expired on December 31, 2021. At the time the Centripetal Term License was entered, the '370 and '917 Patents had issued or had published patent applications and the parent application for the '572 Patent, '343 Patent, '062 Patent, '573 Patent, '009 Patent, '474 Patent, and '266 Patent had issued. All of the Asserted Patents issued before the expiration of the Centripetal Term License.

58. As part of the Centripetal Term License, Keysight was required to pay Centripetal a running royalty on hardware and software products, including VisionONE, Vision 7300, Vision 7303, with AppStack and SecureStack on the hardware, ThreatARMOR, and BreakingPoint with ATI during the term. Keysight was aware of the patents and published applications that it was licensing, which included the Asserted Patents.

59. Because the Centripetal Term License expired, Keysight no longer has any rights to practice any of the Asserted Patents.

60. Centripetal is informed and believes that Keysight has also been aware of Centripetal's Asserted Patents through other publicly available information, including prior patent litigations filed by Centripetal against Keysight competitors, Cisco Systems, Inc. ("Cisco") and Palo Alto Networks ("PAN") in 2018 and 2021 respectively, where the asserted patents are either the same as or in the same families as the Asserted Patents, and the accused PAN products and infringing Cisco products are competitive with the Keysight Accused Products. On information and belief, Keysight has been aware, based on publicly available

information, that Centripetal obtained a judgment of validity and infringement against Cisco in October 2020 and awarded damages of $2.6 to $3.2 billion based on a 5-10% royalty rate.

61. Centripetal is informed and believes that Keysight was aware of the Asserted Patents, and has done nothing to curtail its infringement.

62. Centripetal is informed and believes that despite Keysight's knowledge of the Asserted Patents and Centripetal's patented technology, Keysight made the deliberate decision to continue to make, use, sell and offer for sale at least the Accused Products that it knew infringes Centripetal's Asserted Patents.

63. Centripetal is informed and believes that Keysight has undertaken no efforts to avoid infringement of the Asserted Patents, despite Keysight's knowledge and understanding that Keysight's products and services infringe these patents. Thus, Keysight's infringement of the Asserted Patents is willful and egregious, warranting enhancement of damages.

64. Centripetal is informed and believes that Keysight knew or was willfully blind to Centripetal's patented technology. Despite this knowledge and/or willful blindness, Keysight has acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

FIRST CAUSE OF ACTION
(Direct Infringement of the '370 Patent pursuant to 35 U.S.C. § 271(a))

65. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

66. Keysight has infringed and continues to infringe at least one or more claims of the '370 Patent.

67. Keysight's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

68. Keysight's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

69. Keysight's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the '370 Patent, including, but not limited to the following products and services: the Network Visibility products, the Network Tap products, the Bypass Switch products, the ThreatArmor Suite, and the Testing products, and any other products or services with Keysight's AppStack, SecureStack, packet logging and correlation, and the ATI technology (the "'370 Accused Products").

70. Keysight also infringes jointly with its customers, users, and vendors. Keysight directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, Keysight puts the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

71. The '370 Accused Products embody the patented invention of the '370 Patent and infringe the '370 Patent because they include a system with at least one processor, and memory comprising instructions that, when executed by the at least one processor, cause the system to: provision a device in a communication link interfacing a network device and a first network with one or more rules configured to identify a plurality of packets received by the network device from a host located in the first network; provision a device in a communication link interfacing the network device and a second network with one or more rules configured to identify a plurality of packets transmitted by the network device to a host located in a second

network; provision the device in the communication link interfacing the network device and the first network and the device in the communication link interfacing the network device and the second network with one or more rules specifying a set of network addresses and configured to cause the system to log packets destined for one or more network addresses in the set of network addresses; configure the device in the communication link interfacing the network device with the first network to: identify the plurality of packets received by the network device; generate a plurality of log entries corresponding to the plurality of packets received by the network device; and communicate, to the system, the plurality of log entries corresponding to the plurality of packets received by the network device; configure the device in the communication link interfacing the network device with the second network to: identify the plurality of packets transmitted by the network device; generate a plurality of log entries corresponding to the plurality of packets transmitted by the network device; and communicate, to the system, the plurality of log entries corresponding to the plurality of packets transmitted by the network device; correlate, based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device, the plurality of packets transmitted by the network device with the plurality of packets received by the network device; and responsive to correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device: generate data identifying the host located in the first network; and communicate, to a device located in the first network, the data identifying the host located in the first network.

72. The ‘370 Accused Products are, or run on, computers with processors and memory (including RAM and a hard drive) that stores instructions executed by the processors.

73. The ‘370 Accused Products include a packet-filtering system provisioned with packet-filtering rules that allow the packet-filtering system to identify packets. For example, Keysight’s Vision One is a packet broker which filters packets. Vision One sits in a communication link with a network device and can obtain information on packets transmitted and/or received by the network device, including packets to/from a host in a first network. Vision One uses threat intelligence based rules to filter packets. These rules are provisioned onto the ‘370 Accused Products with the ATI technology. As another example, Keysight advertises its ThreatArmor product as a threat intelligence gateway. The ThreatArmor product is a packet filtering system that inspects inbound and outbound network packets and applies threat intelligence based rules to filter the packets.

74. The ’370 Accused Products generate packet log entries corresponding to these packets that are received. For example, Vision One generates packet log entries in the form of IxFlow (NetFlow modified with additional Keysight-specific metadata). Ex. 68. ThreatArmor and the Testing products also generate log entries. Ex. 56; Ex. 69. Additionally, Keysight’s Network Tap products and Bypass Switch products generate log entries to provide visibility into the network traffic. Ex. 70; Ex. 45.

75. The ‘370 Accused Products correlate packet log entries in a number of ways. For example, the ATI technology retrieves NetFlow data from collectors and correlates the data to generate Rap Sheets or Threat Insight identifying compromised IP addresses. Ex. 71. The Testing products correlate log entries with its machine learning and analytics technology. Ex. 69. The Network Visibility products also correlate log entries. As another example, the ‘370 Accused Products correlate packet log entries. *See, e.g.*, Ex. 24; Ex. 72; Ex. 36 (“With the GTP/SIP session correlation feature, you can recreate a subscriber's full data session by

tapping the various control and data plane interfaces and directing all traffic belonging to a given user to the same monitoring probe. Offloading the correlation to Vision X, Vision ONE, GTP Session Controller (GSC) or CloudLens can free probe resources by up to 50% — allowing you to scale out your monitoring infrastructure.”). The log entries can come from other network elements, such as those generated by the Network Tap products and the Bypass Switch products. *See id*.

76. The ‘370 Accused Products generate data identifying a host in the first network in the form of a Rap Sheet, Threat Insight, or other forms of threat intelligence data identifying the host as hijacked, associated with a botnet, or otherwise compromised. Based on this identification, the ‘370 Accused Products communicate to a device data identifying a host associated with a malicious entity. The ‘370 Accused Products can block data sent from the host when that data is being sent to an IP address associated with the matching threat intelligence information.

Rap Sheets Describe Network Risks

Whenever ThreatARMOR blocks traffic to or from a known-bad site, a Rap Sheet is provided to explain why that IP address is considered bad. This helps customers better understand the risks facing their network and also avoid the risk of false positive. ThreatARMOR only blocks an IP address if the ATI Research Center has 100% certainty there is malicious or criminal activity at that site, and the Rap Sheet details the proof. The Rap Sheets themselves provide information such as the URL information of individual threats, the binary checksum of that malware, screen shots of a phishing page or malware installer, and the last date the individual piece of malicious activity was validated.

Fig. 1: Rap Sheet example of malicious activity

Ex. 71.

77. As a result of Keysight's unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

78. Keysight has willfully infringed the '370 Patent, as set forth in the preceding paragraphs. Centripetal is informed and believes that Keysight had knowledge of the '370 Patent through various channels, and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

79. Keysight thus knew or, in the alternative, was willfully blind to Centripetal's technology and the '370 Patent.

80. Despite this knowledge and/or willful blindness, Keysight acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

81. 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. As such, Keysight has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously in infringement of the '370 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

82. Keysight's infringement of the '370 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

83. Keysight's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

84. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

SECOND CAUSE OF ACTION
(Indirect Infringement of the '370 Patent)

85. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

86. Keysight has induced and continues to induce infringement of one or more claims of the '370 Patent under 35 U.S.C. § 271(b). Keysight has contributorily infringed and continues to contributorily infringe one or more claims of the '370 Patent under 35 U.S.C. § 271(c).

87. 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 steps of the method claims, or provide one or more components of a system 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, taps, or bypass switches, to execute the functions of one or more claims of the '370 Patent. Keysight instructs, directs and/or requires its customers, users, and vendors, or some combination thereof, to set up the system where bypass switches and taps identify packets and generate log entries. The log entries may

be provided to ThreatArmor and Vision One 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 '370 Accused Products, such as the monitoring function in ThreatArmor, to perform one or more steps in the claims of the '370 Patent. Keysight has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with Keysight, one or more claims of the '370 Patent.

88. 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 '370 Accused Products. Such use is consistent with how the '370 Accused 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: (a) advising its customers and users to use the '370 Accused 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; (b) advertising and promoting the use of the '370 Accused Products in an infringing manner; (c) and distributing guidelines and instructions on how to setup the '370 Accused 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 obtains 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.

89. Keysight updates and maintains a support website that includes technical documentation encouraging the use of the '370 Accused Products in an infringing manner. Example technical documentation includes knowledge articles, videos, user guides, technical support articles, and a knowledge center. The technical documentation covers the operation of the '370 Accused Products in-depth, including by advertising the '370 Accused Products' infringing features and instructing customers, users, and vendors to configure and use the '370 Accused Products in an infringing manner. *See, e.g.*, Ex. 73 (https://www.keysight.com/us/en/support.html); Ex. 74 (https://support.keysight.com/s/?language=en_US); Ex. 75 (https://support.ixiacom.com/).

90. Keysight contributorily infringes the '370 Patent pursuant to 35 U.S.C. § 271(c) because it provides the '370 Accused Products as software and computer systems with software installed which act as a material component of the '370 Patent claims when combined with other components to create a complete network security system. Keysight knows that its products are particularly suited to be used in an infringing manner. The '370 Accused Products, including their associated software, are highly developed and 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.

91. 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 '370 Accused Products together with its customers, users, and vendors to meet the elements of the '370 Patent, as described above and incorporated by reference here. To the extent Keysight's 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 for CloudLens, which infringes when a third party runs this software on processors and memory in a cloud environment. As another example, Keysight sells the Network Visibility products, the Testing products, and ThreatArmor, which infringes when a third party combines them for use with the Bypass Switch products, the Network Tap products, or devices with similar functionalities. As a further example, through simulating network traffic and conditions, the Testing products can cause other Keysight's products, such as the Network Visibility pfroducts, ThreatArmor, the Network Tap products and the Bypass Switch products to perform the infringing functions. To the extent Keysight's customers, users, and vendors direct and control the systems and methods in the claims, Keysight obtains benefits from the control of the 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 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.

92. Keysight's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

93. 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.

94. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

THIRD CAUSE OF ACTION
(Direct Infringement of the '917 Patent pursuant to 35 U.S.C. § 271(a))

95. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

96. Keysight has infringed and continues to infringe at least one or more claims of the '917 Patent.

97. Keysight's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

98. Keysight's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

99. Keysight's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the '917 Patent, including, but not limited to the following products and services: the Network Visibility products, the ThreatArmor Suite, the Testing products, and the Ixia Fabric Controller, and any other products or services with Keysight's AppStack, SecureStack, and the

ATI technology (the "'917 Accused Products"). Keysight also infringes these claims jointly with its customers, users, and vendors. Keysight directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, Keysight puts the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

100. The '917 Accused Products embody the patented invention of the '917 Patent and infringe the '917 Patent because they include a packet filtering device with one or more processors; and memory storing instructions that, when executed by the one or more processors, cause the packet filtering device to: receive a plurality of packets; responsive to a determination by the packet-filtering device that a first packet of the plurality of packets corresponds to one or more packet-filtering rules: apply, to the first packet, an operator specified by a corresponding packet-filtering rule and configured to cause the packet-filtering device to either prevent the first packet from continuing toward a destination of the first packet or allow the first packet to continue toward the destination of the first packet; and generate a packet log entry comprising at least one threat indicator corresponding to the first packet and data indicating whether the packet-filtering device prevented the first packet from continuing toward the destination of the first packet or allowed the packet to continue toward the destination of the first packet; update, based on the packet log entry, a packet flow entry, corresponding to the generated packet log entry, of packet flow analysis data for a plurality of logged packets, wherein the packet flow analysis data comprises data corresponding to a plurality of packet flow entries, and wherein each packet flow entry consolidates a plurality of packet log entries corresponding to a common threat identifier; communicate, to a computing device, the packet flow analysis data; and cause, based on the communicated packet flow

analysis data, display of at least a portion of the packet flow analysis data, wherein the packet flow analysis data comprises at least one threat identifier corresponding to each of the plurality of logged packets, packet time data for packets corresponding to the packet flow entry, and data indicating whether the packet-filtering device prevented packets from continuing toward a respective destination or allowed packets to continue toward the respective destination.

101. The '917 Accused Products include a packet-filtering device. For example, the Network Visibility products are packet-filtering devices that sit in a communication link and filter packets. *See, e.g.*, Ex. 24. ThreatArmor is a threat intelligence gateway that filters inbound and outbound packets. Ex. 52 at 1. The Testing products include the functionalities of the Network Visibility products, such as those in Vision One. For example, the Testing products "[v]alidate the security posture of your networks with real applications and a complete range of threat vectors," which involves analyzing threats in the packets. The '917 Accused Products are, or run on, computers with processors and memory (including RAM and a hard drive) that stores instructions executed by the processors.

102. The '917 Accused Products receive and inspect packet information. Ex. 52 at 1; Ex. 24. For example, as shown in the image below, both Vision One and ThreatArmor receive packets from the Internet.

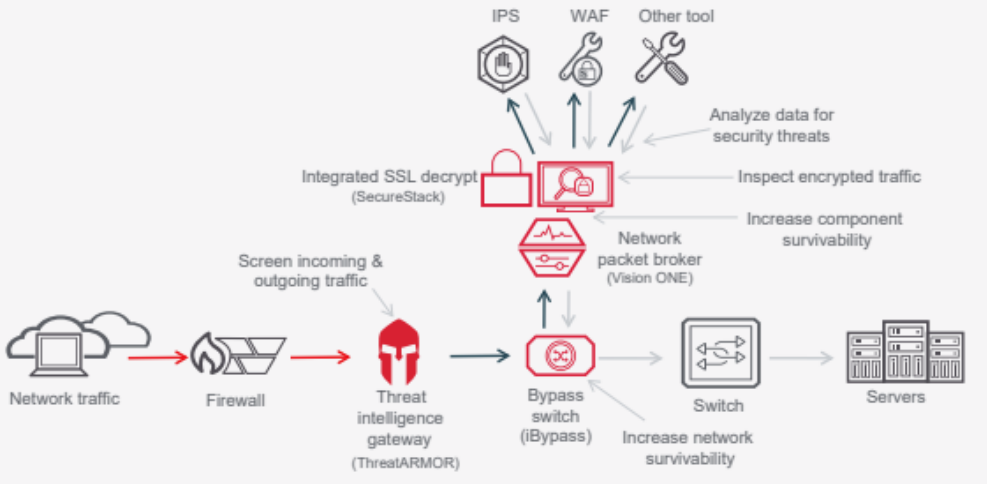


Figure 13. Ixia's inline security solution

Ex. 76 at 29.

103. The ’917 Accused Products use Keysight’s threat intelligence technology and receive updated threat information from Keysight’s ATI servers. The ’917 Accused Products determine whether a packet corresponds to packet-filtering rule(s). The ’917 Accused Products use threat-intelligence based rules to inspect packets and apply an operator that allows or drops a packet. The ‘917 Accused Products also generate a packet log entry with a threat indicator and data indicating whether the packet was allowed or dropped. https://www.youtube.com/watch?v=aKnotioCHlg&t=4s; https://www.youtube.com/watch?v=_TbHu8-exZQ&t=17s; Ex. 77 at 3; Ex. 57; *see also* Ex. 54.

104. The ’917 Accused Products update a packet flow entry associated with a threat identifier. For example, threat information associated with a packet flow is updated when it is aggregated, communicated, and/or displayed on a dashboard (associated with a computing device) or a SIEM system. *See, e.g.*, https://www.youtube.com/watch?v=aKnotioCHlg&t=4s; Ex. 78; Ex. 71; *see also* Ex. 79. Threat information associated with a packet flow can include IP addresses, explanations of why the IP addresses is malicious (e.g., in the form of a Rap

Sheet), among other information. *Id.* For example, the '917 Accused Products display packet flow analysis information (such as malicious IP addresses, the time that a threat is last seen) and data indicating whether the packets were blocked or allowed.

Ex. 78.

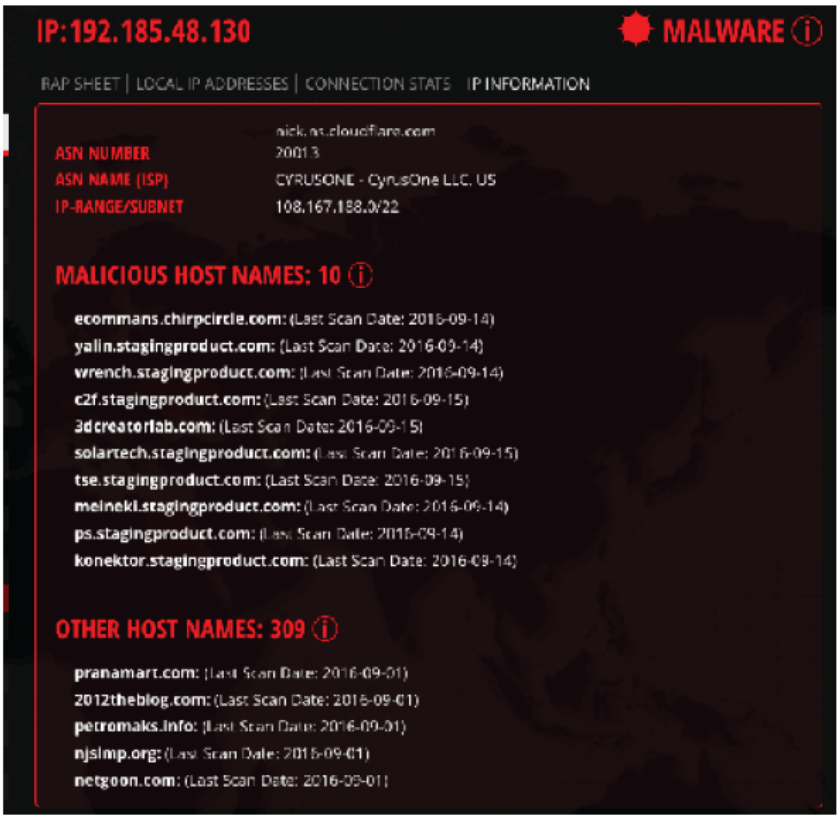
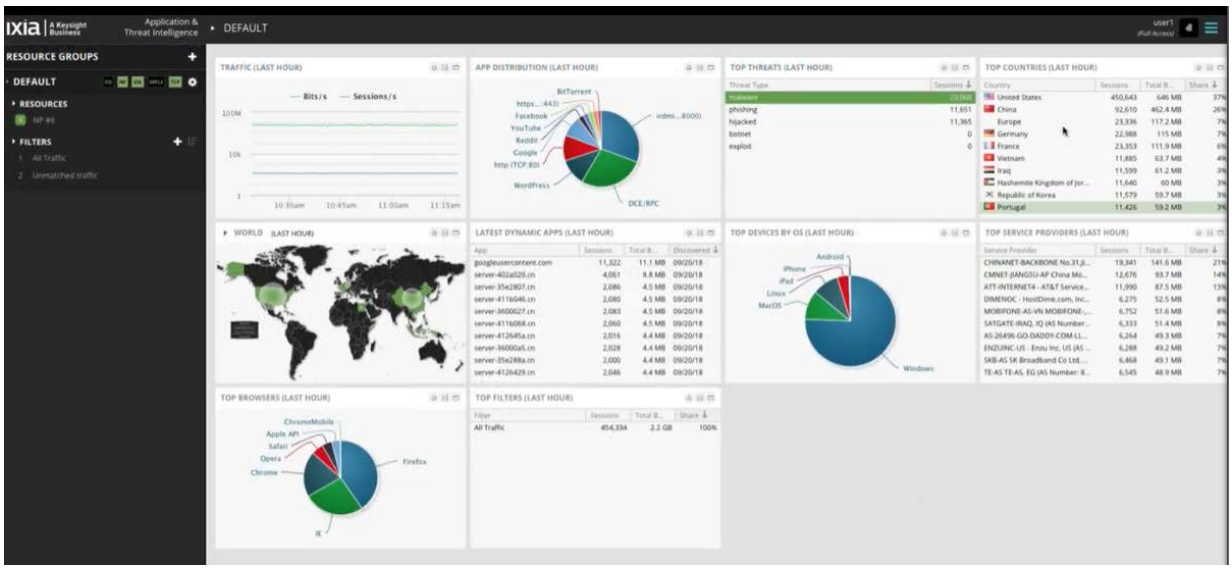


Fig. 1: Rap Sheet example of malicious activity

Ex. 71.



https://www.youtube.com/watch?v=_TbHu8-exZQ&t=17s; *see also* Ex. 79. As another

example, the Ixia Fabric Controller can display packet flow and the results of packet analysis because "IFC Centralized Manager can aid your historical trend analysis and capacity planning by gathering data in real time from discovered devices." Exs. 80-81.

105. As a result of Keysight's unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

106. Keysight has willfully infringed the '917 Patent. As discussed above in the preceding paragraphs, Centripetal is informed and believes that Keysight had knowledge of the '917 Patent through various channels, and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

107. Keysight thus knew or, in the alternative, was willfully blind to Centripetal's technology and the '917 Patent.

108. Despite this knowledge and/or willful blindness, Keysight has acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

109. 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. As such, Keysight has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '917 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

110. Keysight's infringement of the '917 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

111. Keysight's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

112. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

FOURTH CAUSE OF ACTION
(Indirect Infringement of the '917 Patent)

113. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

114. Keysight has induced and continues to induce infringement of one or more claims of the '917 Patent under 35 U.S.C. § 271(b). Keysight has contributorily infringed and continues to contributorily infringe one or more claims of the '917 Patent under 35 U.S.C. § 271(c).

115. 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 steps of the method claims, or provide one or more components of a system 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 execute the functions of one or more claims of the '917 Patent. Keysight instructs, directs and/or requires its customers, users,

and vendors to set up the system where the ’917 Accused Products cause another device, such as a user device, a SIEM system, ThreatArmor Central, or the Ixia Fabric Controller to display packet analysis information.

116. Keysight has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with Keysight, one or more claims of the ‘917 Patent.

117. 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 ‘917 Accused Products. Such use is consistent with how the Accused Products are described to directly infringe the ‘917 Patent and how the ‘917 Accused Products 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: (a) advising its customers and users to use the ‘917 Accused 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; (b) advertising and promoting the use of the ‘917 Accused Products in an infringing manner; and (c) distributing guidelines and instructions on how to setup the ‘917 Accused 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 obtains 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.

118. Keysight updates and maintains a support website that includes technical documentation encouraging the use of the '917 Accused Products in an infringing manner. This technical documentation includes knowledge articles, videos, user guides, technical support articles, and a knowledge center. The technical documentation covers the operation of the '917 Accused Products in-depth, including by advertising the '917 Accused Products' infringing features and instructing customers, users, and vendors to configure and use the Accused Products in an infringing manner. *See, e.g.*, Ex. 73 (https://www.keysight.com/us/en/support.html); Ex. 74 (https://support.keysight.com/s/?language=en_US); Ex. 75 (https://support.ixiacom.com/).

119. Keysight contributorily infringes the '917 Patent pursuant to 35 U.S.C. § 271(c) because it provides the '917 Accused Products as software and computer systems with software installed which act as a material component of the '917 Patent claims when combined with other components to create a complete network security system. Keysight knows that its products are particularly suited to be used in an infringing manner. The '917 Accused Products and their associated software are highly developed and 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.

120. 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 '917 Accused Products together with its customers, users, and vendors to meet the elements of the '917 Patent, as described above and incorporated by reference here. To the extent Keysight's 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 for CloudLens, which infringes when a third party runs this software on processors and memory in a cloud environment. As another example, Keysight sold the Testing products which infringe when a third party combines them for use with ThreatArmor or the Network Visibility products. To the extent Keysight's customers, users, and vendors direct and control the systems and methods in the claims, Keysight obtains 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.

121. Keysight's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

122. 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.

123. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

FIFTH CAUSE OF ACTION
(Direct Infringement of the '526 Patent pursuant to 35 U.S.C. § 271(a))

124. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

125. Keysight has infringed and continues to infringe at least one or more claims of the '526 Patent.

126. Keysight's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

127. Keysight's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

128. Keysight's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the '526 Patent, including, but not limited to the following products and services: the Network Visibility products, and the Testing products, and any other products or services with Keysight's SecureStack and Threat Insights technologies (the "'526 Accused Products"). Keysight also infringes these claims jointly with its customers, users, and vendors. Keysight directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, Keysight puts the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

129. The '526 Accused Products embody the patented invention of the '526 Patent and infringe the '526 Patent because they determine, by an apparatus system with at least one processor; and memory comprising instructions that, when executed by the at least one

processor, cause the apparatus to: store a list of identification data and at least one corresponding action to perform on encrypted communication flows associated with each corresponding identification data; receive one or more packets initiating at least one encrypted communication flow; identify flow identification data associated with the one or more packets initiating the at least one encrypted communication flow; compare the identified flow identification data with the list of identification data; decrypt, based on comparing the identified flow identification data with the list of the identification data resulting in a match with data of the list, each packet of an encrypted communication flow associated with the match with data of the list and performing a corresponding action on each packet of the encrypted communication flow associated with the match with data of the list; and re-encrypt, after performing the corresponding action, each packet of the encrypted communication flow associated with the match with data of the list and transmit each packet of the encrypted communication flow to its intended destination.

130. The ‘526 Accused Products are, or run on, computers with processors and memory (including RAM and a hard drive) that store instructions executed by the processors.

131. The ‘526 Accused Products receive threat intelligence from ATI and store a list of identification data and associated actions.

Threat Intelligence

Today's organizations are under cyberattack. Malware can find its way into an organization in a multitude of ways including email, clicking on malicious links, mobile devices, USBs used by employees, as well as physical intrusions into a network. Cyber Security Ventures reported that ransomware will attack a business every 14 seconds by the end of 2019.

With our threat insights feature, you will be able to:

- Recognize malware, botnet, exploits, hijacked IPs and phishing activity with your Vision ONE, Vision X, Vision 7300, or CloudLens
- Send threat information automatically via NetFlow to existing security appliances

Threat intelligence from our Application and Threat Intelligence (ATI) Research Center, also used in Keysight's ThreatARMOR, provide what you need to secure your network without requiring any additional threat intelligence feed. You can ensure the security of your network by easily:

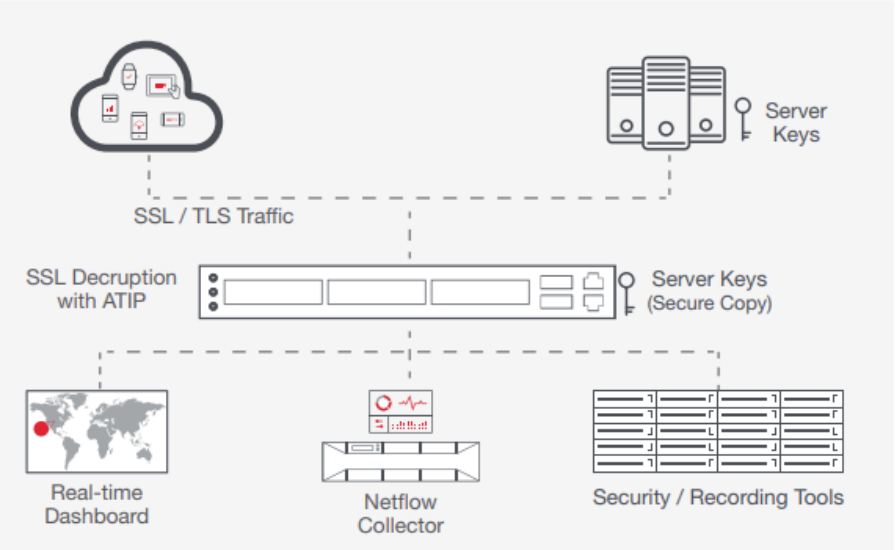
- Detecting IoT attacks
- Tagging suspicious or rogue applications and monitoring them for unusual activity
- Tracking traffic to or from unauthorized geographies
- Tracking questionable file transfers and brute-force attacks

Ex. 32; *see also* https://www.youtube.com/watch?v=_TbHu8-exZQ&t=17s; Ex. 57.

132. The ’526 Accused Products operate in a network to receive packets, including packets initiating encrypted communications flow. The ’526 Accused Products use threat intelligence to inspect packet data from the packets, such as flow identification data.

The Decryption Platform: Intelligent Network Packet Brokers (NPBs)

The stateful SSL decryption should be done using a dedicated platform, such as a network packet broker (NPB), which supports application intelligence with SSL decryption. Application intelligence is the ability to monitor packets based on application type and usage. It can be used to decrypt network packets, and dynamically identify the applications running (along with any malware that may be hidden by the encrypted traffic) on a network. And since the decryption is performed on a high performance specialized platform, there is no impact on network performance, nor on the performance of firewalls or other security products.



Ex. 82 at 6; *see also* Ex. 77 at 3 ("Recognize malware connections, botnets, exploits, hijacked IPs, and phishing activity").

133. The '526 Accused Products inspect packets with threat intelligence and decrypt packets if they meet certain criteria. The '526 Accused Products can send decrypted packet data to other tools, re-encrypt the packets, and send them to their intended destinations.

Using Active SSL, also known as an intermediary to both decrypt and re-encrypt traffic, is often referred to as using an "SSL Proxy."

Active SSL or an SSL proxy does the following:

- First, it terminates the SSL connection from the user to a given website, which decrypts traffic to cleartext.
- Then, it observes the decrypted traffic. In most cases, traffic is passed to security and monitoring tools for inspection.
- Once traffic has been inspected, it initiates a new SSL session to the external server, meaning it re-encrypts traffic to send it back onto the original path.

Ex. 83 at 4.

Scenario 4: Deployment of Active SSL Decryption

Decryption is another important scenario. Without active SSL/TLS decryption, inline security appliances (like an IPS, WAF, or UTM) cannot inspect encrypted traffic. Integrated decryption capabilities allow Ixia NPBs to decrypt traffic, send it to security appliances for inspection, then re-encrypt and return that traffic to the network for delivery. The solution is quick, simple, and easy.

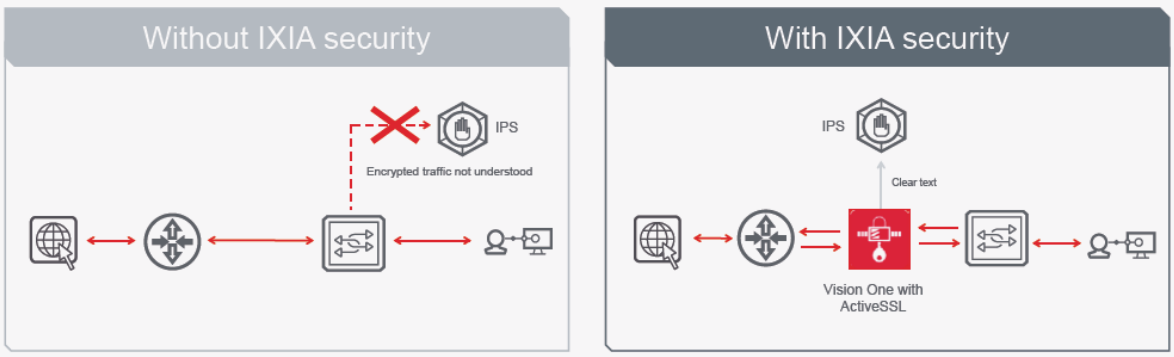


Figure 17. Decrypt and inspect traffic with an in-line monitoring tool

Ex. 76 at 31.

134. As a result of Keysight's unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

135. Keysight has willfully infringed the '526 Patent. As discussed above in the foregoing paragraphs, Centripetal is informed and believes that Keysight had knowledge of the

‘526 Patent through various channels, and despite its knowledge of Centripetal’s patent rights, engaged in egregious behavior warranting enhanced damages.

136. Keysight thus knew or, in the alternative, was willfully blind to Centripetal’s technology and the ‘526 Patent.

137. Despite this knowledge and/or willful blindness, Keysight has acted with blatant and egregious disregard for Centripetal’s patent rights with an objectively high likelihood of infringement.

138. 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. As such, Keysight has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the ‘526 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys’ fees and costs incurred under 35 U.S.C. § 285.

139. Keysight’s infringement of the ‘526 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

140. Keysight’s infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

141. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

SIXTH CAUSE OF ACTION
(Indirect Infringement of the '526 Patent)

142. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

143. Keysight has induced and continues to induce infringement of one or more claims of the '526 Patent under 35 U.S.C. § 271(b). Keysight has contributorily infringed and continues to contributorily infringe one or more claims of the '526 Patent under 35 U.S.C. § 271(c).

144. 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 steps of the method claims, or provide one or more components of a system 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 execute the functions of one or more claims of the '526 Patent. 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.

145. Keysight has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with Keysight, one or more claims of the '526 Patent.

146. 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 '526 Accused Products. Such use is consistent with how the '526 Accused Products are described to directly infringe the '526 Patent and how the '526 Accused Products 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: (a) advising its customers and users to use the '526 Accused 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; (b) advertising and promoting the use of the '526 Accused Products in an infringing manner; and (c) distributing guidelines and instructions on how to setup the '526 Accused 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 obtains 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.

147. Keysight updates and maintains a support website that includes technical documentation encouraging the use of the '526 Accused Products in an infringing manner. This technical documentation includes knowledge articles, videos, user guides, technical support articles, and a knowledge center. The technical documentation covers the operation of the '526 Accused Products in-depth, including by advertising the '526 Accused Products' infringing features and instructing customers, users, and vendors to configure and use the '526 Accused Products in an infringing manner. *See, e.g.*, Ex. 73

(https://www.keysight.com/us/en/support.html); Ex. 74 (https://support.keysight.com/s/?language=en_US); Ex. 75 (https://support.ixiacom.com/).

148. Keysight contributorily infringes the '526 Patent pursuant to 35 U.S.C. § 271(c) because it provides the '526 Accused Products as software and computer systems with software installed which act as a material component of the '526 Patent claims when combined with other components to create a complete network security system. Keysight knows that its products are particularly suited to be used in an infringing manner. The '526 Accused Products and their associated software are highly developed and 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.

149. 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 '526 Accused Products together with its customers, users, and vendors to meet the elements of the '526 Patent, as described above and incorporated by reference here. To the extent Keysight's 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), which is a material component that can be combined with other components, such as Keysight's Threat Insight to create an infringing system. As another example, Keysight sold the Testing products which infringe when a third party combines them for use with

ThreatArmor or Network Visibility products. To the extent Keysight's customers, users, and vendors direct and control the systems and methods in the claims, Keysight obtains benefits from the control of the system as a whole. For example, Keysight's other products, such as ThreatArmor, can use the decrypted packet information to provide analytics, which enables them to analyze information from the encrypted packets. 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.

150. Keysight's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

151. 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.

152. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

SEVENTH CAUSE OF ACTION
(Direct Infringement of the '572 Patent pursuant to 35 U.S.C. § 271(a))

153. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

154. Keysight has infringed and continues to infringe at least one or more claims of the ‘572 Patent.

155. Keysight’s infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

156. Keysight’s acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

157. Keysight’s infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal’s technology covered by the ’572 Patent, including, but not limited to the following products and services: the Network Visibility products, the Ixia Fabric Controller, and the Testing products, and any other products or services with Keysight’s NetStack, AppStack, SecureStack, and the ATI technology (the “’572 Accused Products”). Keysight also infringes these claims jointly with its customers, vendors, distributors, and subsidiaries. Keysight directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, Keysight puts the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

158. The ‘572 Accused Products embody the patented invention of the ‘572 Patent and infringe the ‘572 Patent because they include a network device with at least one processor; and memory storing instructions that when executed by the at least one processor cause the system to: receive a first rule set; modify the first rule set; configure the network device to process packets in accordance with the first rule set; receive, after modifying the first rule set and the configuring of the network device to process packets in accordance with the first rule

set, a plurality of packets; process a first portion of the plurality of packets in accordance with the first rule set; receive a second rule set; modify the second rule set; and based on a signal to process packets in accordance with the second rule set: cease processing of one or more packets of the plurality of packets; cache the one or more packets of the plurality of packets; reconfigure the at least one processor to process packets in accordance with the second rule set; and after completion of the reconfiguring of the at least one processor to process packets in accordance with the second rule set, process the one or more cached packets in accordance with the second rule set .

159. The ‘572 Accused Products are, or run on, computers with processors and memory (including RAM and a hard drive) that store instructions executed by the processors.

160. The ’572 Accused Products receive rule sets, modify rule sets and configure a network device, such as the Network Visibility products or the Testing products with rule sets. For example, the ’572 Accused Products utilize Keysight’s ATI technology, which receives and modifies rule sets based on threat intelligence information. *See, e.g.*, Ex. 39; Ex. 84. The rule sets can be dynamically provided to network devices based on the threat intelligence information. *See, e.g.*, Ex. 39 (“Our Application and Threat Intelligence (ATI) subscription service provides up-to-the-moment threat intelligence.”); Exs. 32-33; *see also* Ex. 85 at 4. As another example, the Ixia Fabric Controller receives, modifies, and configures the Network Visibility products with rule sets. Exs. 80-81. As yet another example, the Network Visibility products receive and modify rule sets, and configure the devices with the hitless change feature. Ex. 31; Ex. 24.

161. The ’572 Accused Products receive packets and process the packets based on rule sets. *See, e.g.*, https://www.youtube.com/watch?v=_TbHu8-exZQ&t=17s; Ex. 77 at 3; Ex. 57; Exs. 34-35.

162. When the ’572 Accused Products swap rule sets, the ’572 Accused Products cease processing packets, cache packets, reconfigure the device’s processor(s) with the new rule set and process the packets with the new rule set. *See, e.g.*, Ex. 24. Using the ’572 Patent’s technology, the ’572 Accused Products swap rule sets without dropping packets with the hitless change feature. Ex. 31; Ex. 24.

163. As a result of Keysight’s unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

164. Keysight has willfully infringed the ‘572 Patent. As discussed above in the preceding paragraphs, Centripetal is informed and believes that Keysight had knowledge of the ‘572 Patent through various channels, and despite its knowledge of Centripetal’s patent rights, engaged in egregious behavior warranting enhanced damages.

165. Keysight thus knew or, in the alternative, was willfully blind to Centripetal’s technology and the ‘572 Patent.

166. Despite this knowledge and/or willful blindness, Keysight has acted with blatant and egregious disregard for Centripetal’s patent rights with an objectively high likelihood of infringement.

167. Centripetal is informed and believes that Keysight has undertaken no efforts to design these products or services around the ‘572 Patent to avoid infringement despite Keysight’s knowledge and understanding that its products and services infringe the ‘572

Patent. As such, Keysight has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '572 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

168. Keysight's infringement of the '572 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

169. Keysight's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

170. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

EIGHTH CAUSE OF ACTION
(Indirect Infringement of the '572 Patent)

171. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

172. Keysight has induced and continues to induce infringement of one or more claims of the '572 Patent under 35 U.S.C. § 271(b). Keysight has contributorily infringed and continues to contributorily infringe one or more claims of the '572 Patent under 35 U.S.C. § 271(c).

173. Keysight has induced infringement of the '572 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 steps of the method claims, or provide one or more components of a system 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 execute the functions of one or more claims of the ’572 Patent. 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 hitless change) to perform one or more steps in the claims of the ’572 Patent.

174. Keysight has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with Keysight, one or more claims of the ‘572 Patent.

175. Keysight has knowingly and actively aided and abetted the direct infringement of the ‘572 Patent by instructing and encouraging its customers, users, and vendors to meet the elements of the ‘572 Patent with the ‘572 Accused Products. Such use is consistent with how the Accused Products are described to directly infringe the ‘572 Patent and how the ‘572 Accused Products 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: (a) advising its customers and users to use the ‘572 Accused 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; (b) advertising and promoting the use of the ‘572 Accused Products in an infringing manner; and (c) distributing guidelines and instructions on how to setup the ‘572 Accused 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 obtains 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.

176. Keysight updates and maintains a support website that includes technical documentation encouraging the use of the '572 Accused Products in an infringing manner. This technical documentation includes knowledge articles, videos, user guides, technical support articles, and a knowledge center. The technical documentation covers the operation of the '572 Accused Products in-depth, including by advertising the '572 Accused Products' infringing features and instructing customers, users, and vendors to configure and use the '572 Accused Products in an infringing manner. *See, e.g.*, Ex. 73 (https://www.keysight.com/us/en/support.html); Ex. 74 (https://support.keysight.com/s/?language=en_US); Ex. 75 (https://support.ixiacom.com/).

177. Keysight contributorily infringes the '572 Patent pursuant to 35 U.S.C. § 271(c) because it provided its '572 Accused Products as software and computer systems with software installed which act as a material component of the '572 Patent claims when combined with other components to create a complete network security system. Keysight knows that its products are particularly suited to be used in an infringing manner. The '572 Accused Products and their associated software are highly developed and 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 '572 Patent.

178. Keysight has knowingly and actively contributed to the direct infringement of the '572 Patent by its manufacture, use, offer to sell, sale and importation of the '572 Accused

Products together with its customers, users, and vendors to meet the elements of the '572 Patent, as described above and incorporated by reference here. To the extent Keysight's 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 for CloudLens, which infringes when a third party runs this software on processors and memory in a cloud environment. As another example, Keysight sold the Testing products which infringe when a third party combines them for use with other Keysight's products, such as its Network Visibility products. To the extent Keysight's customers, users, and vendors direct and control the systems and methods in the claims, Keysight obtains 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. For example, Keysight is able to keep the performance of its products without needing to bring them offline for rule updates or otherwise miss network traffic.

179. Keysight's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

180. Keysight has known or, in the alternative, has been willfully blind to Centripetal's technology and the '572 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 '572 Patent to avoid infringement despite Keysight's knowledge and understanding that its products and services infringe the '572 Patent.

181. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

NINTH CAUSE OF ACTION
(Direct Infringement of the '343 Patent pursuant to 35 U.S.C. § 271(a))

182. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

183. Keysight has infringed and continues to infringe at least one or more claims of the '343 Patent.

184. Keysight's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

185. Keysight's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

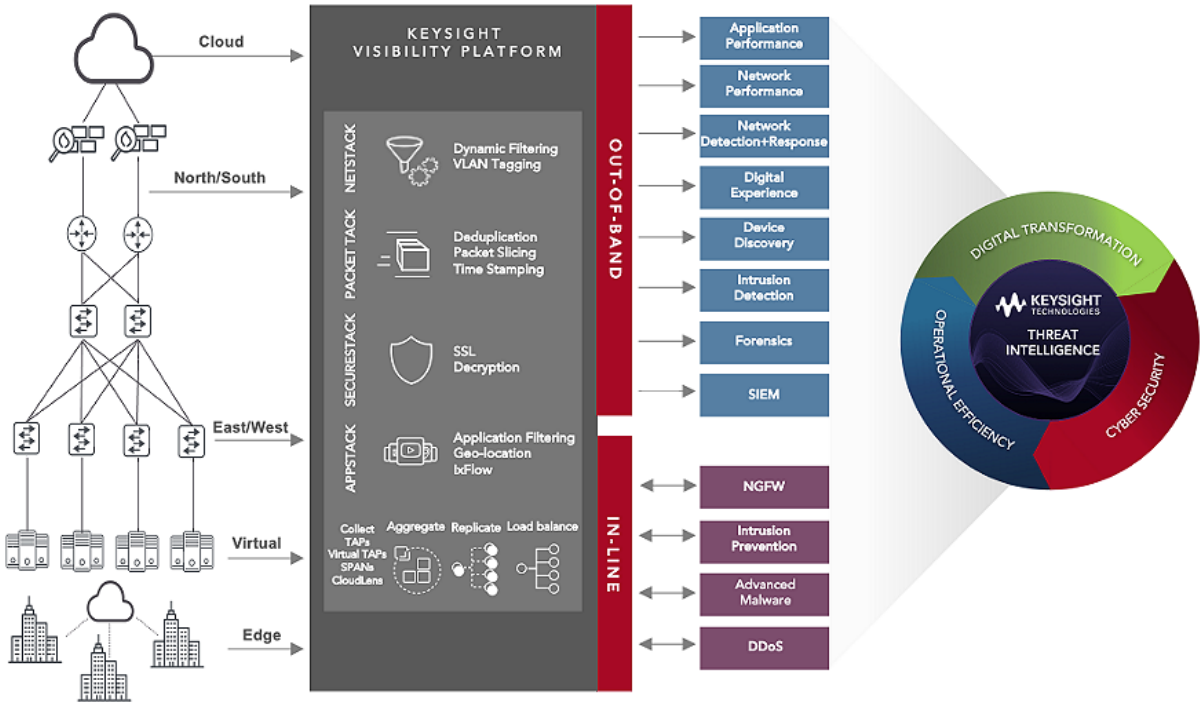
186. Keysight's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the '343 Patent, including, but not limited to the following products and services: the Network Visibility products, and the Testing products, and any other products or services with Keysight's AppStack, SecureStack, packet-filtering and the ATI technology (the "'343 Accused Products"). Keysight also infringes these claims jointly with its customers, vendors, distributors, subsidiaries, and/or other agents of Keysight, to the extent specific components are provided by those customers or vendors. Keysight directs and controls the systems and

methods in the claims and obtains benefits from the control of the system as a whole. In particular, Keysight puts the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

187. The ’343 Accused Products embody the patented invention of the ’343 Patent and infringe the ’343 Patent because they include at least one processor; and memory comprising instructions that, when executed by the one or more processors, cause the apparatus to: receive a plurality of packets; determine, based on a packet header field value, whether the plurality of packets comprises data corresponding to first criterion specified by one or more packet-filtering rules; responsive to a determination that a packet header field value of a first portion of packets comprises data corresponding to the first criterion specified by at least one matching packet-filtering rule, apply, to each packet in the first portion of packets, one or more operators specified by the at least one matching packet-filtering rule; determine, based on an application header field value, a second portion of packets based on whether the first portion of packets comprises data corresponding to second criterion specified by one or more operators specified by the at least one matching packet-filtering rule; and responsive to determining the second portion of packets that comprises data corresponding to the second criterion specified by one or more operators specified by the at least one matching packet-filtering rule, apply, to each packet in the second portion of packets, at least one packet transformation function configured to prevent an exfiltration operation, wherein the at least one packet transformation function indicates whether each packet in the second portion of packets is allowed to continue toward its destination.

188. The ’343 Accused Products include system components that include one or more processors and memory, including instructions. For example, the Network Visibility products are appliances which have processors and memories. Ex. 24. The Testing products also run on appliances which have processors and memories. *See, e.g.*, Ex. 86 at 53.

189. The ’343 Accused Products prevent a variety of threats, including data exfiltration and data loss.



Ex. 37. For example, the ’343 Accused Products can cause packets to be dropped or diverted if they are associated with a threat.

190. The ’343 Accused Products apply threat intelligence based rules to inspect packets. For example, the ’343 Accused Products receive packets, determine whether the packet information matches a packet filtering rule based on the packet header field value, and apply an operator on the packet based on the packet filtering rule. https://www.youtube.com/watch?v=_TbHu8-exZQ&t=17s; Ex. 77 at 3; Ex. 57.

191. The ’343 Accused Products inspect packets in a flow based on application header field value. The inspection can occur using the AppStack technology. *See, e.g.*, Exs. 34-35 (“our capabilities allow filtering based on L2 through L7”).

192. As a result of Keysight’s unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

193. Keysight has willfully infringed the ‘343 Patent. As discussed above in the preceding paragraphs, Centripetal is informed and believes that Keysight had knowledge of the ‘343 Patent through various channels, and despite its knowledge of Centripetal’s patent rights, engaged in egregious behavior warranting enhanced damages.

194. Keysight thus knew or, in the alternative, was willfully blind to Centripetal’s technology and the ‘343 Patent.

195. Despite this knowledge and/or willful blindness, Keysight has acted with blatant and egregious disregard for Centripetal’s patent rights with an objectively high likelihood of infringement.

196. Centripetal is informed and believes that Keysight has undertaken no efforts to design these products or services around the ‘343 Patent to avoid infringement despite Keysight’s knowledge and understanding that its products and services infringe the ‘343 Patent. As such, Keysight has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the ‘343 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys’ fees and costs incurred under 35 U.S.C. § 285.

197. Keysight's infringement of the '343 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

198. Keysight's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

199. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

TENTH CAUSE OF ACTION
(Indirect Infringement of the '343 Patent)

200. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

201. Keysight has induced and continues to induce infringement of one or more claims of the '343 Patent under 35 U.S.C. § 271(b). Keysight has contributorily infringed and continues to contributorily infringe one or more claims of the '343 Patent under 35 U.S.C. § 271(c).

202. Keysight has induced infringement of the '343 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 steps of the method claims, or provide one or more components of a system 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 execute the functions of one or more claims of the '343 Patent. Keysight instructs, directs and/or requires its customers, users,

and vendors, or some combination thereof, to set up the system to analyze packets based on packet header field value and application header field value. 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 '343 Accused Products, such as the AppStack functions, to perform one or more steps in the claims of the '343 Patent. Keysight has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with Keysight, one or more claims of the '343 Patent.

203. Keysight has knowingly and actively aided and abetted the direct infringement of the '343 Patent by instructing and encouraging its customers, users, and vendors to meet the elements of the '343 Patent with the Accused Products. Such use is consistent with how the Accused Products are described to directly infringe the '343 Patent and how the Accused Products 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: (a) advising its customers and users to use the '343 Accused 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; (b) advertising and promoting the use of the '343 Accused Products in an infringing manner; and (c) distributing guidelines and instructions on how to setup the '343 Accused 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 obtains 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.

204. Keysight updates and maintains a support website that includes technical documentation encouraging the use of the '343 Accused Products in an infringing manner. This technical documentation includes knowledge articles, videos, user guides, technical support articles, and a knowledge center. The technical documentation covers the operation of the '343 Accused Products in-depth, including by advertising the '343 Accused Products' infringing features and instructing customers, users, and vendors to configure and use the Accused Products in an infringing manner. *See, e.g.*, Ex. 73 (https://www.keysight.com/us/en/support.html); Ex. 74 (https://support.keysight.com/s/?language=en_US); Ex. 75 (https://support.ixiacom.com/).

205. Keysight contributorily infringes the '343 Patent pursuant to 35 U.S.C. § 271(c) because it provided its '343 Accused Products as software and computer systems with software installed, which act as a material component of the '343 Patent claims when combined with other components to create a complete network security system. Keysight knows that its products are particularly suited to be used in an infringing manner. The '343 Accused Products and their associated software are highly developed and 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 '343 Patent.

206. Keysight has knowingly and actively contributed to the direct infringement of the '343 Patent by its manufacture, use, offer to sell, sale and importation of the '343 Accused Products together with its customers, users, and vendors to meet the elements of the '343

Patent, as described above and incorporated by reference here. To the extent Keysight's 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 for CloudLens, which infringes when a third party runs this software on processors and memory in a cloud environment. As another example, Keysight sold the Network Visibility products and the Testing products, which infringe when a third party combines them for use. To the extent Keysight's customers, users, and vendors direct and control the systems and methods in the claims, Keysight obtains 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.

207. Keysight's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

208. Keysight has known or, in the alternative, has been willfully blind to Centripetal's technology and the '343 Patent. Centripetal is informed and believes that Keysight has undertaken no efforts to design these products or services around the '343 Patent to avoid infringement despite Keysight's knowledge and understanding that its products and services infringe the '343 Patent.

209. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

ELEVENTH CAUSE OF ACTION
(Direct Infringement of the '062 Patent pursuant to 35 U.S.C. § 271(a))

210. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

211. Keysight has infringed and continues to infringe at least one or more claims of the '062 Patent.

212. Keysight's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

213. Keysight's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

214. Keysight's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the '062 Patent, including, but not limited to the following products and services: the Network Visibility products, the ThreatArmor Suite, the Testing products, and the Ixia Fabric Controller, and any other products or services with Keysight's AppStack, SecureStack, and the ATI technology (the "'062 Accused Products"). Keysight also infringes these claims jointly with its customers, users, and vendors. Keysight directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, Keysight put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

215. The '062 Accused Products embody the patented invention of the '062 Patent and infringe the '062 Patent because they include packet filtering device that includes at least one processor; and memory comprising instructions that, when executed by the one or more

processors, cause the packet filtering device to: receive a plurality of packet filtering rules configured to cause the packet filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators, wherein the plurality of network-threat indicators are associated with network-threat-intelligence reports supplied by one or more independent network-threat-intelligence providers; receive a plurality of packets that comprises a first packet and a second packet; responsive to a determination that the first packet satisfies a first packet filtering rule, of the plurality of packet filtering rules, based on one or more network-threat indicators, of the plurality of network-threat indicators, specified by the first packet filtering rule: apply, to the first packet, an operator specified by the first packet filtering rule and configured to cause the packet filtering device to allow the first packet to continue toward a destination of the first packet; and communicate information that identifies the one or more network-threat indicators and data indicative that the first packet was allowed to continue toward the destination of the first packet; cause, in an interface, display of the information in at least one portion of the interface corresponding to the packet filtering rule and the one or more network-threat indicators; receive, based on user selection of the at least one portion of the interface, an update to the first packet filtering rule; modify, based on the received update to the first packet filtering rule, at least one operator specified by the first packet filtering rule to reconfigure the packet filtering device to prevent packets corresponding to the one or more network-threat indicators from continuing toward their respective destinations; and responsive to a determination that the second packet satisfies the first packet filtering rule: based on the modified at least one operator specified by the first packet filtering rule, prevent the second packet from continuing toward a destination of the second packet; and communicate data

indicative that the second packet was prevented from continuing toward the destination of the second packet.

216. The '062 Accused Products include a packet-filtering device. For example, the Network Visibility products are packet-filtering devices that sit in a communication link and filter packets. *See, e.g.*, Ex. 24. ThreatArmor is a threat intelligence gateway that filters inbound and outbound packets. Ex. 52 at 1. The Testing products include the functionalities of the Network Visibility products, such as those in Vision One. For example, the Testing products analyze threats in packets when they "[v]alidate the security posture of your networks with real applications and a complete range of threat vectors." The '062 Accused Products are, or run on, computers with processors and memory (including RAM and a hard drive) that stores instructions executed by the processors.

217. The '062 Accused Products have the ATI technology and receive data feeds from the ATI Center. The ATI Center provides continuously updated threat intelligence feeds based on network threat information from threat intelligence providers.

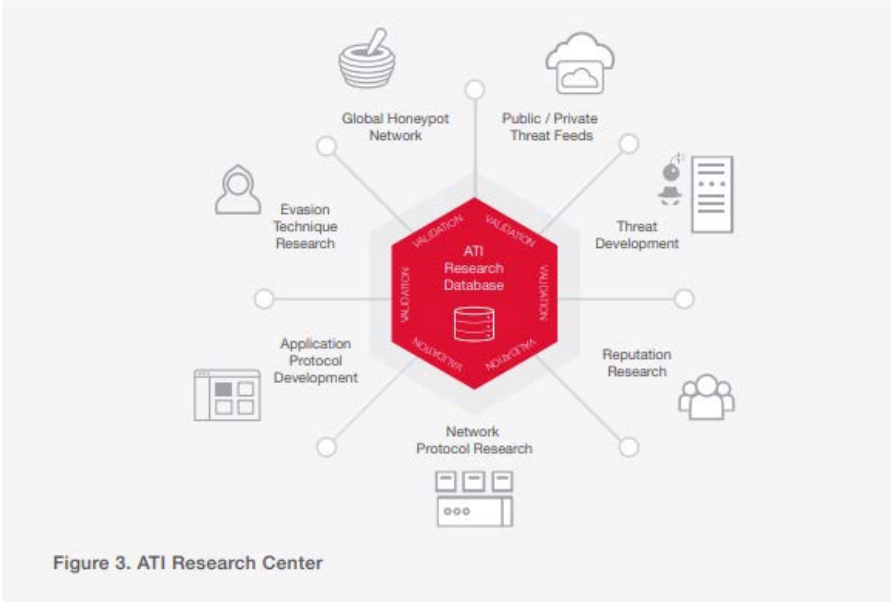
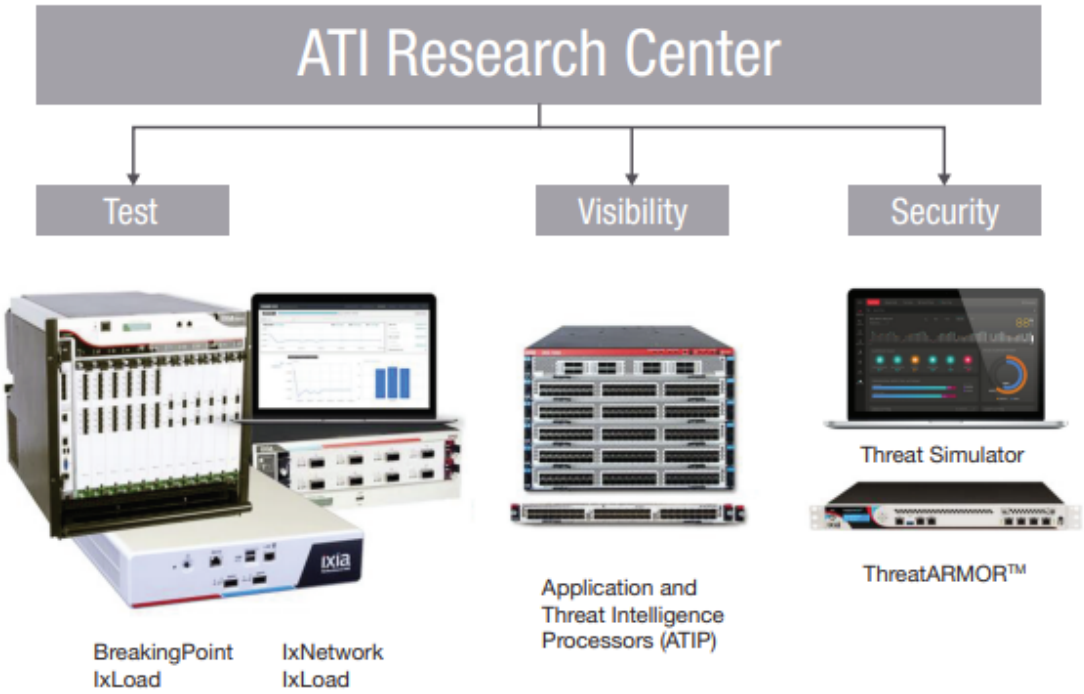


Figure 3. ATI Research Center

Source Feeds are collected from different public and private streams, including commercial Threat Intelligence feeds which some users and security vendors apply without further validation. The ATI Research Center also collects feed data from the open-source community and various security partnerships. Of course, the data from these feeds are just considered suspects – they aren't treated as criminal until the ATI Research Center has validated each one individually.

Ex. 84 at 4; *see also*, Ex. 39 ("From proprietary research, we aggregate newly discovered attacks and malware, providing application insights that include protocols, security attacks, and product enhancements on 400+ applications."); Ex. 57

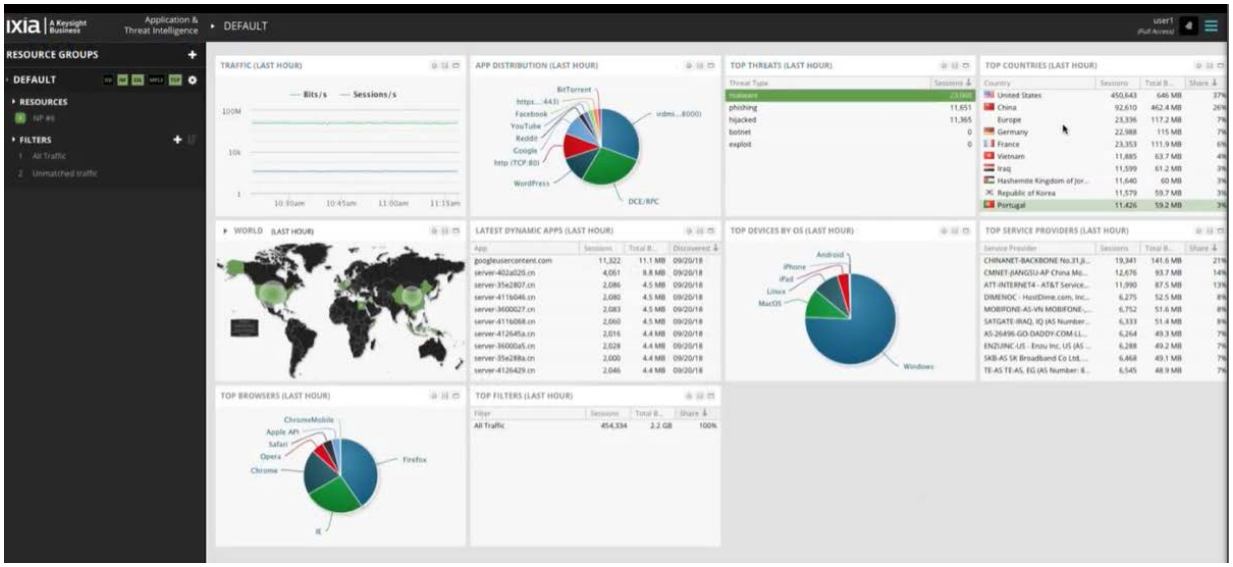


The reach of the ATI research center spans Keysight product lines to ensure the most up-to-date application and threat intelligence.

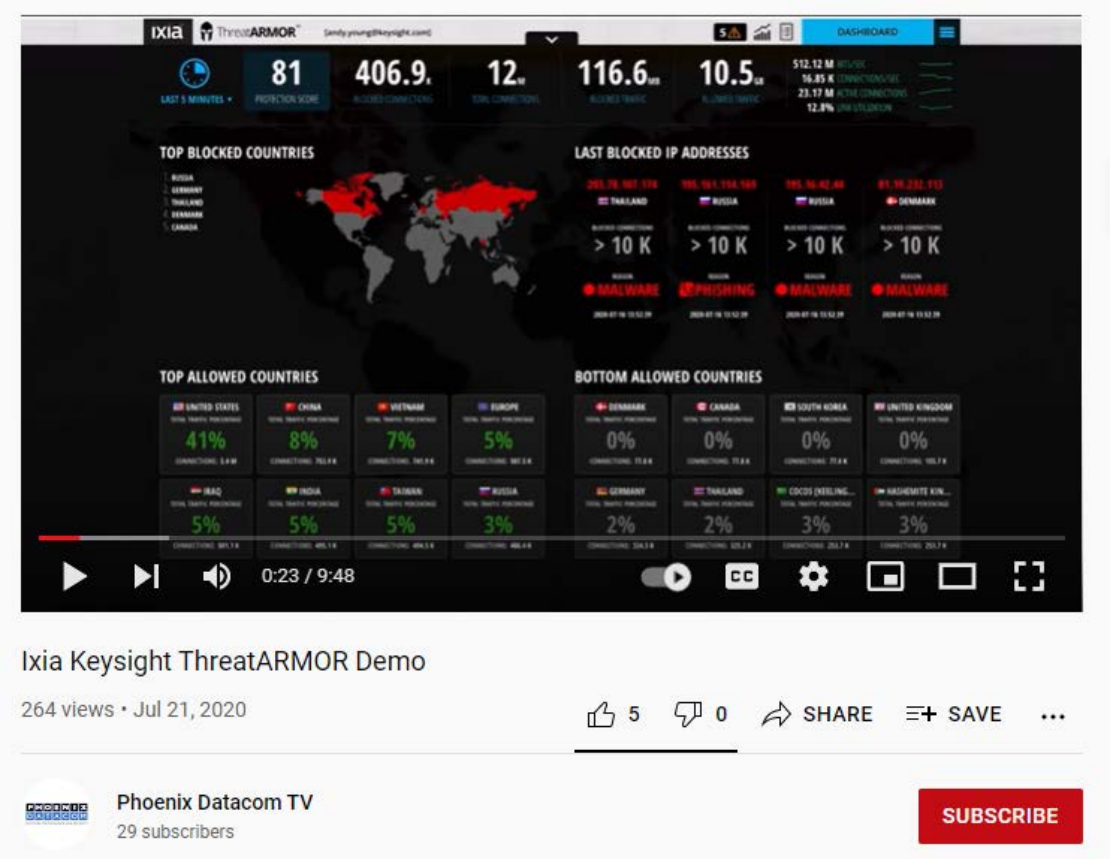
Ex. 85 at 4.

218. The ’062 Accused Products use threat-intelligence based rules to inspect packet information, apply operators to allow or drop a packet, and communicate information identifying a threat indicator (e.g., IP address associated with the threat indicator) and whether the packet is allowed or dropped. https://www.youtube.com/watch?v=aKnotioCHlg&t=4s; https://www.youtube.com/watch?v=_TbHu8-exZQ&t=17s; Ex. 77 at 3; Ex. 57; *see also* Ex. 54.

219. The ’062 Accused Products cause an interface to display threat related information. For example, the ’062 Accused Products cause a dashboard or a SIEM system to display information corresponding to the packet filtering rule (e.g., allow or block) and the associated network threat indicator (e.g., IP addresses or countries) as shown below.



https://www.youtube.com/watch?v=_TbHu8-exZQ&t=17s



https://www.youtube.com/watch?v=aKnotioCHlg&t=4s; *see also* Ex. 79.

Rap Sheets Describe Network Risks

Whenever ThreatARMOR blocks traffic to or from a known-bad site, a Rap Sheet is provided to explain why that IP address is considered bad. This helps customers better understand the risks facing their network and also avoid the risk of false positive. ThreatARMOR only blocks an IP address if the ATI Research Center has 100% certainty there is malicious or criminal activity at that site, and the Rap Sheet details the proof. The Rap Sheets themselves provide information such as the URL information of individual threats, the binary checksum of that malware, screen shots of a phishing page or malware installer, and the last date the individual piece of malicious activity was validated.

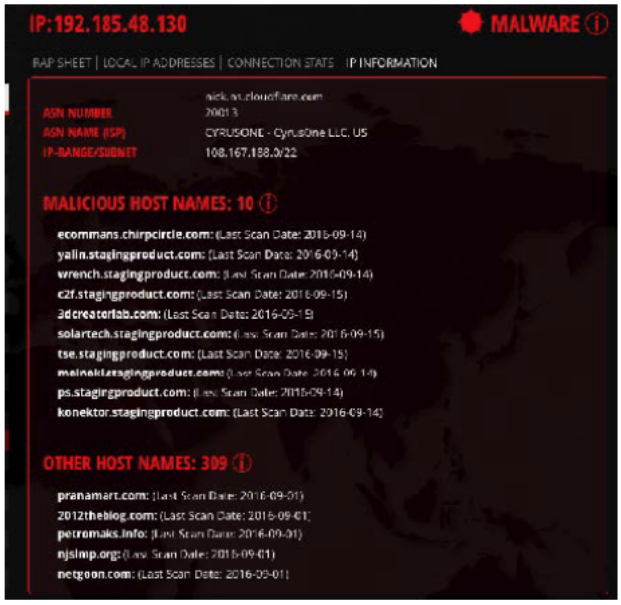


Figure 1. Rap Sheet example of malicious activity

Ex. 84 at 2. As another example, the Ixia Fabric Controller can display packet analysis information because its "IFC Centralized Manager can aid your historical trend analysis and capacity planning by gathering data in real time from discovered devices." Exs. 80-81.

220. The '062 Accused Products receive updates to the packet filtering rules and make a determination on the packets based on the updated rules. For example, the '062 Accused Products allow a user to configure ATI updates, which will cause them to receive updates to packet filtering rules. As another example, the '062 Accused Products allow a user to view analytics of threat information and a user can select one or more countries for blocking. https://www.youtube.com/watch?v=aKnotioCHlg; Ex. 87 ("ThreatARMOR can: . . . block

malicious IP addresses manually or automatically from SIEM tools"); *see also* https://www.youtube.com/watch?v=_TbHu8-exZQ&t=17s.

221. The '062 Accused Products modify an action to be taken on packets so that it will block packets from certain countries or IP addresses. *Id.* ThreatArmor can also receive updated threat feeds that cause it to prevent packets corresponding to network-threat indicators in the threat feeds to reach their destination. Ex. 84 at 2 ("…Ixia collects, validates, and distributes real-time information on global threats through the ATI Research Center.")

222. As a result of Keysight's unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

223. Keysight has willfully infringed the '062 Patent. As discussed above in the preceding paragraphs, Centripetal is informed and believes that Keysight had knowledge of the '062 Patent through various channels, and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

224. Keysight thus knew or, in the alternative, was willfully blind to Centripetal's technology and the '062 Patent.

225. Despite this knowledge and/or willful blindness, Keysight has acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

226. Centripetal is informed and believes that Keysight has undertaken no efforts to design these products or services around the '062 Patent to avoid infringement despite Keysight's knowledge and understanding that its products and services infringe the '062 Patent. As such, Keysight has acted and continues to act recklessly, willfully, wantonly,

deliberately, and egregiously engage in acts of infringement of the '062 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

227. Keysight's infringement of the '062 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

228. Keysight's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

229. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

TWELFTH CAUSE OF ACTION
(Indirect Infringement of the '062 Patent)

230. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

231. Keysight has induced and continues to induce infringement of one or more claims of the '062 Patent under 35 U.S.C. § 271(b). Keysight has contributorily infringed and continues to contributorily infringe one or more claims of the '062 Patent under 35 U.S.C. § 271(c).

232. Keysight has induced infringement of the '062 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 steps of the method claims, or provide one or more components of a system 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 execute the functions of one or more claims of the ’062 Patent. Keysight instructs, directs and/or requires its customers, users, and vendors to set up the system where the ’062 Accused Products cause another device, such as a user device, a SIEM system, ThreatArmor Central Management, or Ixia Fabric Controller to display packet analysis information. Keysight further instructs, directs and/or requires its customers, users, and vendors to set up the system to receive and update packet filtering rules.

233. Keysight has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with Keysight, one or more claims of the ‘062 Patent.

234. Keysight has knowingly and actively aided and abetted the direct infringement of the ‘062 Patent by instructing and encouraging its customers, users, and vendors to meet the elements of the ‘062 Patent with the ’062 Accused Products. Such use is consistent with how the Accused Products are described to directly infringe the ‘062 Patent and how the ’062 Accused Products 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: (a) advising its customers and users to use the ‘062 Accused 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; (b) advertising and promoting the use of the ‘062 Accused Products in an infringing manner; and (c) distributing guidelines and instructions on how to setup the ‘062 Accused 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 obtains 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.

235. Keysight updates and maintains a support website that includes technical documentation encouraging the use of the '062 Accused Products in an infringing manner. This technical documentation includes knowledge articles, videos, user guides, technical support articles, and a knowledge center. The technical documentation covers the operation of the '062 Accused Products in-depth, including by advertising the '062 Accused Products' infringing features and instructing customers, users, and vendors to configure and use the '062 Accused Products in an infringing manner. *See, e.g.*, Ex. 73 (https://www.keysight.com/us/en/support.html); Ex. 74 (https://support.keysight.com/s/?language=en_US); Ex. 75 (https://support.ixiacom.com/).

236. Keysight contributorily infringes the '062 Patent pursuant to 35 U.S.C. § 271(c) because it provided its '062 Accused Products as software and computer systems with software installed which act as a material component of the '062 Patent claims when combined with other components to create a complete network security system. Keysight knows that its products are particularly suited to be used in an infringing manner. The '062 Accused Products and their associated software are highly developed and 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 '062 Patent.

237. Keysight has knowingly and actively contributed to the direct infringement of the '062 Patent by its manufacture, use, offer to sell, sale and importation of the '062 Accused

Products together with its customers, users, and vendors to meet the elements of the '062 Patent, as described above and incorporated by reference here. To the extent Keysight's 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. As another example, Keysight sold the Testing products which infringe when a third party combines them for use with ThreatArmor or the Network Visibility products. 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 for CloudLens, which infringes when a third party runs this software on processors and memory in a cloud environment. To the extent Keysight's customers, users, and vendors direct and control the systems and methods in the claims, Keysight obtains 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.

238. Keysight's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

239. Keysight has known or, in the alternative, has been willfully blind to Centripetal's technology and the '062 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 '062 Patent

to avoid infringement despite Keysight's knowledge and understanding that its products and services infringe the '062 Patent.

240. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

THIRTEENTH CAUSE OF ACTION
(Direct Infringement of the '573 Patent pursuant to 35 U.S.C. § 271(a))

241. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

242. Keysight has infringed and continues to infringe at least one or more claims of the '573 Patent.

243. Keysight's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

244. Keysight's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

245. Keysight's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the '573 Patent, including, but not limited to the following products and services: the Network Visibility products, the Network Tap products, the Bypass Switch products, the ThreatArmor Suite, and the Testing products, and any other products or services with Keysight's AppStack, SecureStack, packet logging and correlation, and the ATI technology (the "'573 Accused Products"). Keysight also infringes these claims jointly with its customers, users, and vendors. Keysight directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, Keysight puts the systems and methods

described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

246. The ’573 Accused Products embody the patented invention of the ’573 Patent and infringe the ’573 Patent because they include a computing device which includes one or more processors; and memory comprising instructions that, when executed by the one or more processors, cause the computing device to: identify a plurality of packets received by a network device from a host located in a first network; generate a first plurality of log entries corresponding to the plurality of packets received by the network device; identify a plurality of encrypted packets transmitted by the network device to a host located in a second network; generate a second plurality of log entries corresponding to the plurality of encrypted packets transmitted by the network device; correlate, based on the first plurality of log entries corresponding to the plurality of packets received by the network device and the second plurality of log entries corresponding to the plurality of encrypted packets transmitted by the network device, the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device; and responsive to the correlating of the plurality of encrypted packets transmitted by the network device with the plurality of packets received by the network device: generate, based on the correlating, one or more rules configured to identify packets received from the host located in the first network; and provision a packet-filtering device with the one or more rules configured to identify packets received from the host located in the first network.

247. The ‘573 Accused Products are, or run on, computers with processors and memory (including RAM and a hard drive) that store instructions executed by the processors.

The ’573 Accused Products are also associated with a cloud component, such as ATI, ThreatArmor Central Management, which also have processors and memories.

248. The ’573 Accused Products identify packets received by a network element, such as a firewall, taps, bypass switches, among others. The ’573 Accused Products log the packets received, using, e.g., Ixia’s IxFlow, syslog, etc. The logs are used to perform correlations or generate statistics associated with a host or malicious IP address.

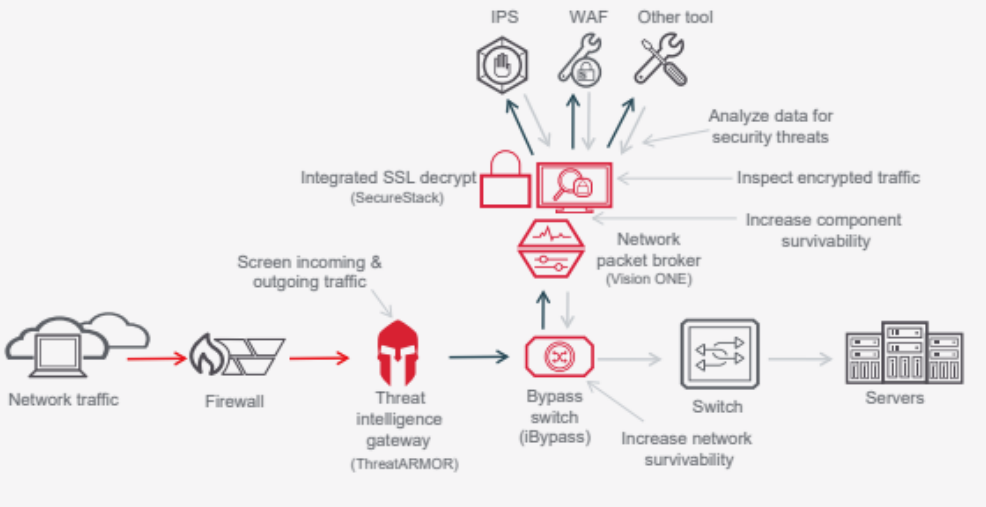


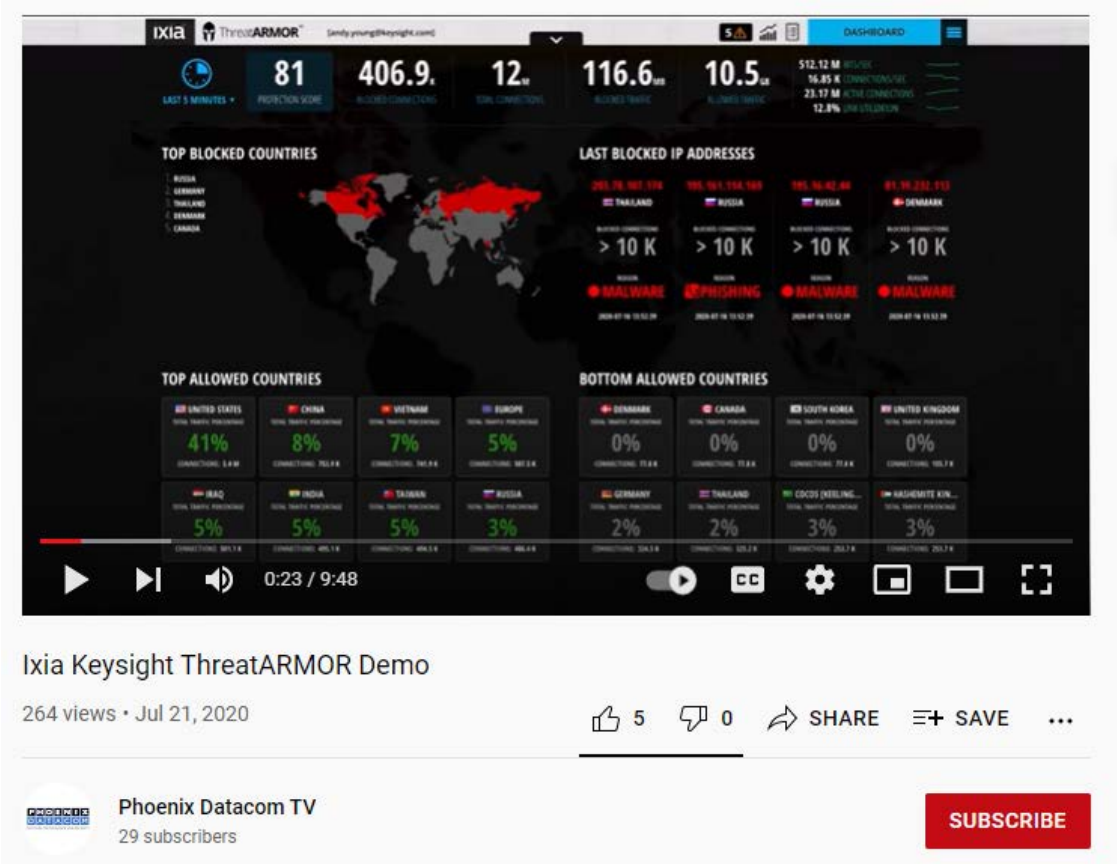
Figure 13. Ixia's inline security solution

Ex. 76 at 29.

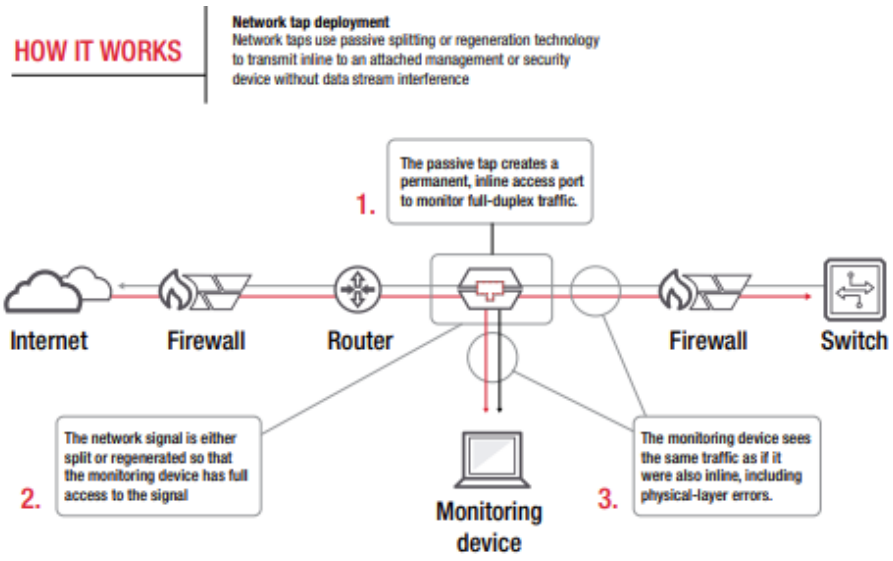
Visibility

- New Ixia's IxFlow extensions (NetFlow/IPFix)
- Send information about malicious activity on your network to Netflow collectors

https://www.youtube.com/watch?v=_TbHu8-exZQ&t=17s.

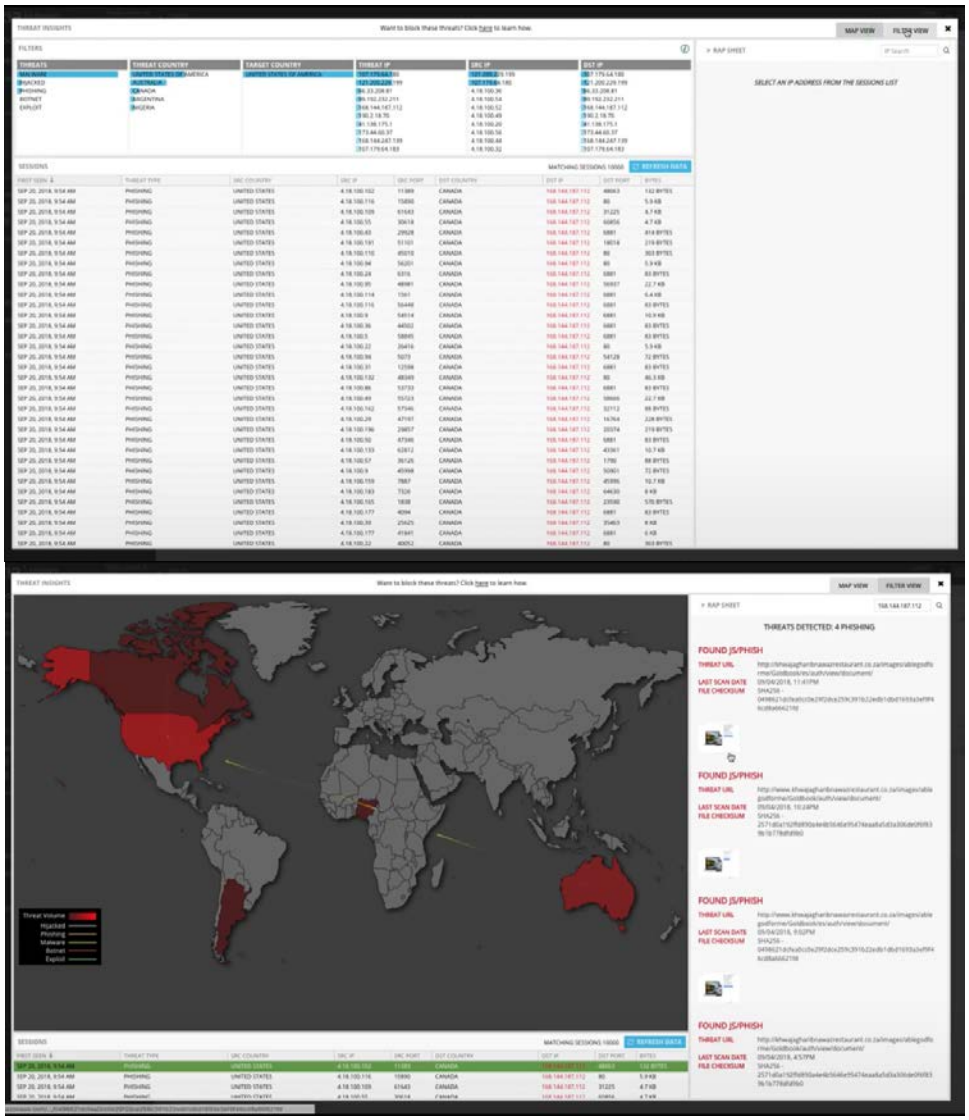


https://www.youtube.com/watch?v=aKnotioCHlg&t=4s; *see also* Ex. 56 ("ThreatARMOR Central Management provides a convenient, secure portal for managing global deployments of ThreatARMOR devices. Leveraging the elastic processing afforded by the cloud, it provides scalable management, log collection, and centralized reporting of policy, inventory, licensing, device health, and synchronization status, as well as aggregated blocking data.").



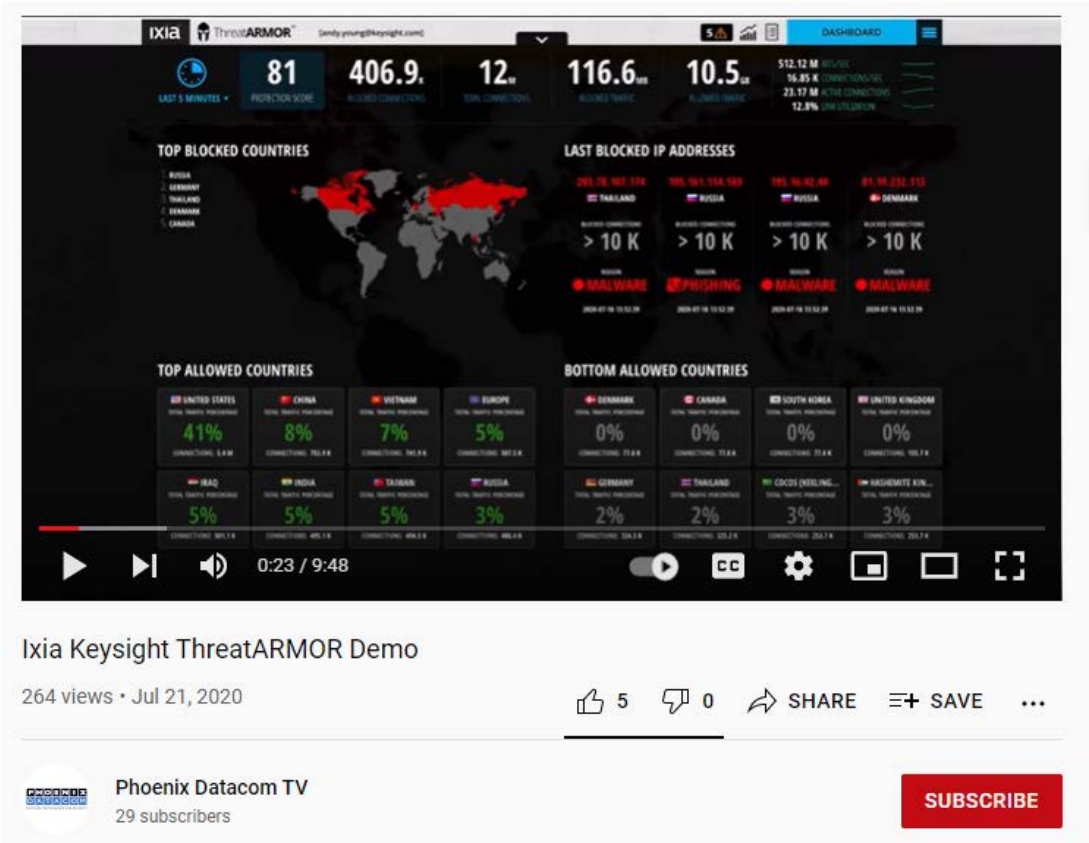
Ex. 86 at 74 ("Any monitoring device connected to a network device receives the same traffic as if it were inline, including all errors. This is achieved as the tap duplicates all traffic on the link and forwards it to the monitoring ports."); Ex. 76 at 2 ("A bypass switch is a special-purpose tap with fail-over capability"). The '573 Accused Products obtain packet information for incoming and outgoing network traffic which include encrypted and unencrypted packets.

249. The '573 Accused Products perform the correlations based on log entries. As one example, the ATIP dashboard for the Network Visibility products shows information and statistics about blocked locations and IP addresses, which include correlations of log entries.



https://www.youtube.com/watch?v=_TbHu8-exZQ&t=17s.

250. As another example, ThreatArmor's dashboard shows information and statistics about blocked locations and IP addresses, which include correlations of log entries.



https://www.youtube.com/watch?v=aKnotioCHlg&t=4s; *see also* Ex. 56 ("ThreatARMOR Central Management provides a convenient, secure portal for managing global deployments of ThreatARMOR devices. Leveraging the elastic processing afforded by the cloud, it provides scalable management, log collection, and centralized reporting of policy, inventory, licensing, device health, and synchronization status, as well as aggregated blocking data.").

Ex. 78.

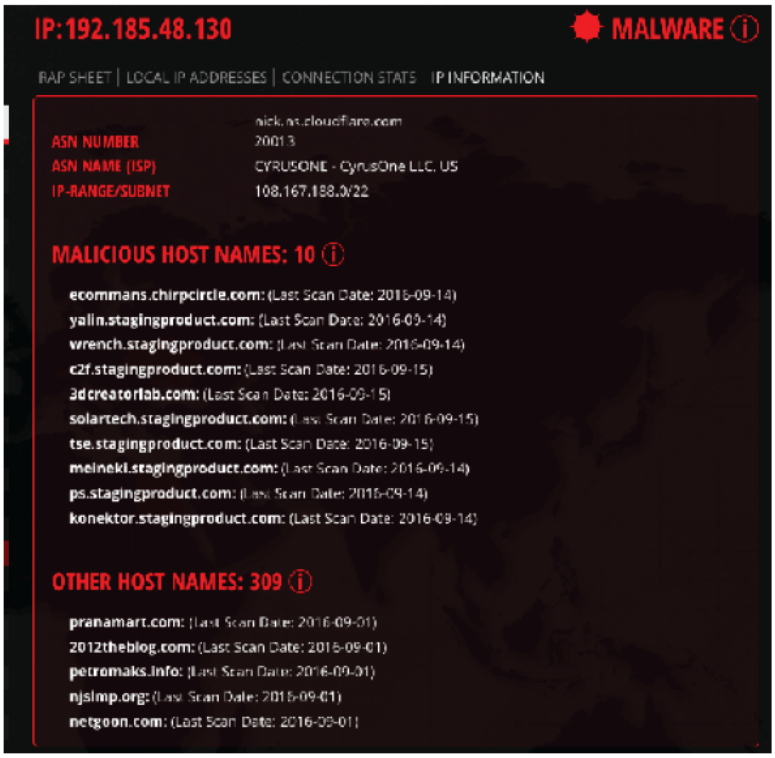


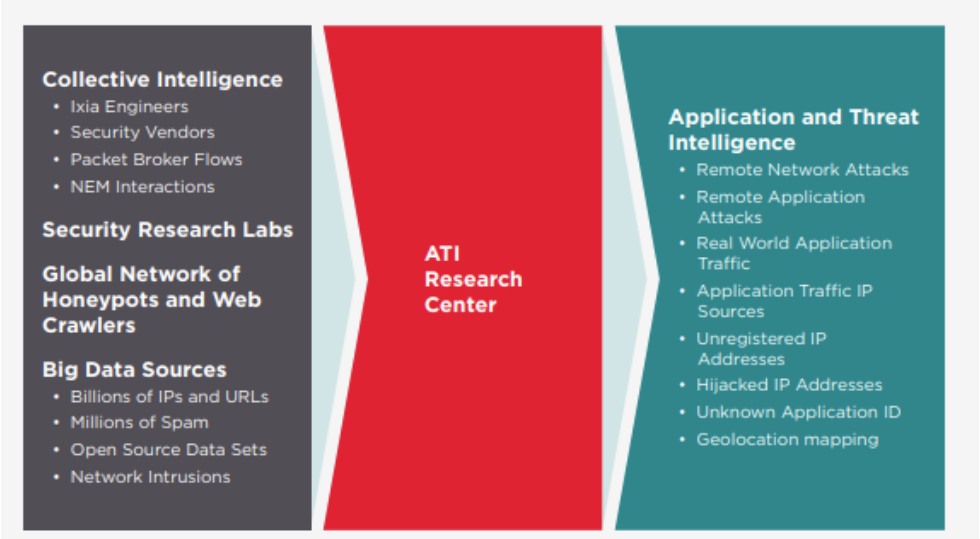
Fig. 1: Rap Sheet example of malicious activity

Ex. 71.

251. As a further example, ATI provides Rap Sheets associated with blocked IP addresses, which uses the correlation of log entries.

The ATI data feeds produce actionable security intelligence on application vulnerabilities as well as threats across networks, endpoints, mobile devices, virtual systems, web, and email. The ATI feeds automate the gathering and analysis of a wide range of threat intelligence data from sources including:

- Billions of IPs and URLs
- Millions of spam
- Millions of malware attacks
- Open source data sets
- Millions of network intrusions



Ex. 88 at 3.

252. ATI generates and provides threat intelligence-based rules based on the correlation. The ’573 Accused Products receive updates from ATI and use threat intelligence based rules, where the updates can be responsive to newly discovered network information and analytics, such as those based on the correlation. Ex. 52 at 1 (“By automatically applying an always-on threat intelligence feed to your network, you can eliminate network traffic from phishing sites, malware distribution sites, botnet controllers, hijacked networks, and unallocated IP addresses.” and “Quickly find compromised internal systems.”); *see also* Ex. 88 at 3; Ex. 57.

253. The rules can identify a host from a first network to prevent, for example, connections or bidirectional communications with a malicious site. Ex. 76 at 27 ("Ixia's ThreatARMOR solution detects infected systems to thwart outbound connections with botnets, phishing scams, and malware exploits. It blocks connections from known malicious IP addresses and untrusted geographies while preventing phishing replies and botnet connections.").

254. As a result of Keysight's unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

255. Keysight has willfully infringed the '573 Patent. As discussed above in the preceding paragraphs, Centripetal is informed and believes that Keysight had knowledge of the '573 Patent through various channels, and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

256. Keysight thus knew or, in the alternative, was willfully blind to Centripetal's technology and the '573 Patent.

257. Despite this knowledge and/or willful blindness, Keysight has acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

258. Centripetal is informed and believes that Keysight has undertaken no efforts to design these products or services around the '573 Patent to avoid infringement despite Keysight's knowledge and understanding that its products and services infringe the '573 Patent. As such, Keysight has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '573 Patent, justifying an

award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

259. Keysight's infringement of the '573 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

260. Keysight's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

261. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

FOURTEENTH CAUSE OF ACTION
(Indirect Infringement of the '573 Patent)

262. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

263. Keysight has induced and continues to induce infringement of one or more claims of the '573 Patent under 35 U.S.C. § 271(b). Keysight has contributorily infringed and continues to contributorily infringe one or more claims of the '573 Patent under 35 U.S.C. § 271(c).

264. Keysight has induced infringement of the '573 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 steps of the method claims, or provide one or more components of a system 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, taps, or bypass switches, to execute the functions of one or more claims of the ’573 Patent. Keysight instructs, directs and/or requires its customers, users, and vendors, or some combination thereof, to set up the system where bypass switches and taps identify packets and generate log entries. The log entries may be provided to ThreatArmor and Vision One 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 ’573 Accused Products, such as the monitoring function in ThreatArmor, to perform one or more steps in the claims of the ’573 Patent. Keysight has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with Keysight, one or more claims of the ‘573 Patent.

265. Keysight has knowingly and actively aided and abetted the direct infringement of the ‘573 Patent by instructing and encouraging its customers, users, and vendors to meet the elements of the ‘573 Patent with the ‘573 Accused Products. Such use is consistent with how the ‘573 Accused Products are described to directly infringe the ‘573 Patent and how the ‘573 Accused Products 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: (a) advising its customers and users to use the ‘573 Accused 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; (b) advertising and promoting the use of the ‘573 Accused Products in an infringing manner; and (c) distributing guidelines and instructions on how to setup the ‘573 Accused 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 obtains 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.

266. Keysight updates and maintains a support website that includes technical documentation encouraging the use of the '573 Accused Products in an infringing manner. This technical documentation includes knowledge articles, videos, user guides, technical support articles, and a knowledge center. The technical documentation covers the operation of the '573 Accused Products in-depth, including by advertising the '573 Accused Products' infringing features and instructing customers, users, and vendors to configure and use the '573 Accused Products in an infringing manner. *See, e.g.*, Ex. 73 (https://www.keysight.com/us/en/support.html); Ex. 74 (https://support.keysight.com/s/?language=en_US); Ex. 75 (https://support.ixiacom.com/).

267. Keysight contributorily infringes the '573 Patent pursuant to 35 U.S.C. § 271(c) because it provided its '573 Accused Products as software and computer systems with software installed, which act as a material component of the '573 Patent claims when combined with other components to create a complete network security system. Keysight knows that its products are particularly suited to be used in an infringing manner. The '573 Accused Products and their associated software are highly developed and 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 '573 Patent.

268. Keysight has knowingly and actively contributed to the direct infringement of the '573 Patent by its manufacture, use, offer to sell, sale and importation of the '573 Accused Products together with its customers, users, and vendors to meet the elements of the '573 Patent, as described above and incorporated by reference here. To the extent Keysight's 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 for CloudLens, which infringes when a third party runs this software on processors and memory in a cloud environment. As another example, Keysight sold the Visibility products, the Testing products, and ThreatArmor, which infringes when a third party combines them for use with a bypass switch, tap, or devices with similar functionalities. To the extent Keysight's customers, users, and vendors direct and control the systems and methods in the claims, Keysight obtains benefits from the control of the 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 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.

269. Keysight's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

270. Keysight has known or, in the alternative, has been willfully blind to Centripetal's technology and the '573 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 '573 Patent to avoid infringement despite Keysight's knowledge and understanding that its products and services infringe the '573 Patent.

271. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

FIFTEENTH CAUSE OF ACTION
(Direct Infringement of the '009 Patent pursuant to 35 U.S.C. § 271(a))

272. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

273. Keysight has infringed and continues to infringe at least one or more claims of the '009 Patent.

274. Keysight's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

275. Keysight's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

276. Keysight's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the

’009 Patent, including, but not limited to the following products and services: the Network Visibility products, the Ixia Fabric Controller, and the Testing products, and any other products or services with Keysight’s NetStack, AppStack, SecureStack, and the ATI technology (the “‘009 Accused Products”). Keysight also infringes these claims jointly with its customers, users, and vendors. Keysight directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, Keysight puts the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

277. The ’009 Accused Products embody the patented invention of the ’009 Patent and infringe the ’009 Patent because they include a network protection device which includes one or more processors; and memory comprising instructions that, when executed by the one or more processors, cause the network protection device to: preprocess a first rule set by performing operations on the first rule set, prior to the first rule set being implemented on the network protection device, to optimize performance of the network protection device; configure the at least one processor to process packets in accordance with the preprocessed first rule set after preprocessing the first rule set; receive a plurality of packets after configuring of the at least one processor to process packets in accordance with the preprocessed first rule set; process a first portion of the plurality of packets in accordance with the preprocessed first rule set; preprocess a second rule set by performing operations on the second rule set, prior to the second rule set being implemented on the network protection device, to optimize performance of the network protection device; signal the at least one processor to process packets in accordance with the second rule set; and responsive to the signaling: cease processing of one or more packets; cache the one or more packets; reconfigure the at least one

processor to process packets in accordance with the preprocessed second rule set; and process the one or more cached packets in accordance with the preprocessed second rule set wherein the operations performed on the first rule set and the second rule set include at least one of: merging two or more rules within the first rule set or the second rule set into one rule; separating one or more rules within the first rule set or the second rule set into two or more rules; or reordering one or more rules within the first rule set or the second rule set.

278. The ’009 Accused Products are, or run on, computers with processors and memory (including RAM and a hard drive) that store instructions executed by the processors.

279. The ’009 Accused Products preprocess a rule set to optimize the performance of a network device and configure the network device with the preprocessed rule set. The preprocessing can be accomplished by merging, separating, and ordering rules in a rule set. For example, the ’009 Accused Products utilize Keysight’s ATI technology, which preprocesses threat intelligence based rule sets. *See, e.g.*, Ex. 39; Ex. 84. The rule sets can be dynamically provided to network devices, which can be configured with the preprocessed rule set. *See, e.g.*, Ex. 39 (“Our Application and Threat Intelligence (ATI) subscription service provides up-to-the-moment threat intelligence.”); Exs. 32-33; *see also* Ex. 85 at 4. As another example, the Ixia Fabric Controller preprocesses and configures the Network Visibility products with rule sets. Exs. 80-81. As another example, the Network Visibility products receive rule sets, preprocess them, and configure their processors with the rule set using the hitless change feature. Ex. 31; Ex. 24.

280. The ’009 Accused Products receive packets and process the packets based on rule sets. *See, e.g.*, https://www.youtube.com/watch?v=_TbHu8-exZQ&t=17s; Ex. 77 at 3; Ex. 57; Exs. 34-35.

281. When the ’009 Accused Products swap rule sets, the ’009 Accused Products cease processing packets, cache packets, reconfigure the device’s processor(s) with the new rule set and process the packets with the new rule set. *See, e.g.*, Ex. 24. Using the ’009 Patent’s technology, the ’009 Accused Products swap rule sets without dropping packets with the hitless change feature. Ex. 31; Ex. 24.

282. Keysight has willfully infringed the ‘009 Patent. As discussed above in the preceding paragraphs, Centripetal is informed and believes that Keysight had knowledge of the ‘009 Patent through various channels, and despite its knowledge of Centripetal’s patent rights, engaged in egregious behavior warranting enhanced damages.

283. Keysight thus knew or, in the alternative, was willfully blind to Centripetal’s technology and the ‘009 Patent.

284. Despite this knowledge and/or willful blindness, Keysight has acted with blatant and egregious disregard for Centripetal’s patent rights with an objectively high likelihood of infringement.

285. Centripetal is informed and believes that Keysight has undertaken no efforts to design these products or services around the ‘009 Patent to avoid infringement despite Keysight’s knowledge and understanding that its products and services infringe the ‘009 Patent. As such, Keysight has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the ‘009 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys’ fees and costs incurred under 35 U.S.C. § 285.

286. Keysight’s infringement of the ‘009 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

287. Keysight's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

288. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

SIXTEENTH CAUSE OF ACTION
(Indirect Infringement of the '009 Patent)

289. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

290. Keysight has induced and continues to induce infringement of one or more claims of the '009 Patent under 35 U.S.C. § 271(b). Keysight has contributorily infringed and continues to contributorily infringe one or more claims of the '009 Patent under 35 U.S.C. § 271(c).

291. Keysight has induced infringement of the '009 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 steps of the method claims, or provide one or more components of a system 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 execute the functions of one or more claims of the '009 Patent. 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 hitless change) to perform one or more steps in the claims of the ’009 Patent.

292. Keysight has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with Keysight, one or more claims of the ‘009 Patent.

293. Keysight has knowingly and actively aided and abetted the direct infringement of the ‘009 Patent by instructing and encouraging its customers, users, and vendors to meet the elements of the ‘009 Patent with the Accused Products. Such use is consistent with how the Accused Products are described to directly infringe the ‘009 Patent and how the Accused Products 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: (a) advising its customers and users to use the ‘009 Accused 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; (b) advertising and promoting the use of the ‘009 Accused Products in an infringing manner; and (c) distributing guidelines and instructions on how to setup the ‘009 Accused 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 obtains 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.

294. Keysight updates and maintains a support website that includes technical documentation encouraging the use of the ‘009 Accused Products in an infringing manner.

This technical documentation includes knowledge articles, videos, user guides, technical support articles, and a knowledge center. The technical documentation covers the operation of the '009 Accused Products in-depth, including by advertising the '009 Accused Products' infringing features and instructing customers, users, and vendors to configure and use the '009 Accused Products in an infringing manner. *See*, *e.g.*, Ex. 73 (https://www.keysight.com/us/en/support.html); Ex. 74 (https://support.keysight.com/s/?language=en_US); Ex. 75 (https://support.ixiacom.com/).

295. Keysight contributorily infringes the '009 Patent pursuant to 35 U.S.C. § 271(c) because it provided its '009 Accused Products as software and computer systems with software installed, which act as a material component of the '009 Patent claims when combined with other components to create a complete network security system. Keysight knows that its products are particularly suited to be used in an infringing manner. The '009 Accused Products and their associated software are highly developed and 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 '009 Patent.

296. Keysight has knowingly and actively contributed to the direct infringement of the '009 Patent by its manufacture, use, offer to sell, sale and importation of the '009 Accused Products together with its customers, users, and vendors to meet the elements of the '009 Patent, as described above and incorporated by reference here. To the extent Keysight's 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 for CloudLens, which infringes when a third party runs this software on processors and memory in a cloud environment. As another example, Keysight sold the Testing products which infringe when a third party combines them for use with other Keysight's products, such as its Network Visibility products. To the extent Keysight's customers, users, and vendors direct and control the systems and methods in the claims, Keysight obtains 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. For example, Keysight is able to keep the performance of its products without needing to bring them offline for rule updates or otherwise miss network traffic.

297. Keysight's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

298. Keysight has known or, in the alternative, has been willfully blind to Centripetal's technology and the '009 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 '009 Patent to avoid infringement despite Keysight's knowledge and understanding that its products and services infringe the '009 Patent.

299. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

SEVENTEENTH CAUSE OF ACTION
(Direct Infringement of the '456 Patent pursuant to 35 U.S.C. § 271(a))

300. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

301. Keysight has infringed and continues to infringe at least one or more the claims of the '456 Patent.

302. Keysight's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

303. Keysight's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

304. Keysight's infringement includes the manufacture, use (including internal testing), and/or offer for sale of products and services incorporating Centripetal's technology covered by the '456 Patent, including, but not limited to the following products and services: the Network Visibility products and the Testing products, and any other products or services with Keysight's SecureStack and the ATI technology (the "'456 Accused Products"). Keysight also infringes these claims jointly with its customers, users, and vendors. Keysight directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, Keysight put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

305. The '456 Accused Products embody the patented invention of the '456 Patent and infringe the '456 Patent because they perform receiving, by a packet-filtering device from an intelligence provider, one or more threat indicators, wherein the one or more threat

indicators comprise a plurality of domain names associated with one or more threats; determining a plurality of packet-filtering rules associated with each of the one or more threat indicators, wherein the one or more threat indicators comprise a matching criterion for the plurality of packet-filtering rules; receiving, from a first device, a plurality of packets, wherein the plurality of packets comprise ciphertext comprising an encrypted server name indication (eSNI) value; determining whether a plaintext hostname is resolvable from the ciphertext; determining, based on a determination that the plaintext hostname is resolvable from the ciphertext, whether the plaintext hostname matches at least one of the one or more threat indicators; and applying, based on a determination that the plaintext hostname matches at least one of the one or more threat indicators, a packet filtering operation associated with one or more of the plurality of packet-filtering rules to the plurality of packets, wherein the packet filtering operation comprises at least one of: blocking the plurality of packets from continuing toward its intended destination, allowing the plurality of packets to continue to its intended destination and forwarding a copy of the plurality of packets to a first proxy for monitoring, or forwarding the plurality of packets to a second proxy.

306. The ‘456 Accused Products are, or run on, computers with processors and memory (including RAM and a hard drive) that store instructions executed by the processors.

307. The ’456 Accused Products receive packets related to encrypted communications, which can include ciphertext comprising an encrypted server name indication (eSNI) value. Keysight is actively making and testing the Testing products that will support eSNI. Ex. 89 at 3. As the Network Visibility products and the Testing products both use threat intelligence information from ATI for packet analytics, malicious eSNI information will also be available to the Network Visibility products as part of the threat intelligence information.

Furthermore, Keysight infringes by internally testing the ’456 Accused Products’ capabilities on the filtering malicious traffic based on eSNI.

308. The ’456 Accused Products receive threat indicators with Keysight’s ATI technology and apply threat intelligence based rules associated with the threat indicators. Exs. 32-33; Ex. 57. The threat indicators include data indicating domain names.

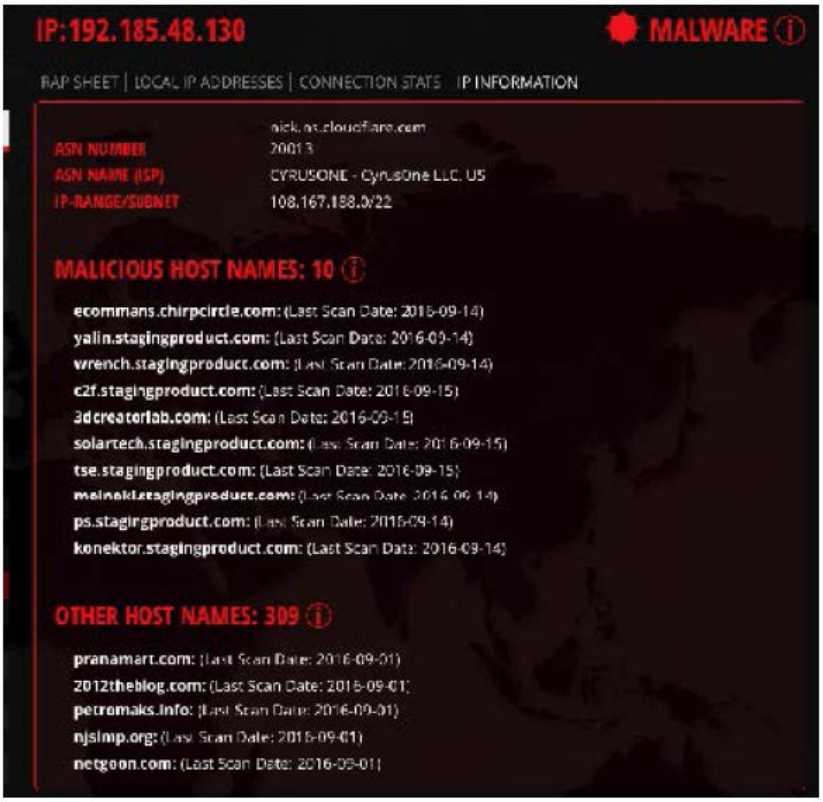


Figure 2. Rap Sheet example of multiple malicious domains at an IP address

Ex. 84 at 3.

309. The ’456 Accused Products determine whether packet information, such as information related to plaintext hostname, meets a threat indicator. *See* Exs. 32-33; Ex. 57. The ’456 Accused Products use SecureStack, which supports the analysis of TLS 1.3/ephemeral key traffic. With support of eSNI information from ATI, the ’456 Accused

Products can determine whether a plaintext hostname is resolvable from the ciphertext. Ex. 89; Ex. 90.

310. The ’456 Accused Products can apply a packet filtering operation based on its analysis and packet filtering rules. For example, the ’456 Accused Products can determine whether to allow, block, or forward the packets to a different destination. *See, e.g.*, Exs. 32-33;

Rap Sheets Describe Network Risks

Whenever ThreatARMOR blocks traffic to or from a known-bad site, a Rap Sheet is provided to explain why that IP address is considered bad. This helps customers better understand the risks facing their network and also avoid the risk of false positive. ThreatARMOR only blocks an IP address if the ATI Research Center has 100% certainty there is malicious or criminal activity at that site, and the Rap Sheet details the proof. The Rap Sheets themselves provide information such as the URL information of individual threats, the binary checksum of that malware, screen shots of a phishing page or malware installer, and the last date the individual piece of malicious activity was validated.

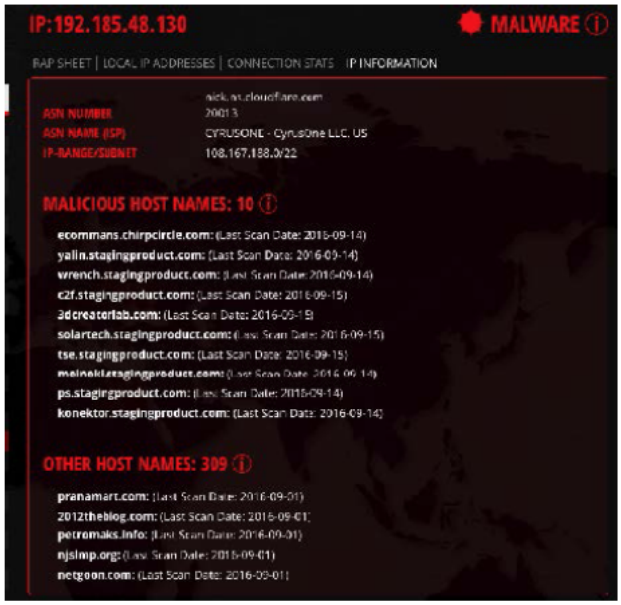


Figure 1. Rap Sheet example of malicious activity

Ex. 84 at 2.

311. As a result of Keysight’s unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

312. Keysight has willfully infringed the '456 Patent. As discussed above in the preceding paragraphs, Centripetal is informed and believes that Keysight had knowledge of the '456 Patent through various channels, and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

313. Keysight thus knew or, in the alternative, was willfully blind to Centripetal's technology and the '456 Patent.

314. Despite this knowledge and/or willful blindness, Keysight has acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

315. Centripetal is informed and believes that Keysight has undertaken no efforts to design these products or services around the '456 Patent to avoid infringement despite Keysight's knowledge and understanding that its products and services infringe the '456 Patent. As such, Keysight has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '456 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

316. Keysight's infringement of the '456 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

317. Keysight's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

318. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

EIGHTEENTH CAUSE OF ACTION
(Indirect Infringement of the '456 Patent)

319. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

320. Keysight has induced and continues to induce infringement of one or more claims of the '456 Patent under 35 U.S.C. § 271(b). Keysight has contributorily infringed and continues to contributorily infringe one or more claims of the '456 Patent under 35 U.S.C. § 271(c).

321. Keysight has induced infringement of the '456 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 steps of the method claims, or provide one or more components of a system 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 execute the functions of one or more claims of the '456 Patent. Keysight instructs, directs and/or requires its customers, users, and vendors to obtain and activate subscriptions (such as Keysight's ATI subscription) and functions to perform one or more steps in the claims of the '456 Patent.

322. Keysight has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with Keysight, one or more claims of the '456 Patent.

323. Keysight has knowingly and actively aided and abetted the direct infringement of the '456 Patent by instructing and encouraging its customers, users, and vendors to meet the

elements of the '456 Patent with the Accused Products. Such use is consistent with how the '456 Accused Products are described to directly infringe the '456 Patent and how the '456 Accused Products 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 '456 Accused 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; advertising and promoting the use of the '456 Accused Products in an infringing manner; and distributing guidelines and instructions on how to setup the '456 Accused 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 obtains 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.

324. Keysight updates and maintains a support website that includes technical documentation encouraging the use of the '456 Accused Products in an infringing manner. This technical documentation includes knowledge articles, videos, user guides, technical support articles, and a knowledge center. The technical documentation covers the operation of the '456 Accused Products in-depth, including by advertising '456 the Accused Products' infringing features and instructing customers, users, and vendors to configure and use the Accused Products in an infringing manner. *See, e.g.*, Ex. 73 (https://www.keysight.com/us/en/support.html); Ex. 74 (https://support.keysight.com/s/?language=en_US); Ex. 75 (https://support.ixiacom.com/).

325. Keysight contributorily infringes the '456 Patent pursuant to 35 U.S.C. § 271(c) because it provides the '456 Accused Products as software and computer systems with software installed, which act as a material component of the '456 Patent claims when combined with other components to create a complete network security system. Keysight knows that its products are particularly suited to be used in an infringing manner. The '456 Accused Products and their associated software are highly developed and 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 '456 Patent.

326. Keysight has knowingly and actively contributed to the direct infringement of the '456 Patent by its manufacture, use, offer to sell, sale and importation of the '456 Accused Products together with its customers, users, and vendors to meet the elements of the '456 Patent, as described above and incorporated by reference here. To the extent Keysight's 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 such as the software of Network Visibility products (including SecureStack) and which is a material component that can be combined with other components, such as Keysight's Threat Insight to create an infringing system. As another example, Keysight sold the Testing products which infringe when a third party combines them for use with ThreatArmor or Network Visibility products. To the extent Keysight's customers, users, and vendors direct and control the systems and methods in the claims, Keysight obtains

benefits from the control of the system as a whole. For example, Keysight's other products, such as ThreatArmor, can use information associated with malicious eSNI information to block network traffic. 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.

327. Keysight's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

328. Keysight has known or, in the alternative, has been willfully blind to Centripetal's technology and the '456 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 '456 Patent to avoid infringement despite Keysight's knowledge and understanding that its products and services infringe the '456 Patent.

329. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

NINETEENTH CAUSE OF ACTION
(Direct Infringement of the '474 Patent pursuant to 35 U.S.C. § 271(a))

330. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

331. Keysight has infringed and continues to infringe at least one or more the claims of the '474 Patent.

332. Keysight's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

333. Keysight's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

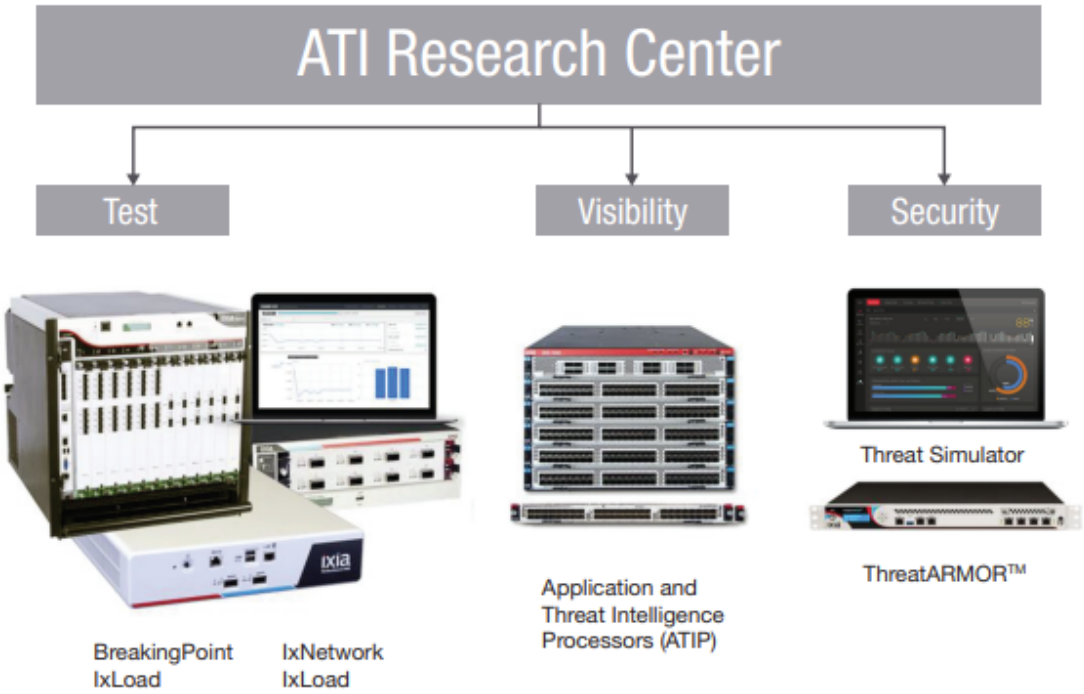
334. Keysight's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the '474 Patent, including, but not limited to the following products and services: the Network Visibility products, the ThreatArmor Suite, the Testing products, and the Ixia Fabric Controller, and any other products or services with Keysight's AppStack, SecureStack, and the ATI technology (the "'474 Accused Products"). Keysight also infringes these claims jointly with its customers, users, and vendors. Keysight directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, Keysight put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

335. The '474 Accused Products embody the patented invention of the '474 Patent and infringe the '474 Patent because they include at least a packet security gateway configured for protection of a network, capable of receiving a plurality of dynamic security policies and associated with a security policy management server external from the network, the packet security gateway comprising: at least one processor; and memory comprising instructions that, when executed by the last least one processor, cause the packet security gateway to: receive, from the security policy management server, a dynamic security policy comprising packet filtering rules, wherein one or both of the dynamic security policy or one or more of the packet filtering rules of the dynamic security policy were automatically created or altered, by the security policy management server, based on malicious traffic information received from a

plurality of malicious host tracker services, wherein at least two of the plurality of malicious host tracker services are managed by different organizations, wherein one or more of the packet filtering rules were added, removed, or altered by the security policy management server based on a correlation between portions of the malicious traffic information, and wherein a first packet matching rule of the packet filtering rules comprises: at least one packet matching criterion, a corresponding packet transformation function, and an indication of a feed managed by at least one of the plurality of malicious host tracker services; and perform, based on the packet filtering rules, packet filtering on individual packets of a plurality of packets associated with the network protected by the packet security gateway, wherein the packet filtering comprises: inspecting individual packets; and filtering each packet based on content determined from the inspection of that individual packet.

336. The '474 Accused Products are, or run on, computers with processors and memory (including RAM and a hard drive) that store instructions executed by the processors.

337. The '474 Accused Products are packet security gateways that provide network security and have ATI, which provides dynamic updates of threat intelligence. *See, e.g.*, Ex. 27 at 25 ("Ixia visibility solutions provide real-time, end-to-end visibility, insight, and security."); Ex. 54; Ex. 57. The servers for ATI are external to the network protected by the '474 Accused Products.



The reach of the ATI research center spans Keysight product lines to ensure the most up-to-date application and threat intelligence.

See, e.g., Ex. 85 at 4.

338. The ’474 Accused Products receive from the ATI servers continuously updated threat intelligence. The threat intelligence updates the security policies used by the ’474 Accused Products to be dynamically updated. Ex. 39 (“Our Application and Threat Intelligence (ATI) subscription service provides up-to-the-moment threat intelligence.”); Exs. 32-33; *see also* Ex. 85 at 4.

339. The ’474 Accused Products use packet-filtering rules to inspect network traffic and filter packets based on packet information. Ex. 91 at 5-6; Ex. 32-33; Ex. 39. The rules are associated with subscriptions to ATI and have an indication of a feed managed by a malicious host tracker service. The rules include packet matching criteria such as geolocation, IP address, etc. (from the ATI feeds) and a corresponding packet transformation function, such as

forward, monitor, log, etc. Id. ATI provides Rap Sheets that include explanations of, e.g., why a host is malicious.

Rap Sheets Describe Network Risks

Whenever ThreatARMOR blocks traffic to or from a known-bad site, a Rap Sheet is provided to explain why that IP address is considered bad. This helps customers better understand the risks facing their network and also avoid the risk of false positive. ThreatARMOR only blocks an IP address if the ATI Research Center has 100% certainty there is malicious or criminal activity at that site, and the Rap Sheet details the proof. The Rap Sheets themselves provide information such as the URL information of individual threats, the binary checksum of that malware, screen shots of a phishing page or malware installer, and the last date the individual piece of malicious activity was validated.

Fig. 1: Rap Sheet example of malicious activity

See, e.g., Ex. 71.

340. As a result of Keysight's unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

341. Keysight has willfully infringed the '474 Patent. As discussed above in the preceding paragraphs, Centripetal is informed and believes that Keysight had knowledge of the '474 Patent through various channels, and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

342. Keysight thus knew or, in the alternative, was willfully blind to Centripetal's technology and the '474 Patent.

343. Despite this knowledge and/or willful blindness, Keysight has acted with blatant and egregious disregard for Centripetal's patent rights with an objectively high likelihood of infringement.

344. Centripetal is informed and believes that Keysight has undertaken no efforts to design these products or services around the '474 Patent to avoid infringement despite Keysight's knowledge and understanding that its products and services infringe the '474 Patent. As such, Keysight has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '474 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

345. Keysight's infringement of the '474 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

346. Keysight's infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

347. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

TWENTIETH CAUSE OF ACTION
(Indirect Infringement of the '474 Patent)

348. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

349. Keysight has induced and continues to induce infringement of one or more claims of the '474 Patent under 35 U.S.C. § 271(b). Keysight has contributorily infringed and continues to contributorily infringe one or more claims of the '474 Patent under 35 U.S.C. § 271(c).

350. Keysight has induced infringement of the '474 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 steps of the method claims, or provide one or more components of a system 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 execute the functions of one or more claims of the '474 Patent. For example, Keysight instructs, directs and/or requires its customers, users, and vendors to setup the system to receive security policy updates from a server external from the network being protected by the '474 Accused Products. Keysight also instructs, directs and/or requires its customers, users, and vendors to obtain and activate subscriptions (such as Keysight's ATI subscription) and functions to perform one or more steps in the claims of the '474 Patent.

351. Keysight has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with Keysight, one or more claims of the '474 Patent.

352. Keysight has knowingly and actively aided and abetted the direct infringement of the '474 Patent by instructing and encouraging its customers, users, and vendors to meet the

elements of the '474 Patent with the Accused Products. Such use is consistent with how the Accused Products are described to directly infringe the '474 Patent and how the Accused Products 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: (a) advising its customers and users to use the '474 Accused 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; (b) advertising and promoting the use of the '474 Accused Products in an infringing manner; and (c) distributing guidelines and instructions on how to setup the '474 Accused 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 obtains 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.

353. Keysight updates and maintains a support website that includes technical documentation encouraging the use of the '474 Accused Products in an infringing manner. This technical documentation includes knowledge articles, videos, user guides, technical support articles, and a knowledge center. The technical documentation covers the operation of the '474 Accused Products in-depth, including by advertising the '474 Accused Products' infringing features and instructing customers, users, and vendors to configure and use the '474 Accused Products in an infringing manner. *See, e.g.*, Ex. 73 (https://www.keysight.com/us/en/support.html); Ex. 74 (https://support.keysight.com/s/?language=en_US); Ex. 75 (https://support.ixiacom.com/).

354. Keysight contributorily infringes the '474 Patent pursuant to 35 U.S.C. § 271(c) because it provides the '474 Accused Products as software and computer systems with software installed, which act as a material component of the '474 Patent claims when combined with other components to create a complete network security system. Keysight knows that its products are particularly suited to be used in an infringing manner. The '474 Accused Products and their associated software are highly developed and 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 '474 Patent.

355. Keysight has knowingly and actively contributed to the direct infringement of the '474 Patent by its manufacture, use, offer to sell, sale and importation of the '474 Accused Products together with its customers, users, and vendors to meet the elements of the '474 Patent, as described above and incorporated by reference here. To the extent Keysight's 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 for CloudLens, which infringes when a third party runs this software on processors and memory in a cloud environment. As another example, Keysight sold the Testing products, which infringe when a third party combines them for use with other Keysight's products, such as its Network Visibility products and ThreatArmor. To the extent Keysight's customers, users, and vendors direct and control the systems and methods in the claims, Keysight obtains 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. For example, threat information obtained through the filtering of packets can be provided to other Keysight's products or to the ATI research center as threat intelligence, which strengthens these other products' ability to prevent network threats.

356. Keysight's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

357. Keysight has known or, in the alternative, has been willfully blind to Centripetal's technology and the '474 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 '474 Patent to avoid infringement despite Keysight's knowledge and understanding that its products and services infringe the '474 Patent.

358. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

TWENTY-FIRST CAUSE OF ACTION
(Direct Infringement of the '266 Patent pursuant to 35 U.S.C. § 271(a))

359. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

360. Keysight has infringed and continues to infringe at least one or more the claims of the '266 Patent.

361. Keysight's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

362. Keysight's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Centripetal.

363. Keysight's infringement includes the manufacture, use, sale, importation and/or offer for sale of products and services incorporating Centripetal's technology covered by the '266 Patent, including, but not limited to the following products and services: the Network Visibility products, the ThreatArmor Suite, the Testing products, and the Ixia Fabric Controller, and any other products or services with Keysight's AppStack, SecureStack, and the ATI technology (the "'266 Accused Products"). Keysight also infringes these claims jointly with its customers, users, and vendors. Keysight directs and controls the systems and methods in the claims and obtains benefits from the control of the system as a whole. In particular, Keysight put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

364. The '266 Accused Products embody the patented invention of the '266 Patent and infringe the '266 Patent because they include at least a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway, comprising: one or more processors; and memory storing instructions that, when executed by the one or more processors, cause the packet security gateway to: receive, from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary, wherein: each packet filtering rule of the first set of packet filtering

rules comprises at least one packet matching criterion and a corresponding packet transformation function, and one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and were automatically created or altered by the security policy management server based on aggregated malicious traffic information, received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic; perform, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets; receive, after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service; and perform, on a packet by packet basis, packet filtering on a second portion of the packets corresponding to network traffic traversing the boundary via the packet security gateway based on the updated second set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the second set of packet filtering rules on the second portion of packets.

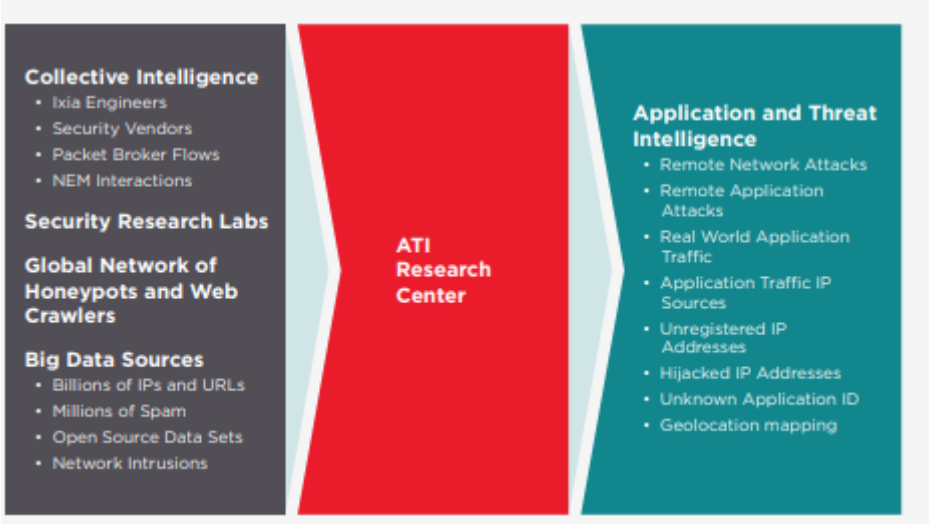
365. The ‘266 Accused Products are, or run on, computers with processors and memory (including RAM and a hard drive) that store instructions executed by the processors.

366. The ’266 Accused Products are packet security gateways that provide network security and have ATI, which provides dynamic updates of threat intelligence. *See, e.g.*, Ex. 76 at 25 (“Ixia visibility solutions provide real-time, end-to-end visibility, insight, and security.”); Ex. 54; Ex. 57. The servers for ATI are external to the network protected by the ’266 Accused Products. *See, e.g.*, Ex. 85 at 4.

367. The ’266 Accused Products receive from the ATI servers continuously updated threat intelligence. The threat intelligence updates the security policies used by the ’266 Accused Products to be dynamically updated. Ex. 39 (“Our Application and Threat Intelligence (ATI) subscription service provides up-to-the-moment threat intelligence.”); Exs. 32-33; *see also* Ex. 85 at 4. The ATI servers receive information from a variety of sources including third party host tracker service and automatically creating packet filtering rules to update the ’266 Accused Products.

The ATI data feeds produce actionable security intelligence on application vulnerabilities as well as threats across networks, endpoints, mobile devices, virtual systems, web, and email. The ATI feeds automate the gathering and analysis of a wide range of threat intelligence data from sources including:

- Billions of IPs and URLs
- Millions of spam
- Millions of malware attacks
- Open source data sets
- Millions of network intrusions



Ex. 88 at 3.

368. The ’266 Accused Products use dynamically updated packet-filtering rules to inspect network traffic and filter packets based on packet information. Ex. 91 at 5-6; Exs. 32-33; Ex. 39. The rules include packet matching criteria such as geolocation, IP address, etc. (from the ATI feeds) and a corresponding packet transformation function, such as forward, monitor, log, etc. Id.

369. As a result of Keysight’s unlawful activities, Centripetal has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Centripetal is entitled to preliminary and/or permanent injunctive relief.

370. Keysight has willfully infringed the ‘266 Patent. As discussed above in the preceding paragraphs, Centripetal is informed and believes that Keysight had knowledge of the

‘266 Patent through various channels, and despite its knowledge of Centripetal’s patent rights, engaged in egregious behavior warranting enhanced damages.

371. Keysight thus knew or, in the alternative, was willfully blind to Centripetal’s technology and the ‘266 Patent.

372. Despite this knowledge and/or willful blindness, Keysight has acted with blatant and egregious disregard for Centripetal’s patent rights with an objectively high likelihood of infringement.

373. Centripetal is informed and believes that Keysight has undertaken no efforts to design these products or services around the ‘266 Patent to avoid infringement despite Keysight’s knowledge and understanding that its products and services infringe the ‘266 Patent. As such, Keysight has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the ‘266 Patent, justifying an award to Centripetal of increased damages under 35 U.S.C. § 284, and attorneys’ fees and costs incurred under 35 U.S.C. § 285.

374. Keysight’s infringement of the ‘266 Patent has injured and continues to injure Centripetal in an amount to be proven at trial, but not less than a reasonable royalty.

375. Keysight’s infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

376. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

TWENTY-SECOND CAUSE OF ACTION
(Indirect Infringement of the '266 Patent)

377. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

378. Keysight has induced and continues to induce infringement of one or more claims of the '266 Patent under 35 U.S.C. § 271(b). Keysight has contributorily infringed and continues to contributorily infringe one or more claims of the '266 Patent under 35 U.S.C. § 271(c).

379. Keysight has induced infringement of the '266 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 steps of the method claims, or provide one or more components of a system 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 execute the functions of one or more claims of the '266 Patent. For example, Keysight instructs, directs and/or requires its customers, users, and vendors to setup the system to receive security policy updates from a server external from the network being protected by the '266 Accused Products. Keysight also instructs, directs and/or requires its customers, users, and vendors to obtain and activate subscriptions (such as Keysight's ATI subscription) and functions to perform one or more steps in the claims of the '266 Patent. As another example, Keysight instructs, directs and/or requires its customers, users, and vendors to setup network elements in a way where a network is protected by multiple packet security gateways.

380. Keysight has known or has been willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with Keysight, one or more claims of the '266 Patent.

381. Keysight has knowingly and actively aided and abetted the direct infringement of the '266 Patent by instructing and encouraging its customers, users, and vendors to meet the elements of the '266 Patent with the Accused Products. Such use is consistent with how the Accused Products are described to directly infringe the '266 Patent and how the Accused Products 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: (a) advising its customers and users to use the '266 Accused 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; (b) advertising and promoting the use of the '266 Accused Products in an infringing manner; and (c) distributing guidelines and instructions on how to setup the '266 Accused 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 obtains 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.

382. Keysight updates and maintains a support website that includes technical documentation encouraging the use of the '266 Accused Products in an infringing manner. This technical documentation includes knowledge articles, videos, user guides, technical support articles, and a knowledge center. The technical documentation covers the operation of

the '266 Accused Products in-depth, including by advertising the '266 Accused Products' infringing features and instructing customers, users, and vendors to configure and use the Accused Products in an infringing manner. *See, e.g.*, Ex. 73 (https://www.keysight.com/us/en/support.html); Ex. 74 (https://support.keysight.com/s/?language=en_US); Ex. 75 (https://support.ixiacom.com/).

383. Keysight contributorily infringes the '266 Patent pursuant to 35 U.S.C. § 271(c) because it provided its '266 Accused Products as software and computer systems with software installed, which act as a material component of the '266 Patent claims when combined with other components to create a complete network security system. Keysight knows that its products are particularly suited to be used in an infringing manner. The '266 Accused Products and their associated software are highly developed and 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 '266 Patent.

384. Keysight has knowingly and actively contributed to the direct infringement of the '266 Patent by its manufacture, use, offer to sell, sale and importation of the '266 Accused Products together with its customers, users, and vendors to meet the elements of the '266 Patent, as described above and incorporated by reference here. To the extent Keysight's 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 for CloudLens, which infringes when a third party runs

this software on processors and memory in a cloud environment. As another example, Keysight sold the Testing products, which infringe when a third party combines them for use with other Keysight's products, such as its Network Visibility products and ThreatArmor. To the extent Keysight's customers, users, and vendors direct and control the systems and methods in the claims, Keysight obtains 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. For example, threat information obtained through the filtering of packets can be provided to other Keysight's products or to the ATI research center as threat intelligence, which strengthens these other products' ability to prevent network threats.

385. Keysight's indirect infringement has caused and is continuing to cause damage and irreparable injury to Centripetal, and Centripetal will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

386. Keysight has known or, in the alternative, has been willfully blind to Centripetal's technology and the '266 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 '266 Patent to avoid infringement despite Keysight's knowledge and understanding that its products and services infringe the '266 Patent.

387. Centripetal is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Centripetal prays for relief and judgment as follows:

(A) An entry of judgment holding that Keysight has infringed and is infringing the Asserted Patents.

(B) A preliminary and permanent injunction against Keysight and its officers, employees, agents, servants, attorneys, instrumentalities, and/or those in privity with them, from infringing the Asserted Patents.

(C) An award to Centripetal of such damages as it shall prove at trial against Keysight that is adequate to fully compensate Centripetal for Keysight's infringement of the Asserted Patents.

(D) A determination that Keysight's infringement has been willful, wanton, deliberate, and egregious;

(E) A determination that the damages against Keysight be trebled or for any other basis within the Court's discretion pursuant to 35 U.S.C. § 284;

(F) A finding that this case is "exceptional" and an award to Centripetal of its costs and reasonable attorneys' fees, as provided by 35 U.S.C. § 285;

(G) An accounting of all infringing sales and revenues, together with post judgment interest and prejudgment interest from the first date of infringement of the Asserted Patents.

(H) Such further and other relief as the Court may deem proper and just.

Respectfully submitted,

Dated: January 1, 2022

By: */s/ Stephen E. Noona*

Stephen E. Noona
Virginia State Bar No. 25367
KAUFMAN & CANOLES, P.C.
150 W Main St., Suite 2100
Norfolk, VA 23510
Telephone: (757) 624-3239
Facsimile: (888) 360-9092
senoona@kaufcan.com

Kevin O'Donnell
Henry & O'Donnell P.C.
300 N. Washington St, Suite 204
Alexandria, VA 22314
Telephone: (703) 548-2100
kmo@henrylaw.com

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

Attorneys for Plaintiff
CENTRIPETAL NETWORKS, INC.

DEMAND FOR JURY TRIAL

In accordance with Rule 38 of the Federal Rules of Civil Procedure, Plaintiff respectfully demands a jury trial of all issues triable to a jury in this action.

Respectfully submitted,

Dated: January 1, 2022

By: */s/ Stephen E. Noona*

Stephen E. Noona
Virginia State Bar No. 25367
KAUFMAN & CANOLES, P.C.
150 W Main St., Suite 2100
Norfolk, VA 23510
Telephone: (757) 624-3239
Facsimile: (888) 360-9092
senoona@kaufcan.com

Kevin O'Donnell
Henry & O'Donnell P.C.
300 N. Washington St, Suite 204
Alexandria, VA 22314
Telephone: (703) 548-2100
kmo@henrylaw.com

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

Attorneys for Plaintiff
CENTRIPETAL NETWORKS, INC.