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

CENTRIPETAL NETWORKS, INC.,	)	
	)	
Plaintiff,	)	No. 2:18-CV-00094-MSD-LRL
	)	
vs.	)	
	)	JURY TRIAL DEMANDED
CISCO SYSTEMS, INC.,	)	
	)	
Defendant.	)	
	)	

AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Centripetal Networks, Inc. ("Centripetal") files this Complaint for Patent Infringement and Demand for Jury Trial against Cisco Systems, Inc. ("Defendant" or "Cisco") 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. Centripetal was founded with a strong focus on innovation and technology leadership that aligns to its core mission and purpose to protect networks from advanced threats. Centripetal has invented core networking technologies that meet the scale of the cyber threat intelligence challenge. Centripetal maintains the largest threat intelligence partner ecosystem, providing community based solutions to defeat sophisticated cyberattacks. In recognition of its innovation and expertise, Centripetal has been awarded numerous patents enabling its key technological advances in the network security area.

2. Cisco is a California Corporation with its principal place of business at 170 West Tasman Drive, San Jose, California 95134. Cisco may be served through its agent for service of process CSC at 2710 Gateway Oaks Dr. Ste. 150N, Sacramento, California 95833. Cisco maintains a regular and established place of business in this District through multiple permanent physical facilities. Cisco maintains a Technical Support Center located at 1051 East Cary Street 5th Floor, Richmond, Virginia 23219. Cisco also maintains the Cisco Systems Customer Experience Center located at 13600 Dulles Technology Drive Building #6, Wilson Building, Herndon, VA 20171. Further, Cisco also maintains another permanent facility located at 1860 Michael Faraday Drive #100, Reston, VA 20190.

3. Cisco 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 and outside of Virginia and within the Eastern District of Virginia. Further, Cisco directly or indirectly uses, distributes, markets, sells, and/or offer to sells throughout the United States, including in this judicial district, various telecommunication products, including networking switches, routers, and cloud products.

JURISDICTION AND VENUE

4. This is an action for patent infringement arising under the patent laws of the United States, Title 35, United States Code. This Court has exclusive subject matter jurisdiction over this case for patent infringement under 28 U.S.C. § 1338.

5. This Court has personal jurisdiction over Cisco. Cisco has conducted and does conduct business within the State of Virginia. Cisco maintains a regular and established place of business in this District through a permanent physical facility located at 1051 East Cary

Street 5th Floor, Richmond, Virginia 23219. Cisco, directly or through subsidiaries or intermediaries (including distributors, retailers, and others), ships, distributes, offers for sale, sells, and advertises (including the provision of an interactive web page) their products and/or services in the United States, the State of Virginia, and the Eastern District of Virginia. Cisco, directly and through subsidiaries or intermediaries (including distributors, retailers, and others), has purposefully and voluntarily placed one or more of their 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. Cisco has committed acts of patent infringement within the State of Virginia and, more particularly, within the Eastern District of Virginia.

6. Venue is proper in the Eastern District of Virginia under 28 U.S.C. §§ 1391 and 1400(b). Cisco has transacted business in this District, and has directly committed acts of patent infringement in this District, and has a regular and established place of business in this District. Cisco maintains several regular and established place of business in this District described above. Centripetal is informed and believes that Cisco employs a number of personnel in this District, including personnel involved in Cisco's infringement by at least through the testing, demonstration, support, use, offer for sale, and sale of the accused products and services within Virginia.

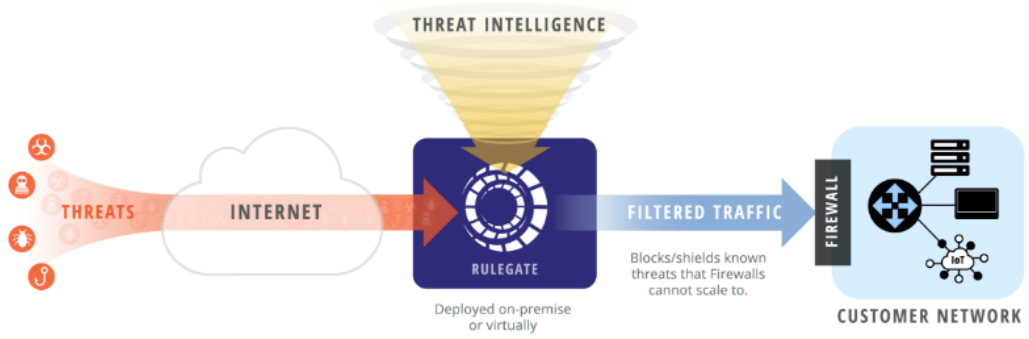
CENTRIPETAL'S INNOVATIONS

7. Centripetal was founded in 2009. Centripetal is the forerunner in developing cybersecurity technologies capable of fully operationalizing and automating threat intelligence at scale. These technologies protect organizations form advanced threats by extrapolating

every and any threat intelligence feed and applying advanced packet filtering at the network edge to prevent unwanted traffic from hitting an organization's network. Centripetal has been awarded, and continues to prosecute, numerous patents covering innovations in the United States and around the world resulting directly from Centripetal's research and development efforts.

8. Centripetal built and sold software and appliances for network security using these patented technologies. Centripetal's CleanINTERNET® solution utilizes its patented Threat Intelligence Gateway, which allows organizations to eradicate threats based on threat intelligence enforcement and furthermore, focuses on investigating the 10% of unknown threats.

Centripetal's Threat Intelligence Gateway solutions are available to enterprise teams as a service, on-premise or virtually.



9. Centripetal's Threat Intelligence Gateway includes the RuleGATE 2000 Gateway series, which "are ultra-high performance threat intelligence gateways with real-time attack visualization and analytics." *See* Centripetal RuleGATE Service Datasheet, available at https://cdn2.hubspot.net/hubfs/3851017/Centripetal_Networks_September2017/PDF/CNI-RuleGATE2000-V0-2.pdf?t=1518206754723, attached hereto as Exhibit 1.

10. Centripetal is recognized as an innovative technology company. Centripetal was named the SINET 16 Innovator for 2017 at the SINET Showcase in Washington D.C. Gartner, the world's leading research and advisory company, recognized Centripetal as a Cool Vendor in Security for Technology and Service Providers in 2017.

CENTRIPETAL'S ASSERTED PATENTS

11. On July 20, 2017, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,686,193 (the "'193 Patent"), entitled "Filtering Network Data Transfers." A true and correct copy of the '193 Patent is attached hereto as Exhibit 2.

12. The '193 Patent is generally directed towards computer networks, and more particularly, provides a system to protect computer networks from network threats. One of the ways this is accomplished is filtering network data packet transfers based on one or more rules to facilitate the protection of computers and networks from network threats.

13. On January 31, 2017, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,560,176 (the "'176 Patent"), entitled "Correlating Packets in Communications Networks." A true and correct copy of the '176 Patent is attached hereto as Exhibit 3.

14. The '176 Patent is generally directed towards computer networks, and more particularly, provides a system to improve the flow of data packets transferring between networks. One of the ways this is accomplished is generating log entries corresponding to the data packets and utilizing the log entries and the packets to correlate the packets transferred between the networks.

15. On January 31, 2017, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,560,077 (the "'077 Patent"), entitled "Methods and Systems

for Protecting a Secured Network." A true and correct copy of the '077 Patent is attached hereto as Exhibit 4.

16. The '077 Patent is generally directed towards computer networks, and more particularly, provides a system to protect computer networks from attacks. One of the ways this is accomplished is filtering network data packet transfers based on dynamic security policies to facilitate the protection of computers and networks from network threats.

17. On August 9, 2016, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,413,722 (the "'722 Patent"), entitled "Rule-Based Network-Threat Detection." A true and correct copy of the '722 Patent is attached hereto as Exhibit 5.

18. The '722 Patent is generally directed towards computer networks, and more particularly, provides a system to protect computer networks from network threats. One of the ways this is accomplished is filtering network data packet transfers based on one or more rules corresponding to one or more network-threat indicators to facilitate the protection of computers and networks from network threats.

19. On December 1, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,203,806 (the "'806 Patent"), entitled "Rule Swapping in a Packet Network." A true and correct copy of the '806 Patent is attached hereto as Exhibit 6.

20. The '806 Patent is generally directed towards computer networks, and more particularly, provides a system to protect computer networks from network threats. One of the ways this is accomplished is processing network data packet transfers based on one or more rule sets to facilitate the protection of computers and networks from network threats.

21. On October 13, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,160,713 (the "'713 Patent"), entitled "Filtering

Network Data Transfers." A true and correct copy of the '713 Patent is attached hereto as Exhibit 7.

22. The '713 Patent is generally directed towards computer networks, and more particularly, provides a system to protect computer networks from network threats. One of the ways this is accomplished is filtering network data packet transfers based on one or more rules to facilitate the protection of computers and networks from network threats.

23. On September 1, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,124,552 (the "'552 Patent"), entitled "Filtering Network Data Transfers." A true and correct copy of the '552 Patent is attached hereto as Exhibit 8.

24. The '552 Patent is generally directed towards computer networks, and more particularly, provides a system to protect computer networks from network threats. One of the ways this is accomplished is filtering network data packet transfers based on one or more rules to facilitate the protection of computers and networks from network threats.

25. On February 7, 2017, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,565,213 (the "'213 Patent"), entitled "Methods and Systems for Protecting a Secured Network." A true and correct copy of the '213 Patent is attached hereto as Exhibit 9.

26. The '213 Patent is generally directed towards computer networks, and more particularly, provides a system to protect computer networks from attacks. One of the ways this is accomplished is filtering network data packet transfers based on dynamic security policies to facilitate the protection of computers and networks from network threats.

27. On September 15, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,137,205 (the " '205 Patent"), entitled "Methods and

Systems for Protecting a Secured Network." A true and correct copy of the '205 Patent is attached hereto as Exhibit 10.

28. The '205 Patent is generally directed towards computer networks, and more particularly, provides a system to protect computer networks from attacks. One of the ways this is accomplished is filtering network data packet transfers based on dynamic security policies to facilitate the protection of computers and networks from network threats.

29. On June 6, 2017, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,674,148 (the "'148 Patent"), entitled "Rule Swapping in a Packet Network." A true and correct copy of the '148 Patent is attached hereto as Exhibit 11.

30. The '148 Patent is generally directed towards computer networks, and more particularly, provides a system to protect computer networks from network threats. One of the ways this is accomplished is processing network data packet transfers based on one or more rule sets to facilitate the protection of computers and networks from network threats.

31. On March 13, 2018, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,917,856 ("the '856 patent"), entitled "Rule-based Network-Threat Detection for Encrypted Communications." A true and correct copy of the '856 patent is attached hereto as Exhibit 49.

32. The '856 patent is generally directed towards computer networks, and more particularly, provides a system to protect computer networks from network threats. One of the ways this is accomplished is detecting network threats in encrypted communications based on one or more rules to facilitate the protection of computers and networks from network threats.

33. Centripetal owns by assignment the entire right, title, and interest in and to the '193 Patent, the '176 Patent, the '077 Patent, the '722 Patent, the '806 Patent, the '713 Patent,

the '552 Patent, the '213 Patent, the '205 Patent, the '148 Patent, and the '856 Patent (collectively, "the Asserted Patents").

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

CISCO PRODUCTS

35. Cisco is a multi-billion dollar company which offers networking products for networks of all sizes. A major portion of Cisco's product line focuses on enterprise grade switches, routers, and cloud products.

36. Cisco makes, uses, sells, offers for sale, and/or imports into the United States and this District, products and services that utilize Cisco's IOS XE 16.6 Networking Software, including but not limited to Cisco's Catalyst Switches (the "Accused Catalyst Products"), Cisco's ASR and ISR Series Routers (the "Accused Router Products"). *See* https://www.cisco.com/c/en/us/products/switches/index.html, attached hereto as Exhibit 12; *see also* https://www.cisco.com/c/en/us/products/routers/index.html attached hereto as Exhibit 13.

37. Cisco makes, uses, sells, offers for sale, and/or imports into the United States and this District, Cisco ASA with FirePOWER Services Products (the "Accused ASA Products"). *See* https://www.cisco.com/c/en/us/products/security/asa-firepower-services/index.html, attached hereto as Exhibit 14.

38. Cisco also makes, uses, sells, offers for sale, and/or imports into the United States and this District, Cisco's Stealthwatch products. *See* https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html, attached hereto as Exhibit 15.

CISCO SWITCH AND ROUTER PRODUCTS

39. The Accused Catalyst Products include the Catalyst 9400 series and Catalyst

9300 series switches. The Catalyst series switches include C9300-24T, C9300-48T, C9300-24P, C9300-48P, C9300-24U, C9300-48U, C9300-24UX, C9300-48UXM, C9300-NM-4G, C9300-NM-8X, C9300-NM-2Q, C9407R, C9410R, C9407R, C9400-LC-48U, C9400-LC-48T, C9400-LC-48UX, and C9400-LC-24XS. *See* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.pdf, attached hereto at Exhibit 16; *see also* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/datasheet-c78-739053.pdf, attached hereto as Exhibit 17.

40. The Accused Router Products include the ASR 1001-X, ASR 1002-X, ASR 1001-HX, ASR 1002-HX, ASR1000 RP2, ASR1000 RP3, ASR1000 ESP-40, Integrated Services Virtual Router (ISRv) including the 5000 Enterprise Network Compute System, and Cloud Services Router (CSR) 1000V. *See* https://www.cisco.com/c/dam/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/at-a-glance-c45-612993.pdf, attached hereto as Exhibit 18; *see also* https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/datasheet-c78-732542.pdf, attached hereto as Exhibit 19.

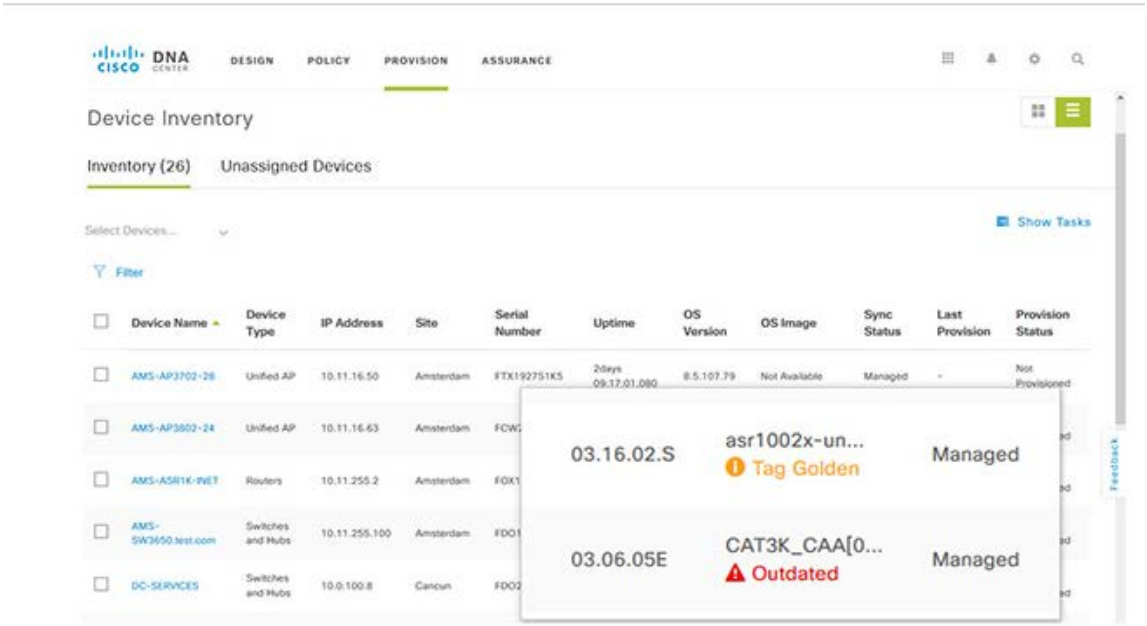
41. The Accused Catalyst Products and Accused Router Products are enterprise level networking products, which includes integrated security to address constantly evolving threats. The Accused Catalyst Products and Accused Router Products operate with the Cisco IOS XE 16 operating system, and includes a number of technologies such as Encrypted Traffic Analytics ("ETA"), Digital Network Architecture ("DNA"), Software-Defined Access ("SD-Access"), policy-based automation, Application Visibility and Control ("AVC"), Next-Generation Network-Based Application Recognition ("NBAR2"), Hitless ACL updates, ACL

Label-Sharing, DNS and SNI correlation, Policy management, and traffic filtering.

42. ETA addresses cyberattacks, where nearly half are hidden in encrypted traffic. ETA analyzes data from Cisco switches, referred to as NetFlow, learning to spot anomalies that could signal an incoming threat. ETA identifies known threats in encrypted traffic – without decrypting the traffic – resulting in a more secure and efficient network.

43. The Accused Catalyst Products and Accused Router Products use SD-Access and Cisco DNA technology to provide policy-based automation and network assurance from edge to cloud. Cisco DNA applies policies at the network edge to monitor suspicious activity in both encrypted and decrypted traffic. DNA also provides analytics and data displayed in an interactive user interface. As shown below, DNA provides automation, which allows policies to be automatically provisioned to multiple devices in the network. *See* https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/top6-cte-amer.pdf?oid=ifgen000258, attached hereto as Exhibit 20.

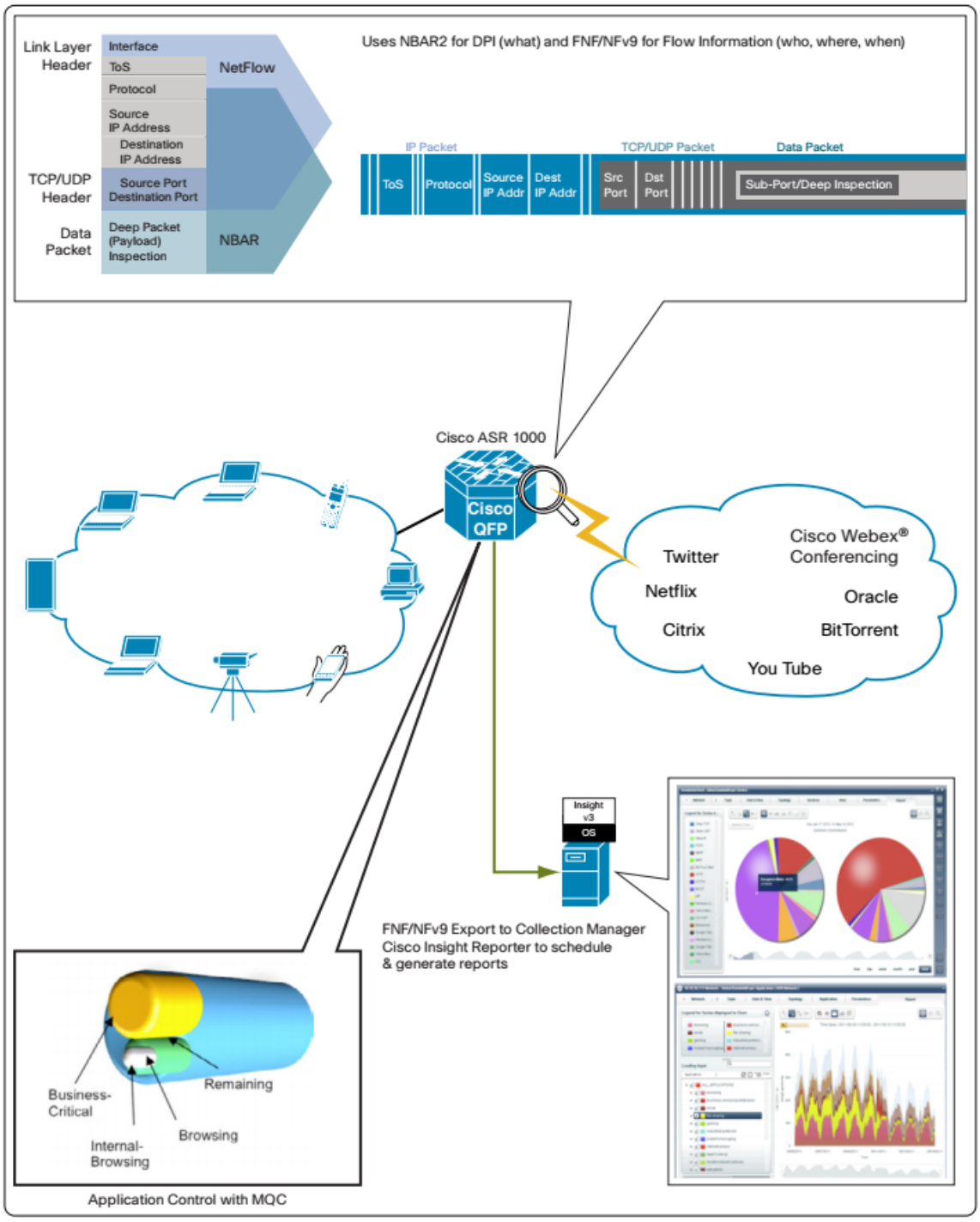
Automated provisioning



https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html#~stickynav=1, attached hereto as Exhibit 21, at 5.

44. The Accused Catalyst Products and Accused Router Products include AVC, which performs deep packet inspection ("DPI") to identify applications running through the network. AVC works in conjunction with NetFlow to gauge application usage and performance statistics, which is useful for analytics and security policies.

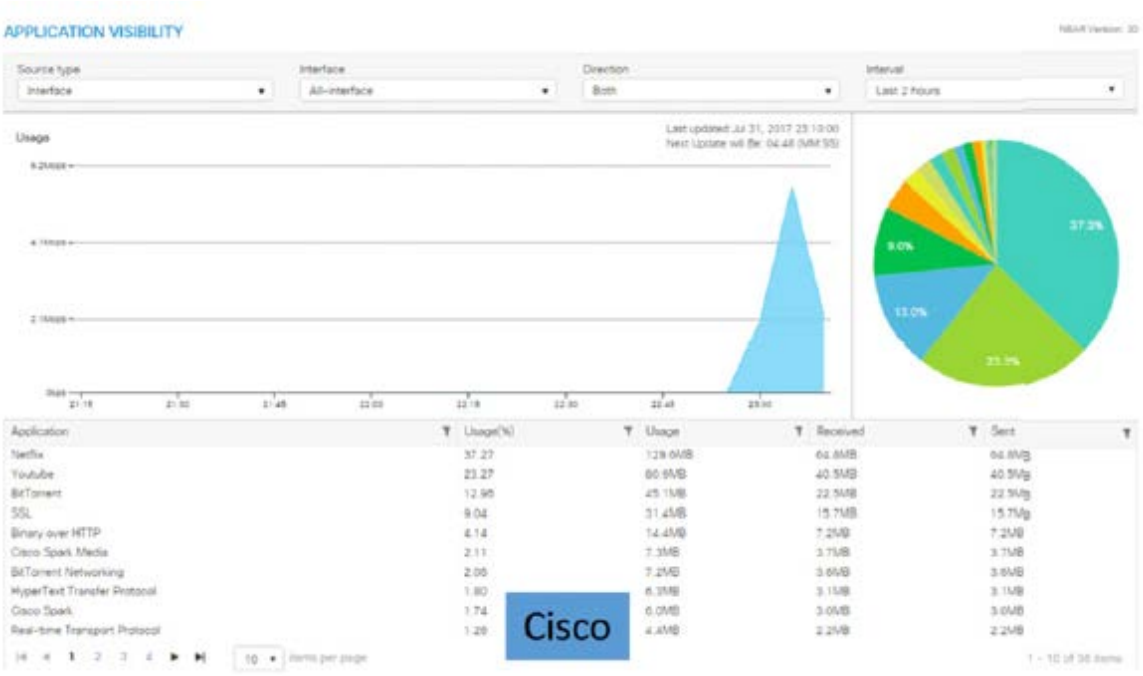
Figure 1. Cisco AVC Solution



https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/unified-wan-services/at_a_glance_c45-649117.pdf, attached hereto as Exhibit 22, at 1.

45. The Accused Catalyst Products and Accused Router Products use data collected

by AVC to generate and provide reports using the Cisco Insight Reporter.



See Miercom-Report-Cisco-vs-Huawei-Network-Architecture-DR170921G.pdf, attached hereto as Exhibit 23, at 20.

46. The Accused Catalyst Products and Accused Router Products include packet filtering rules to control the flow of network traffic. Management of packet filtering rules may be automated. Such packet filtering rules may be implemented using Access Control Lists ("ACL"), and automation allows packets to be dropped or forwarded to another network.

Example: Default Action of Dropping IP Packets and Forwarding MAC Packets

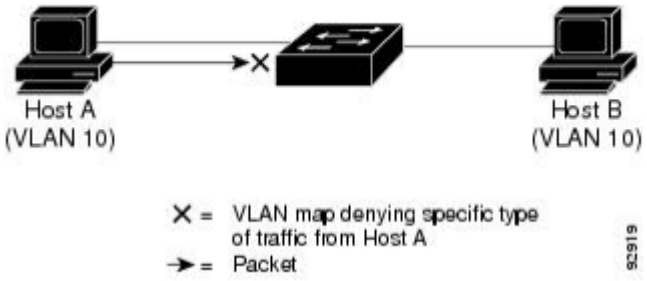
In this example, the VLAN map has a default action of drop for IP packets and a default action of forward for MAC packets. Used with standard ACL 101 and extended named access lists **igmp-match** and **tcp-match**, the map will have the following results:

- Forward all UDP packets
- Drop all IGMP packets
- Forward all TCP packets
- Drop all other IP packets
- Forward all non-IP packets

(Security Configuration Guide, Cisco IOS XE Everest 16.5.1a (Catalyst 9300 Switches)). https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-

5/configuration_guide/sec/b_165_sec_9300_cg.pdf, attached hereto as Exhibit 24, at 200.

Figure 15: Using VLAN Maps to Control Traffic



Id. at 209.

47. The Accused Catalyst Products and Accused Router Products include ACLs, which are configurable to prevent from continuing toward a destination based on one or more criteria.

Configuration Examples for ACLs and VLAN Maps

Example: Creating an ACL and a VLAN Map to Deny a Packet

This example shows how to create an ACL and a VLAN map to deny a packet. In the first map, any packets that match the *ip1* ACL (TCP packets) would be dropped. You first create the *ip1* ACL to permit any TCP packet and no other packets. Because there is a match clause for IP packets in the VLAN map, the default action is to drop any IP packet that does not match any of the match clauses.

```
Device(config)# ip access-list extended ip1
Device(config-ext-nacl)# permit tcp any any
Device(config-ext-nacl)# exit
Device(config)# vlan access-map map_1 10
Device(config-access-map)# match ip address ip1
Device(config-access-map)# action drop
```

Example: Creating an ACL and a VLAN Map to Permit a Packet

This example shows how to create a VLAN map to permit a packet. ACL *ip2* permits UDP packets and any packets that match the *ip2* ACL are forwarded. In this map, any IP packets that did not match any of the previous ACLs (that is, packets that are not TCP packets or UDP packets) would get dropped.

```
Device(config)# ip access-list extended ip2
Device(config-ext-nacl)# permit udp any any
Device(config-ext-nacl)# exit
Device(config)# vlan access-map map_1 20
Device(config-access-map)# match ip address ip2
Device(config-access-map)# action forward
```

Id. at 200.

48. The Accused Catalyst Products and Accused Router Products provide logging

information regarding packet filtering rules and network-threat indicators.

Examples: ACL Logging

Two variations of logging are supported on router ACLs. The **log** keyword sends an informational logging message to the console about the packet that matches the entry; the **log-input** keyword includes the input interface in the log entry.

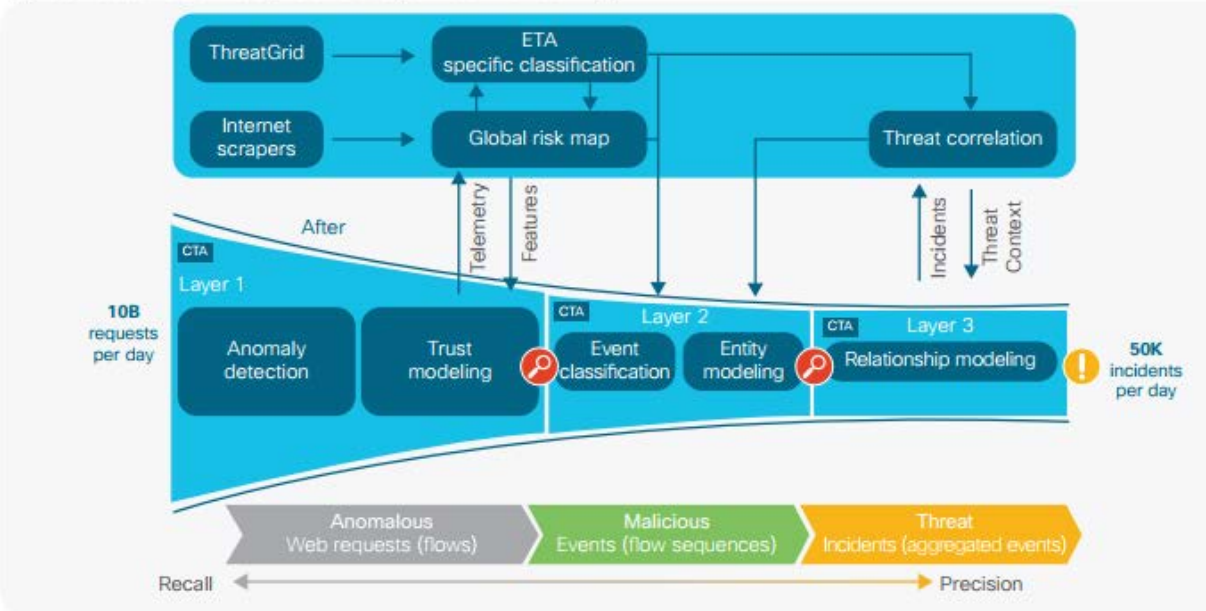
In this example, standard named access list *stan1* denies traffic from 10.1.1.0 0.0.0.255, allows traffic from all other sources, and includes the **log** keyword.

```
Device(config)# ip access-list standard stan1
Device(config-std-nacl)# deny 10.1.1.0 0.0.0.255 log
Device(config-std-nacl)# permit any log
Device(config-std-nacl)# exit
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group stan1 in
Device(config-if)# end
Device# show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level debugging, 37 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 37 messages logged
    File logging: disabled
    Trap logging: level debugging, 39 message lines logged

Log Buffer (4096 bytes):

00:00:48: NTP: authentication delay calculation problems

<output truncated>

00:09:34:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
00:09:59:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 1 packet
00:10:11:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
```

Id. at 198-99.

49. The Accused Catalyst Products and Accused Router Products include Multi-layer Machine Learning to receive packets at multiple OSI layers.

Figure 3. Stealtwatch Enterprise Multi-layer Machine Learning



(Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at 5.

50. The Accused Catalyst Products and Accused Router Products include policy-based automation, which allows provision of multiple devices using "policy-based automation from edge to cloud with foundational capabilities":

> The Cisco® Digital Network Architecture (DNA) with Software Defined Access (SD-Access) is the network fabric that powers business. Cisco DNA is an open and extensible, software-driven architecture that accelerates and simplifies your enterprise network operations. The programmable architecture frees your IT staff from time consuming, repetitive network configuration tasks so they can focus instead on innovation that positively transforms your business. SD-Access enables policy-based automation from edge to cloud with foundational capabilities. These include:
>
> - Simplified device deployment
> - Unified management of wired and wireless networks
> - Network virtualization and segmentation
> - Group-based policies
> - Context-based analytics

(Cisco Catalyst Data Sheet). https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/datasheet-c78-739053.pdf, attached hereto as Exhibit 17, at 1.

51. The Accused Catalyst Products and Accused Router Products include ports

which receive packets via communication interfaces that do not have network-layer addresses. Furthermore, the Accused Catalyst Products and Accused Router Products include ports which receive packets via communication interfaces that do have network-layer addresses.

Management Ports

The management ports connect the switch to a PC running Microsoft Windows or to a terminal server.

- Ethernet management port. See Ethernet Management Port, on page 18.
- RJ-45 console port (EIA/TIA-232). See RJ-45 Console Port, on page 19.
- USB mini-Type B console port (5-pin connector).

The 10/100/1000 Ethernet management port connection uses a standard RJ-45 crossover or straight-through cable. The RJ-45 console port connection uses the supplied RJ-45-to-DB-9 female cable. The USB console port connection uses a USB Type A to 5-pin mini-Type B cable. The USB console interface speeds are the same as the RJ-45 console interface speeds.

If you use the USB mini-Type B console port, the Cisco Windows USB device driver must be installed on any PC connected to the console port (for operation with Microsoft Windows). Mac OS X or Linux do not require special drivers.

The 4-pin mini-Type B connector resembles the 5-pin mini-Type B connectors. They are not compatible. Use only the 5-pin mini-Type B.

(Cisco Catalyst 9300 Series Switches Hardware Installation Guide). https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/hardware/install/b_c9300_hig.pdf, attached hereto as Exhibit 26, at 5.

CISCO STEALTHWATCH PRODUCTS

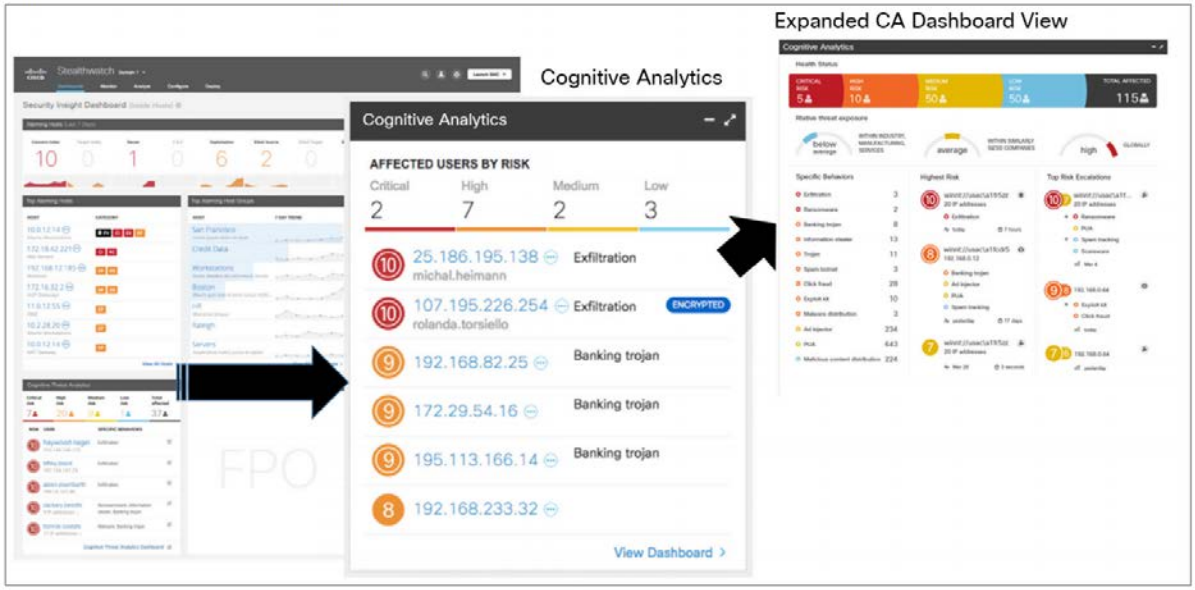
52. Cisco Stealthwatch Products include Cisco Stealthwatch Endpoint License and Stealthwatch Cloud (the "Accused Stealthwatch Products"). *See* https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch/datasheet-c78-739398.pdf, attached hereto as Exhibit 27.

53. Cisco Stealthwatch Enterprise is a scalable solution to provide visibility and security analytics in an enterprise network. Stealthwatch Cloud is available as a cloud solution. Stealthwatch uses machine learning and behavioral modeling to detect threats and protect critical data in the network.

54. Stealthwatch also includes ETA, DNA with SD-Access, and AVC, discussed above.

55. Stealthwatch also includes Cognitive Threat Analytics ("CTA"), which pinpoints attacks before they can exfiltrate data. CTA analyzes data from multiple sources and uses machine learning techniques to identify malicious activity. CTA provides threat summaries in an interactive user interface, and also works with ETA to detect malware in encrypted traffic. *See* https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-a-glance-c45-736555.pdf, attached hereto as Exhibit 28.

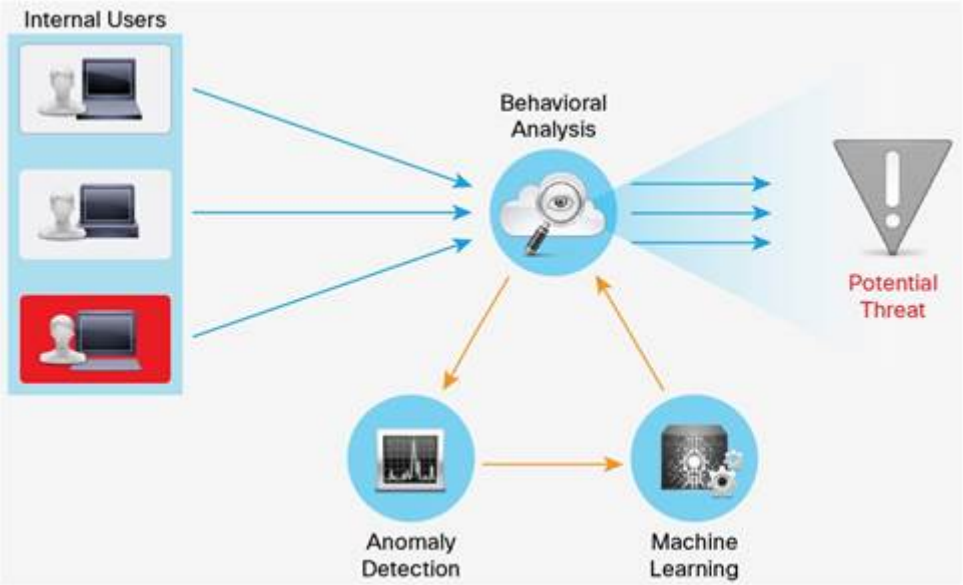
Figure 4. Stealthwatch security insight dashboard



(Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at 6.

56. CTA "[a]nalyz[es] more than 10 billion web requests daily, [and] finds malicious activity that has bypassed security controls, or entered through unmonitored channels (including removable media), and is operating inside an organization's environment. Cognitive Threat Analytics is a cloud-based product that uses machine learning and statistical modeling of networks. It creates a baseline of the traffic in your network and identifies anomalies. It analyzes user and device behavior, and web traffic, to discover command-and-

control communications, data exfiltration, and potentially unwanted applications operating in your infrastructure (Figure 1)."

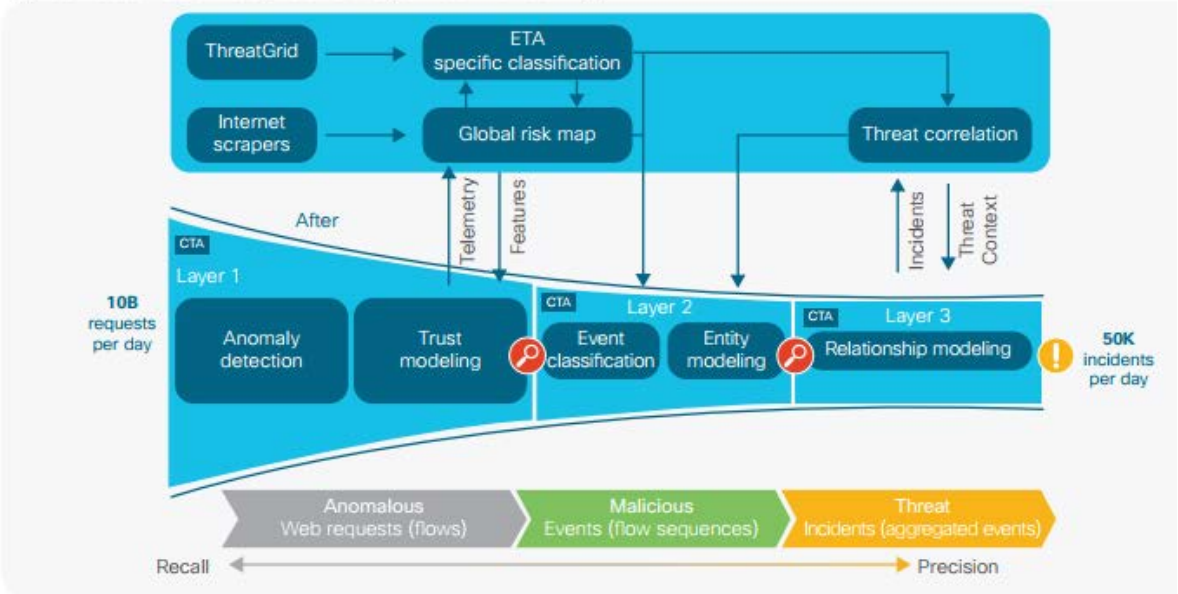


https://www.cisco.com/c/en/us/products/collateral/security/cognitive-threat-analytics/datasheet-c78-736557.html, attached hereto as Exhibit 29, at 1.

57. CTA "is integrated with Cisco AMP Threat Grid. When CTA independently detects command-and-control communication in the web channel, it queries the AMP Threat Grid database and correlates the indicators of compromise with the millions of malware artifacts seen by AMP Threat Grid to identify the malware that caused the anomaly." *Id.* at 2. CTA also provides Automated Response and "integrates with existing security monitoring technologies, including Security Information and Event Management (SIEM) platforms. Organizations can integrate and automate their response with an established workflow." *Id.*

58. As shown below, Stealthwatch may receive and filter packets based on packet filtering rules. Stealthwatch may identify packets received by a network device from a host machine in one network and generate log entries corresponding to those packets.

Figure 3. Stealtwatch Enterprise Multi-layer Machine Learning



(Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at 5.

CISCO ASA WITH FIREPOWER SERVICES PRODUCTS

59. The Accused ASA Products include Cisco ASA 5506-X, Cisco ASA 5506W-X, Cisco ASA 5506H-X, Cisco ASA 5508-X, Cisco ASA 5516-X, Cisco ASA 5512-X, Cisco ASA 5515-X, Cisco ASA 5525-X, Cisco ASA 5545-X, Cisco ASA 5555-X, Cisco ASA 5585-X SSP-10, Cisco ASA 5585-X SSP-20, Cisco ASA 5585-X SSP-40, Cisco ASA 5585-X SSP-60, Cisco ASA 5585-X SSP EP 10/40, and Cisco ASA 5585-X SSP EP 20/60, as described in https://www.cisco.com/c/en/us/products/security/asa-firepower-services/index.html, attached hereto as Exhibit 14.

60. Cisco ASA with FirePOWER Services is a security appliance, also known as a Next Generation Firewall ("NGFW"), designed to protect organizations from cyber attacks. The Cisco ASA with FirePOWER Services includes technologies such as unified security services and task automation, CTA, AVC, Adaptive Security Device Manager ("ASDM"), and

Transactional Commit Modeling.

61. Cisco ASA with FirePOWER Services includes Transactional-Commit Modeling, which is "a new feature for rule updation" of ACL rules. With Transactional-Commit Modeling, "a rule update is applied after the rule compilation is completed; without affecting the rule matching performance. With the legacy model, rule updates take effect immediately but rule matching slows down during the rule compilation period. This feature is useful to prevent potential packet drops during large compilation of rules under high traffic conditions."

Transactional-Commit Model

The ASA rule-engine supports a new feature for rule updation called the Transactional-Commit Model. When this feature is enabled, a rule update is applied after the rule compilation is completed; without affecting the rule matching performance. With the legacy model, rule updates take effect immediately but rule matching slows down during the rule compilation period. This feature is useful to prevent potential packet drops during large compilation of rules under high traffic conditions. This feature is also useful to reduce the rule compilation time under two specific patterns of configurations:

- Preventing packet drops while compiling large rules during high traffic rates.
- Reducing rule compilation time while updating a large number of similar rules.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/firewall/asa_91_firewall_config/access_rules.html, attached hereto as Exhibit 30, at 6-4.

CISCO'S INFRINGEMENT OF CENTRIPETAL'S PATENTS

62. Cisco 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 Catalyst Products, the Accused Router Products, the Accused ASA Products, and the Accused Stealthwatch Products, alone or in conjunction with one another (collectively, "the Accused Products").

63. In addition to directly infringing the Asserted Patents pursuant to 35 U.S.C. § 271(a), either literally or under the doctrine of equivalents, or both, Cisco indirectly infringes all the Asserted Patents by instructing, directing and/or requiring others, including its

customers, purchasers, users, and developers, to perform all or some of the steps of the method claims, either literally or under the doctrine of equivalents, or both, of the Asserted Patents.

64. Centripetal's products and services are marked with Centripetal's patents. For example, Centripetal builds and sells RuleGATE 2000, a product which is marked with at least the '806 Patent, the '713 Patent, the '205 Patent, the '552 Patent, the '213 Patent, the '077 Patent, and the '176 Patent.

65. Cisco has willfully infringed each of the Asserted Patents. Centripetal is informed and believes that Cisco had knowledge of the Asserted Patents through various channels and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

66. On or around 2014, Centripetal partnered with ThreatGRID, a company which included threat intelligence technology which Centripetal integrated with their patented products that used some of the Asserted Patents. Cisco later acquired ThreatGRID in 2016. Centripetal is informed and believes that Cisco gained increased exposure to Centripetal's patented technology as a result of the acquisition of ThreatGRID. https://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/threatgrid.html, attached hereto as Exhibit 31.

67. Centripetal is further informed and believes that, on or around January 2016, Cisco requested an introduction to Centripetal through a third party, Granite Hill Capital Partners. Later, Centripetal received a point of contact introduction to Cisco from Granite Hill Capital Partners.

68. In 2016, Cisco invited Centripetal to participate in Cisco Live, which is Cisco's partner conference – in which Centripetal was asked to demonstrate its technology in Cisco's

"Security Partner Village" booth. On or around June 2016, Centripetal attended the Cisco Live conference and demonstrated its patented technology, including the RuleGATE Threat Intelligence Gateway product which encompasses at least some of the Asserted Patents. Cisco currently lists Centripetal on its website located at www.cisco.com, as part of a "partner ecosystem" whose "[t]hreat intelligence platforms" use Threat Grid. https://www.cisco.com/c/en/us/products/security/threat-grid/integrations.html#~stickynav=2, attached hereto as Exhibit 32, at 3.

69. Centripetal is informed and believes that despite Cisco's knowledge of the Asserted Patents and Centripetal's patented technology, Cisco made the deliberate decision to sell products and services that it knew infringes Centripetal's Asserted Patents.

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

71. Centripetal is informed and believes that Cisco knew or was willfully blind to Centripetal's technology. Despite this knowledge and/or willful blindness, Cisco 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 '193 Patent pursuant to 35 U.S.C. § 271(a))

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

73. Cisco has infringed and continues to infringe Claims 1-20 of the '193 Patent in violation of 35 U.S.C. § 271(a).

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

75. Cisco'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.

76. Cisco's infringement includes the manufacture, use, sale, importation and/or offer for sale of Cisco's products and services, including but not limited to the Accused Catalyst Products, the Accused Router Products, and the Accused Stealthwatch Products, alone or in conjunction with one another (collectively, the "Accused '193 Products").

77. The Accused '193 Products embody the patented invention of the '193 Patent and infringe the '193 Patent because they practice a method comprising:

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

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

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

dropping, by the computing system, each packet in first portion of packets; and
responsive to a determination by the computing system that the second portion of packets
comprises data that does not correspond to the criteria wherein the data indicates that the second portion of packets is destined for a third network:

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

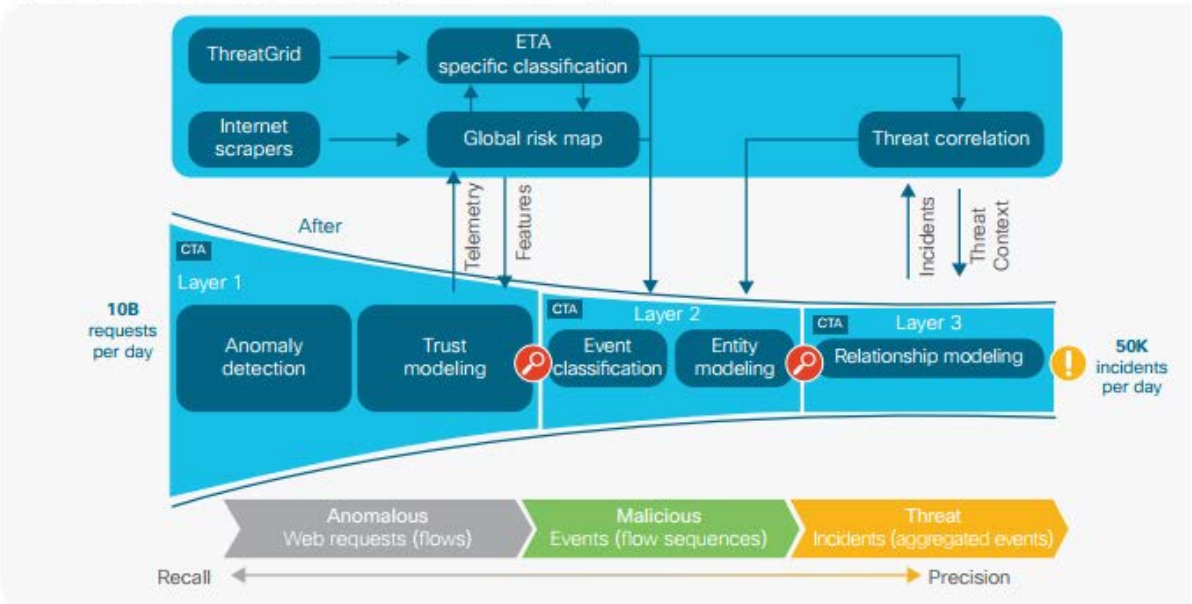
with the particular type of data transfer toward the third network; and

forwarding, by the computing system, each packet in the second portion of packets toward the third network.

'193 Patent, Claim 1.

78. As shown below, the Accused '193 Products perform the step of "receiving, by a computing system and from a computing device located in a first network, a plurality of packets, wherein the plurality of packets comprises a first portion of packets and a second portion of packets":

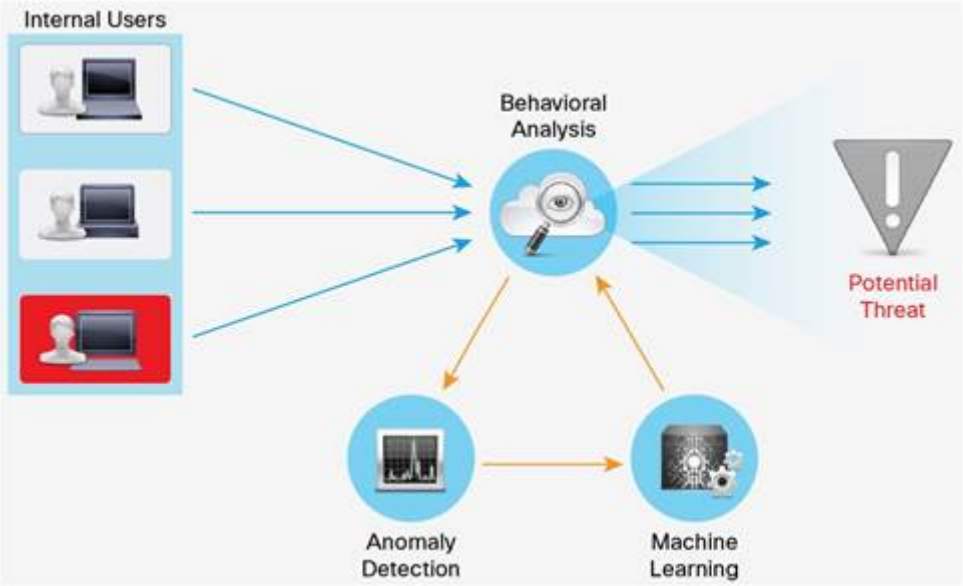
Figure 3. Stealtwatch Enterprise Multi-layer Machine Learning



(Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at 5.

79. The Accused '193 Products include Cognitive Threat Analytics ("CTA"). CTA "[a]nalyz[es] more than 10 billion web requests daily, [and] finds malicious activity that has bypassed security controls, or entered through unmonitored channels (including removable media), and is operating inside an organization's environment. Cognitive Threat Analytics is a

cloud-based product that uses machine learning and statistical modeling of networks. It creates a baseline of the traffic in your network and identifies anomalies. It analyzes user and device behavior, and web traffic, to discover command-and-control communications, data exfiltration, and potentially unwanted applications operating in your infrastructure (Figure 1)."



https://www.cisco.com/c/en/us/products/collateral/security/cognitive-threat-analytics/datasheet-c78-736557.html, attached hereto as Exhibit 29, at 1.

80. CTA "is integrated with Cisco AMP Threat Grid. When CTA independently detects command-and-control communication in the web channel, it queries the AMP Threat Grid database and correlates the indicators of compromise with the millions of malware artifacts seen by AMP Threat Grid to identify the malware that caused the anomaly." *Id.* at 2. CTA also provides Automated Response and "integrates with existing security monitoring technologies, including Security Information and Event Management (SIEM) platforms. Organizations can integrate and automate their response with an established workflow." *Id.*

81. As shown below, the Accused '193 Products perform the step of "responsive to a determination by the computing system that the first portion of packets comprises data

corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network: applying, by the computing system and to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and dropping, by the computing system, each packet in first portion of packets." '193 Patent, Claim 1. As shown below, the Accused '193 Products "turns the network into an end-to-end sensor and enforcer that detects, contains and prevents emerging sophisticated security threats":

Conclusion

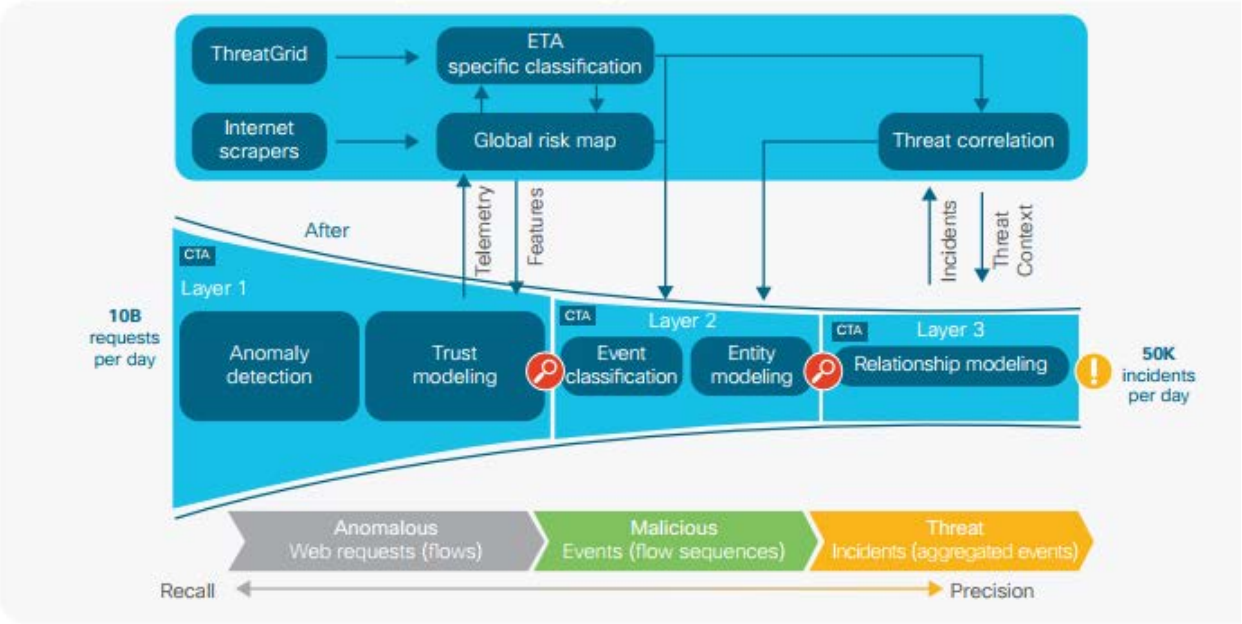
In summary, the network is now an even more advanced security sensor, capable of detecting threats in encrypted traffic. A Cisco Digital Network Architecture-ready infrastructure turns the network into an end-to-end sensor and enforcer that detects, contains and prevents emerging, sophisticated security threats.

(Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf., attached hereto as Exhibit 25, at 8.

82. Further, the Accused '193 Products perform the step of "responsive to a determination by the computing system that the second portion of packets comprises data that does not correspond to the criteria wherein the data indicates that the second portion of packets is destined for a third network: applying, by the computing system and to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the third network; and forwarding, by the computing system, each packet in the second portion of packets toward the third network." '193 Patent, Claim 1. As

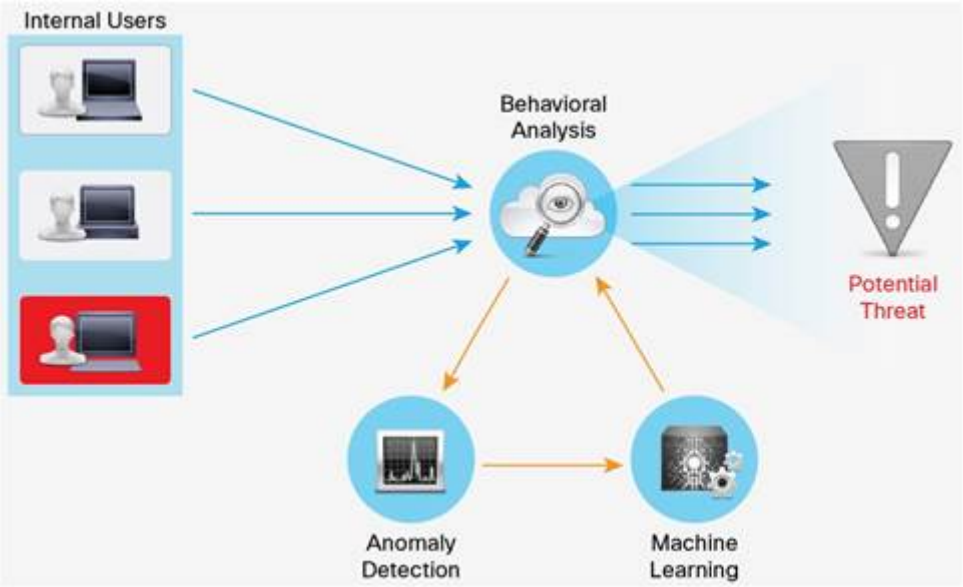
shown below, the Accused '193 Products "correlate traffic with global threat behaviors to automatically identify infected hosts, command and control communication and suspicious traffic":

Figure 3. Stealtwatch Enterprise Multi-layer Machine Learning



Id. at 5.

83. The Accused '193 Products include Cognitive Threat Analytics ("CTA"). CTA "[a]nalyz[es] more than 10 billion web requests daily, [and] finds malicious activity that has bypassed security controls, or entered through unmonitored channels (including removable media), and is operating inside an organization's environment. Cognitive Threat Analytics is a cloud-based product that uses machine learning and statistical modeling of networks. It creates a baseline of the traffic in your network and identifies anomalies. It analyzes user and device behavior, and web traffic, to discover command-and-control communications, data exfiltration, and potentially unwanted applications operating in your infrastructure (Figure 1)."



https://www.cisco.com/c/en/us/products/collateral/security/cognitive-threat-analytics/datasheet-c78-736557.html, attached hereto as Exhibit 29, at 1.

84. CTA "is integrated with Cisco AMP Threat Grid. When CTA independently detects command-and-control communication in the web channel, it queries the AMP Threat Grid database and correlates the indicators of compromise with the millions of malware artifacts seen by AMP Threat Grid to identify the malware that caused the anomaly." *Id.* at 2. CTA also provides Automated Response and "integrates with existing security monitoring technologies, including Security Information and Event Management (SIEM) platforms. Organizations can integrate and automate their response with an established workflow." *Id.*

85. The Accused '193 Products use "[t]raditional flow monitoring, as implemented in the Cisco® Network as a Sensor (NaaS) solution and through the use of NetFlow, provides a high-level view of network communications by reporting the addresses, ports, and byte and packet counts of a flow. In addition, *intraflow metadata*, or information about events that occur inside of a flow, can be collected, stored, and analyzed within a flow monitoring framework. This data is especially valuable when traffic is encrypted, because deep-packet inspection is no

longer viable. This intraflow metadata, called *Encrypted Traffic Analytics* (ETA), is derived by using new data elements or telemetry that are independent of protocol details, such as the lengths and arrival times of packets within a flow. These data elements have the property of applying equally well to both encrypted and unencrypted flows. ETA focuses on identifying malware communications in encrypted traffic through passive monitoring, the extraction of relevant data elements, and supervised machine learning with cloud based global visibility. ETA extracts three main data elements: the initial data packet, the sequence of packet length and times, and TLS-specific features." (Encrypted Traffic Analytics Deployment Guide). CVD-Encrypted-Traffic-Analytics-Deployment-Guide-2017DEC.pdf. attached hereto as Exhibit 33, at 1.

Appendix A: ETA Data Elements

Data Element Name	Description
Sequence of Packet Lengths and Times	An array of LENGTH values followed by an array of INTERARRIVAL TIME values describing the first N packets of a flow that carry application payload. Each LENGTH is encoded as a 16-bit integer to form a 20-byte array. Immediately following this, each INTERARRIVAL TIME is encoded as a 16-bit integer to form another 20-byte array.
Initial data packet	The content of the first packet of this flow that contains actual payload data, starting at the beginning of the IP header.
TLS records	An array of LENGTH values, followed by an array of INTERARRIVAL TIME values, followed by an array of CONTENT TYPE values, followed by an array of HANDSHAKE TYPE values. These arrays describe the first N records of a TLS flow.
TLS record lengths	A sequence of record lengths for up to the first N records of a TLS flow.
TLS record times	A sequence of TLS interarrival times for up to the first N records of a TLS flow.
TLS content types	A sequence of ContentType values for up to the first N records of a TLS flow.
TLS handshake types	A sequence of HandshakeType values for up to the first N records of a TLS flow.
TLS cipher suites	A list of up to N cipher suites offered by the client, or selected by the server in a TLS flow.
TLS extensions	An array of LENGTH values followed by an array of EXTENSION TYPE values describing the TLS extensions observed in the Hello message for a TLS flow.
TLS extension lengths	A list of extension lengths for up to the first N TLS extensions observed in the TLS Hello message for a flow.
TLS extension types	A list of extension types for up to the first N TLS extensions observed in the TLS Hello message for a flow.
TLS version	The TLS version number observed in the TLS Hello message for a flow.
TLS key length	The length of the client key observed in the TLS ClientKeyExchange message.
TLS session ID	The session ID value observed (if any) in the TLS Hello message for a flow.
TLS random	The random value observed in the TLS Hello message for this flow.

Id. at 60.

86. The Accused '193 Products use "NetFlow, proxy servers, endpoint telemetry, policy and access engines, traffic segmentation and more to establish baseline 'normal' behavior for hosts and users across the enterprise. Stealthwatch can correlate traffic with global threat behaviors to automatically identify infected hosts, command and control communication and suspicious traffic. Stealthwatch maintains a global risk map – a very broad behavioral profile about servers on the Internet, identifying servers that are related to attacks, may be exploited, or may be used as a part of an attack in the future (Figure 3). This is not a blacklist, but a holistic picture from a security perspective. Stealthwatch analyzes the new encrypted

traffic data elements in enhanced NetFlow by applying machine learning and statistical modeling. The global risk map and Encrypted Traffic Analytics data elements reinforce using advance security analytics. Rather than decrypting the traffic, Stealthwatch uses machine learning algorithms to pinpoint malicious patterns in encrypted traffic to help identify threats and improve incident response." (Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at 5.

87. As a result of Cisco'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.

88. Cisco's infringement of the '193 Patent has injured and continues to injure Centripetal in an amount to be proven at trial.

89. Cisco has willfully infringed each of the Asserted Patents. Centripetal is informed and believes that Cisco had knowledge of the Asserted Patents through various channels and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

90. On or around 2014, Centripetal partnered with ThreatGRID, a company which included threat intelligence technology which Centripetal integrated with their patented products that used some of the Asserted Patents. Cisco later acquired ThreatGRID in 2016. Centripetal is informed and believes that Cisco gained increased exposure to Centripetal's patented technology as a result of the acquisition of ThreatGRID. https://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/threatgrid.html, attached hereto as Exhibit 31.

91. Centripetal is further informed and believes that, on or around January 2016, Cisco requested an introduction to Centripetal through a third party, Granite Hill Capital Partners. Later, Centripetal received a point of contact introduction to Cisco from Granite Hill Capital Partners.

92. In 2016, Cisco invited Centripetal to participate in Cisco Live, which is Cisco's partner conference – in which Centripetal was asked to demonstrate its technology in Cisco's "Security Partner Village" booth. On or around June 2016, Centripetal attended the Cisco Live conference and demonstrated its patented technology, including the RuleGATE Threat Intelligence Gateway product which encompasses at least some of the Asserted Patents. Cisco currently lists Centripetal on its website located at www.cisco.com, as part of a "partner ecosystem" whose "[t]hreat intelligence platforms" use Threat Grid. https://www.cisco.com/c/en/us/products/security/threat-grid/integrations.html#~stickynav=2, attached hereto as Exhibit 32, at 3.

93. Cisco thus knew or, in the alternative, was willfully blind to Centripetal's technology and its Asserted Patents. Cisco's infringement of the '193 Patent is egregious because despite this knowledge, Centripetal is informed and believes that Cisco deliberately copied Centripetal's patented technology, which it implemented into its products and services, such as Centripetal's CleanINTERNET service and Threat Intelligence Gateway, including the RuleGATE 2000. The blatant copying of Centripetal's patented technology and disregard for Centripetal's patent rights with an objectively high likelihood of infringement is egregious behavior warranting a finding of willful infringement and enhanced damages.

94. Centripetal is informed and believes that Cisco has undertaken no efforts to design these products or services around the '193 Patent to avoid infringement despite Cisco's

knowledge and understanding that its products and services infringe the '193 Patent. As such, Cisco has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '193 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.

SECOND CAUSE OF ACTION
(Indirect Infringement of the '193 Patent pursuant to 35 U.S.C. § 271(b))

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. Cisco has induced and continues to induce infringement of one or more claims of the '193 Patent under 35 U.S.C. § 271(b).

97. In addition to directly infringing the '193 Patent, Cisco indirectly infringes the '193 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '193 Patent, where all the steps of the method claims are performed by either Cisco, its customers, purchasers, users or developers, or some combination thereof. Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the '193 Patent, including Claims 1-17 and 20.

98. Cisco knowingly and actively aided and abetted the direct infringement of the '193 Patent by instructing and encouraging its customers, purchasers, users and developers to use the '193 Accused Products. Such instructions and encouragement include, but are not limited to, advising third parties to use the '193 Accused Products in an infringing manner,

providing a mechanism through which third parties may infringe the '193 Patent, specifically through the use of the Accused Catalyst Products, the Accused Router Products, and the Accused Stealthwatch Products, alone or in conjunction with one another, and by advertising and promoting the use of the '193 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '193 Accused Products in an infringing manner.

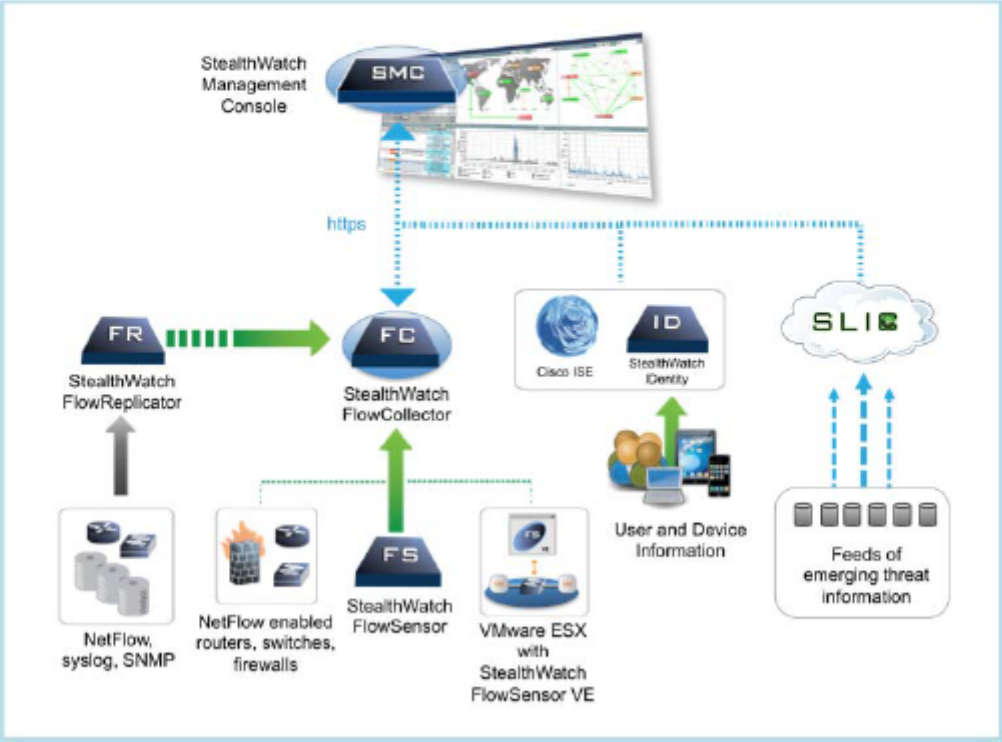
99. Cisco updates and maintains an HTTP site with Cisco's quick start guides, administration guides, user guides, operating instructions, blogs, white papers, data sheets and training certification programs which cover in depth aspects of operating Cisco's offerings. *See* https://www.cisco.com/c/en/us/support/switches/catalyst-9300-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 34; https://www.cisco.com/c/en/us/support/switches/catalyst-9400-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 35; https://www.cisco.com/c/en/us/support/switches/catalyst-9500-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 36; https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.pdf, attached hereto as Exhibit 16; *see also* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/datasheet-c78-739053.pdf, attached hereto as Exhibit 17; https://www.cisco.com/c/en/us/support/routers/index.html, attached hereto as Exhibit 37; *see also* https://www.cisco.com/c/dam/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/at-a-glance-c45-612993.pdf, attached hereto as Exhibit 18; *see also* https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-

routers-isr/datasheet-c78-732542.pdf, attached hereto as Exhibit 19; https://blogs.cisco.com/enterprise/cisco-traffic-analysis-encrypted-threat-analytics, attached hereto as Exhibit 38; https://communities.cisco.com/docs/DOC-76964, attached hereto as Exhibit 39; https://www.cisco.com/c/en/us/support/security/stealthwatch/tsd-products-support-series-home.html, attached hereto as Exhibit 40; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-guides-list.html, attached hereto as Exhibit 41; https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/hardware/installation/SW_6_9_1_Hardware_Installation_DV_1_2.pdf, attached hereto as Exhibit 42; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-and-configuration-guides-list.html, attached hereto as Exhibit 43; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-programming-reference-guides-list.html, attached hereto as Exhibit 44; https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-routing-switching.html, attached hereto as Exhibit 45.

100. These documents provide instructions, directions and/or require others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '193 Patent, where all the steps of the method claims are performed by either Cisco, its customers, purchasers, users or developers, or some combination thereof. For example, Cisco includes the Stealthwatch System Hardware Installation Guide, which provides instructions and recommendations on how to install and deploy the Accused '193 Products in an infringing manner as shown below.

Placement Considerations

As shown in the figure below, Stealthwatch system products can be strategically deployed to provide optimal coverage of key network segments throughout the network, whether in the internal network, at the perimeter, or in the DMZ.



Placing the SMC

As the management device, the Stealthwatch Management Console (SMC) should be installed at a location on your network that is accessible to all the devices sending data to it.

If you have a failover pair of SMCs, it is recommended that you install the primary SMC and the secondary SMC in separate physical locations. This strategy will enhance a disaster recovery effort should it become necessary.

Placing the Stealthwatch Flow Collector

As collection and monitoring devices, the Stealthwatch Flow Collector for NetFlow appliance and the Stealthwatch Flow Collector for sFlow appliance should be installed at a location on your network that is accessible to the NetFlow or sFlow devices sending the data to a Flow Collector, as well as any devices you plan to use to access the management interface.

Note: When you place a Flow Collector outside a firewall, Lancope recommends that you turn off the setting "Accept traffic from any exporter."

Placing the Stealthwatch Flow Sensor

As a passive monitoring device, the Stealthwatch Flow Sensor can sit at multiple points on your network to observe and record IP activity, thereby protecting network integrity and detecting security breaches. The Flow Sensor features integrated Web-based management systems that facilitate either centralized or remote management and administration.

The Flow Sensor appliance is most effective when placed at critical segments of your corporate network as follows:

- Inside your firewall to monitor traffic and determine if a firewall breach has occurred
- Outside your firewall, monitoring traffic flow to analyze who is threatening your firewall
- At sensitive segments of your network, offering protection from disgruntled employees or hackers with root access
- At remote office locations that constitute vulnerable network extensions
- On your business network for protocol use management (for example, on your transaction services subnet to determine if a hacker is running Telnet or FTP and compromising your customers' financial data)

Placing Other Stealthwatch Products

The only requirement for the placement of other Stealthwatch products, such as the Stealthwatch UDP Director (also known as FlowReplicator), or a VM server containing a Stealthwatch Flow Sensor Virtual Edition (VE), is that they have an unobstructed communication path to the rest of your Stealthwatch products as applicable.

Exhibit 42 at 11-12.

101. As such, Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the '193 Patent.

THIRD CAUSE OF ACTION
(Direct Infringement of the '176 Patent pursuant to 35 U.S.C. § 271(a))

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

103. Cisco has infringed and continues to infringe Claims 1-30 of the '176 Patent in violation of 35 U.S.C. § 271(a).

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

105. Cisco'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.

106. Cisco's infringement includes the manufacture, use, sale, importation and/or offer for sale of Cisco's products and services, including but not limited to the Accused Catalyst Products, the Accused Router Products, and the Accused Stealthwatch Products, alone or in conjunction with one another (collectively, the "Accused '176 Products").

107. The Accused '176 Products embody the patented invention of the '176 Patent and infringe the '176 Patent because they practice a method comprising:

identifying, by a computing system, a plurality of packets received by a network device from a host located in a first network;

generating, by the computing system, a plurality of log entries corresponding to the plurality of packets received by the network device;

identifying, by the computing system, a plurality of packets transmitted by the network

device to a host located in a second network;

generating, by the computing system, a plurality of log entries corresponding to the plurality of packets transmitted by the network device;

correlating, by the computing system and 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:

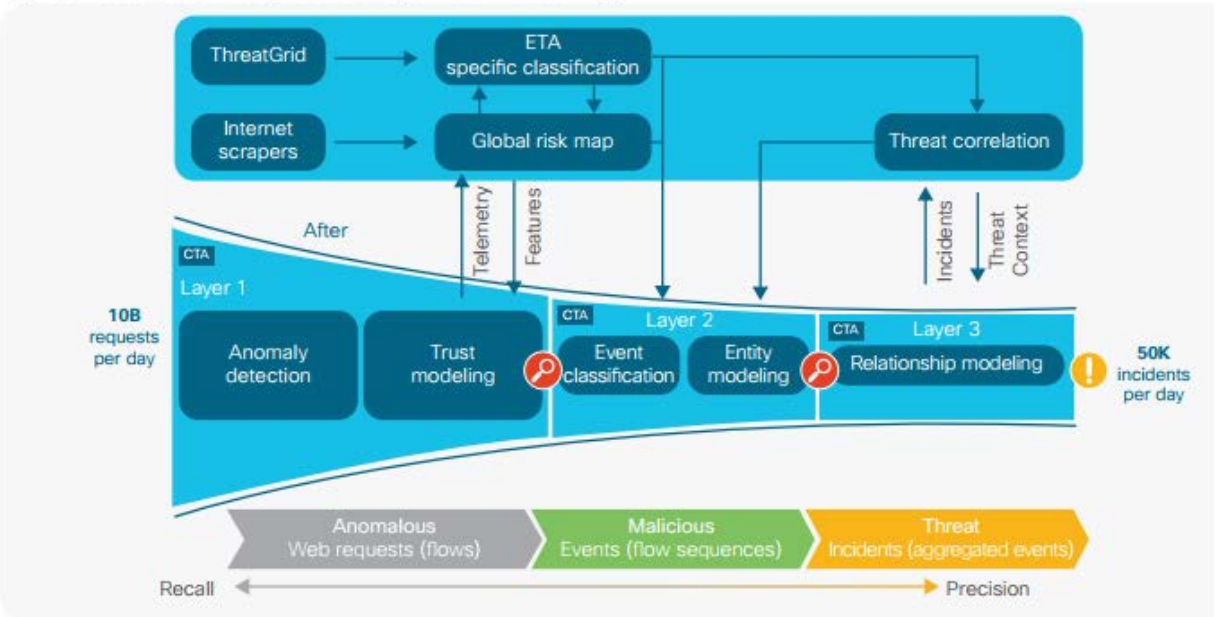
generating, by the computing system and based on the correlating, one or more rules configured to identify packets received from the host located in the first network; and

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

'176 Patent, Claim 1.

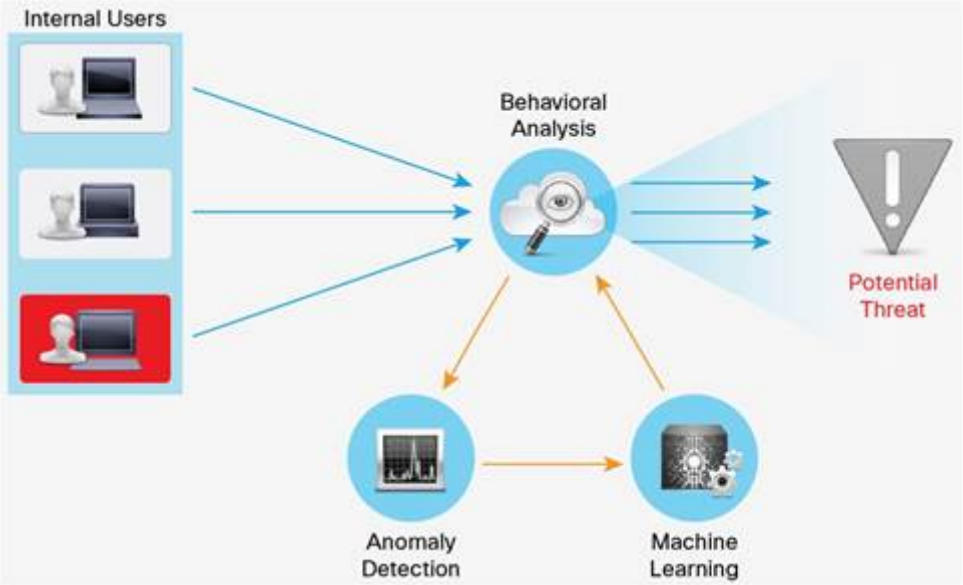
108. As shown below, the Accused '176 Products perform the step of "identifying, by a computing system, a plurality of packets received by a network device from a host located in a first network":

Figure 3. Stealtwatch Enterprise Multi-layer Machine Learning



(Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at 5.

109. The Accused '176 Products include Cognitive Threat Analytics ("CTA"). CTA "[a]nalyz[es] more than 10 billion web requests daily, [and] finds malicious activity that has bypassed security controls, or entered through unmonitored channels (including removable media), and is operating inside an organization's environment. Cognitive Threat Analytics is a cloud-based product that uses machine learning and statistical modeling of networks. It creates a baseline of the traffic in your network and identifies anomalies. It analyzes user and device behavior, and web traffic, to discover command-and-control communications, data exfiltration, and potentially unwanted applications operating in your infrastructure (Figure 1)."



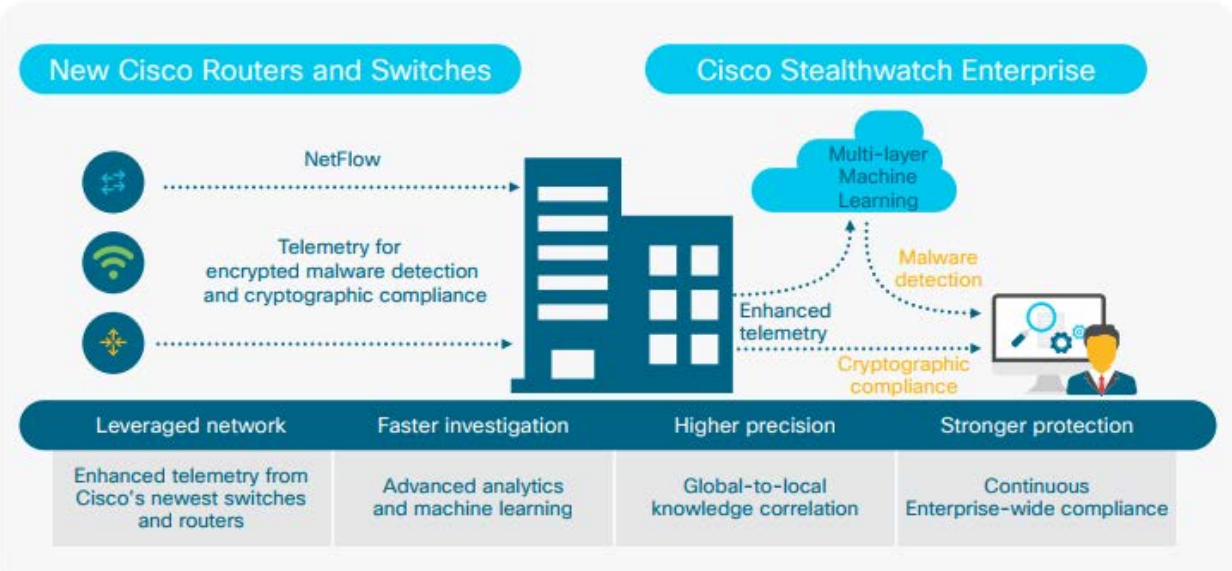
https://www.cisco.com/c/en/us/products/collateral/security/cognitive-threat-analytics/datasheet-c78-736557.html, attached hereto as Exhibit 29, at 1.

110. CTA "is integrated with Cisco AMP Threat Grid. When CTA independently detects command-and-control communication in the web channel, it queries the AMP Threat Grid database and correlates the indicators of compromise with the millions of malware

artifacts seen by AMP Threat Grid to identify the malware that caused the anomaly." *Id.* at 2. CTA also provides Automated Response and "integrates with existing security monitoring technologies, including Security Information and Event Management (SIEM) platforms. Organizations can integrate and automate their response with an established workflow." *Id.*

111. The Accused '176 Products perform the step of "generating, by the computing system, a plurality of log entries corresponding to the plurality of packets received by the network device; identifying, by the computing system, a plurality of packets transmitted by the network device to a host located in a second network," "generating, by the computing system, a plurality of log entries corresponding to the plurality of packets transmitted by the network device," and "correlating, by the computing system and 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." As shown below, the Accused '176 Products collect, store, and analyze both traditional flow data and intraflow metadata and "[o]btain contextual threat intelligence with real-time analysis correlated with user and device information." Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at 2-4.

Figure 2. Encrypted Traffic Analytics – technical solution overview



Id. at 3.

112. The Accused '176 Products perform the step of "responsive to correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device: generating, by the computing system and based on the correlating, one or more rules configured to identify packets received from the host located in the first network; and provisioning a packet-filtering device with the one or more rules configured to identify packets received from the host located in the first network." As shown below, the Accused '176 Products "[o]btain contextual threat intelligence with real-time analysis correlated with user and device information":

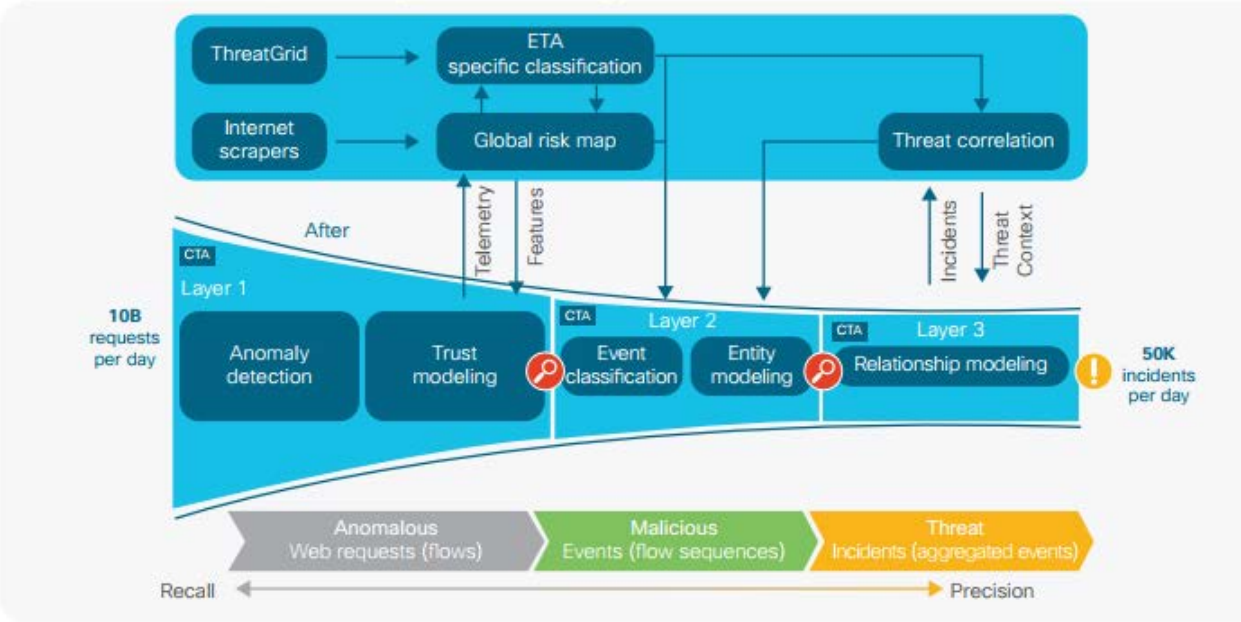
Table 2. Benefits of using Encrypted Traffic Analytics

Benefits
• Security visibility: Gain insight into threats in encrypted traffic using network analytics. Obtain contextual threat intelligence with real-time analysis correlated with user and device information.
• Cryptographic assessment: Ensure enterprise compliance with cryptographic protocols and visibility into and knowledge of what is being encrypted and what is not being encrypted on your network.
• Faster time to response: Quickly contain infected devices and users.
• Time and cost savings: Use the network as the foundation for the security posture, capitalizing on security investments in the network.

Id. at 4.

113. As shown below, the Accused '176 Products "correlate traffic with global threat behaviors to automatically identify infected hosts, command and control communication and suspicious traffic":

Figure 3. Stealtwatch Enterprise Multi-layer Machine Learning



Id. at 5.

114. The Accused '176 Products include "intraflow metadata, called *Encrypted Traffic Analytics* (ETA), is derived by using new data elements or telemetry that are independent of protocol details, such as the lengths and arrival times of packets within a flow. These data elements have the property of applying equally well to both encrypted and unencrypted flows. ETA focuses on identifying malware communications in encrypted traffic through passive monitoring, the extraction of relevant data elements, and supervised machine learning with cloud based global visibility. ETA extracts three main data elements: the initial data packet, the sequence of packet length and times, and TLS-specific features." (Encrypted Traffic Analytics Deployment Guide) CVD-Encrypted-Traffic-Analytics-Deployment-Guide-

2017DEC.pdf, attached hereto as Exhibit 33, at 1.

Appendix A: ETA Data Elements

Data Element Name	Description
Sequence of Packet Lengths and Times	An array of LENGTH values followed by an array of INTERARRIVAL TIME values describing the first N packets of a flow that carry application payload. Each LENGTH is encoded as a 16-bit integer to form a 20-byte array. Immediately following this, each INTERARRIVAL TIME is encoded as a 16-bit integer to form another 20-byte array.
Initial data packet	The content of the first packet of this flow that contains actual payload data, starting at the beginning of the IP header.
TLS records	An array of LENGTH values, followed by an array of INTERARRIVAL TIME values, followed by an array of CONTENT TYPE values, followed by an array of HANDSHAKE TYPE values. These arrays describe the first N records of a TLS flow.
TLS record lengths	A sequence of record lengths for up to the first N records of a TLS flow.
TLS record times	A sequence of TLS interarrival times for up to the first N records of a TLS flow.
TLS content types	A sequence of ContentType values for up to the first N records of a TLS flow.
TLS handshake types	A sequence of HandshakeType values for up to the first N records of a TLS flow.
TLS cipher suites	A list of up to N cipher suites offered by the client, or selected by the server in a TLS flow.
TLS extensions	An array of LENGTH values followed by an array of EXTENSION TYPE values describing the TLS extensions observed in the Hello message for a TLS flow.
TLS extension lengths	A list of extension lengths for up to the first N TLS extensions observed in the TLS Hello message for a flow.
TLS extension types	A list of extension types for up to the first N TLS extensions observed in the TLS Hello message for a flow.
TLS version	The TLS version number observed in the TLS Hello message for a flow.
TLS key length	The length of the client key observed in the TLS ClientKeyExchange message.
TLS session ID	The session ID value observed (if any) in the TLS Hello message for a flow.
TLS random	The random value observed in the TLS Hello message for this flow.

Id. at 60.

115. The Accused '176 Products "extract[] four main data elements: the sequence of packet lengths and times, the byte distribution, TLS-specific features and the initial data packet. Cisco's unique Application-Specific Integrated Circuit (ASIC) architecture provides the ability to extract these data elements without slowing down the data network," which includes the Initial Data Packet ("IDP"). (Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at 4.

"IDP is used to obtain packet data from the first packet of a flow. It allows extraction of interesting data such as an HTTP URL, DNS hostname/address and other data elements. The TLS handshake is composed of several messages that contain interesting, unencrypted metadata used to extract data elements such as cipher suites, TLS versions and the client's public key length." *Id.*

116. The Accused '176 Products use "NetFlow, proxy servers, endpoint telemetry, policy and access engines, traffic segmentation and more to establish baseline "normal" behavior for hosts and users across the enterprise. Stealthwatch can correlate traffic with global threat behaviors to automatically identify infected hosts, command and control communication and suspicious traffic. Stealthwatch maintains a global risk map – a very broad behavioral profile about servers on the Internet, identifying servers that are related to attacks, may be exploited, or may be used as a part of an attack in the future (Figure 3). This is not a blacklist, but a holistic picture from a security perspective. Stealthwatch analyzes the new encrypted traffic data elements in enhanced NetFlow by applying machine learning and statistical modeling. The global risk map and Encrypted Traffic Analytics data elements reinforce using advance security analytics. Rather than decrypting the traffic, Stealthwatch uses machine learning algorithms to pinpoint malicious patterns in encrypted traffic to help identify threats and improve incident response." *Id.* at 5.

117. As a result of Cisco'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.

118. Cisco's infringement of the '176 Patent has injured and continues to injure Centripetal in an amount to be proven at trial.

119. Cisco has willfully infringed each of the Asserted Patents. Centripetal is informed and believes that Cisco had knowledge of the Asserted Patents through various channels and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

120. On or around 2014, Centripetal partnered with ThreatGRID, a company which included threat intelligence technology which Centripetal integrated with their patented products that used some of the Asserted Patents. Cisco later acquired ThreatGRID in 2016. Centripetal is informed and believes that Cisco gained increased exposure to Centripetal's patented technology as a result of the acquisition of ThreatGRID. https://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/threatgrid.html, attached hereto as Exhibit 31.

121. Centripetal is further informed and believes that, on or around January 2016, Cisco requested an introduction to Centripetal through a third party, Granite Hill Capital Partners. Later, Centripetal received a point of contact introduction to Cisco from Granite Hill Capital Partners.

122. In 2016, Cisco invited Centripetal to participate in Cisco Live, which is Cisco's partner conference – in which Centripetal was asked to demonstrate its technology in Cisco's "Security Partner Village" booth. On or around June 2016, Centripetal attended the Cisco Live conference and demonstrated its patented technology, including the RuleGATE Threat Intelligence Gateway product which encompasses at least some of the Asserted Patents. Cisco currently lists Centripetal on its website located at www.cisco.com, as part of a "partner ecosystem" whose "[t]hreat intelligence platforms" use Threat Grid. https://www.cisco.com/c/en/us/products/security/threat-grid/integrations.html#~stickynav=2,

attached hereto as Exhibit 32, at 3.

123. Cisco thus knew or, in the alternative, was willfully blind to Centripetal's technology and its Asserted Patents. Cisco's infringement of the '176 Patent is egregious because despite this knowledge, Centripetal is informed and believes that Cisco deliberately copied Centripetal's patented technology, which it implemented into its products and services, such as Centripetal's CleanINTERNET service and Threat Intelligence Gateway, including the RuleGATE 2000. The blatant copying of Centripetal's patented technology and disregard for Centripetal's patent rights with an objectively high likelihood of infringement is egregious behavior warranting a finding of willful infringement and enhanced damages.

124. Centripetal is informed and believes that Cisco has undertaken no efforts to design these products or services around the '176 Patent to avoid infringement despite Cisco's knowledge and understanding that its products and services infringe the '176 Patent. As such, Cisco has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '176 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.

FOURTH CAUSE OF ACTION
(Indirect Infringement of the '176 Patent pursuant to 35 U.S.C. § 271(b))

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

126. Cisco has induced and continues to induce infringement of one or more claims of the '176 Patent under 35 U.S.C. § 271(b).

127. In addition to directly infringing the '176 Patent, Cisco indirectly infringes the '176 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others,

including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '176 Patent, where all the steps of the method claims are performed by either Cisco, its customers, purchasers, users or developers, or some combination thereof. Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the '176 Patent, including Claims 1-10.

128. Cisco knowingly and actively aided and abetted the direct infringement of the '176 Patent by instructing and encouraging its customers, purchasers, users and developers to use the '176 Accused Products. Such instructions and encouragement include, but are not limited to, advising third parties to use the '176 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '176 Patent, specifically through the use of the Accused Catalyst Products, the Accused Router Products, and the Accused Stealthwatch Products, alone or in conjunction with one another, and by advertising and promoting the use of the '176 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '176 Accused Products in an infringing manner.

129. Cisco updates and maintains an HTTP site with Cisco's quick start guides, administration guides, user guides, operating instructions, blogs, white papers, data sheets and training certification programs which cover in depth aspects of operating Cisco's offerings. *See* https://www.cisco.com/c/en/us/support/switches/catalyst-9300-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 34; https://www.cisco.com/c/en/us/support/switches/catalyst-9400-series-switches/tsd-products-

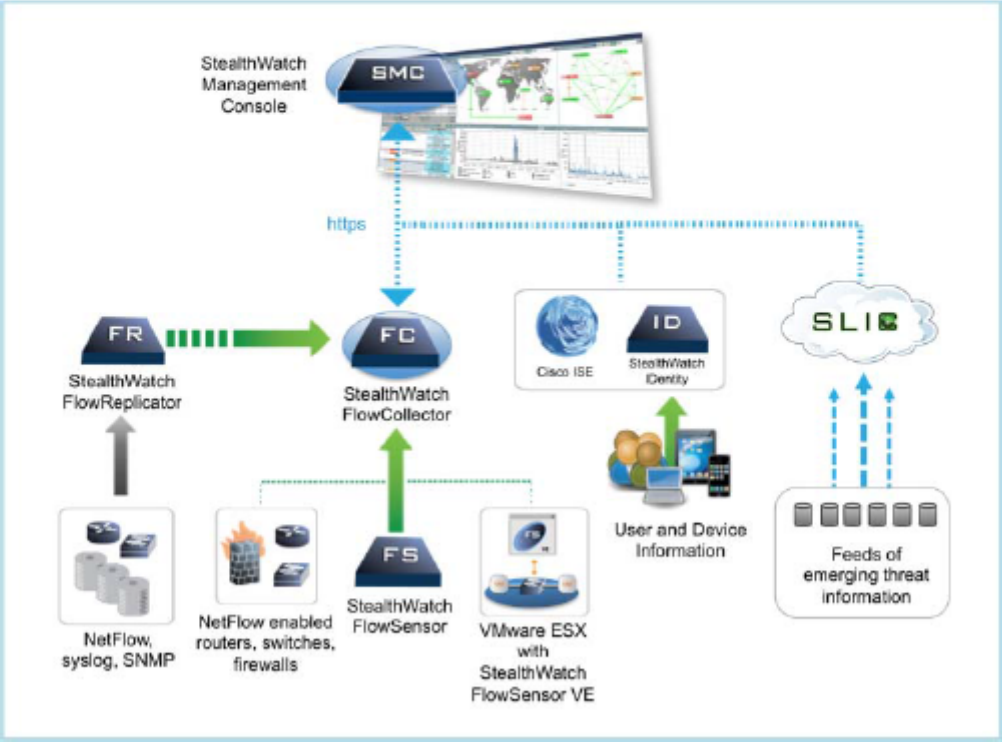
support-series-home.html, attached hereto as Exhibit 35; https://www.cisco.com/c/en/us/support/switches/catalyst-9500-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 36; https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.pdf, attached hereto as Exhibit 16; *see also* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/datasheet-c78-739053.pdf, attached hereto as Exhibit 17; https://www.cisco.com/c/en/us/support/routers/index.html, attached hereto as Exhibit 37; *see also* https://www.cisco.com/c/dam/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/at-a-glance-c45-612993.pdf, attached hereto as Exhibit 18; *see also* https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/datasheet-c78-732542.pdf, attached hereto as Exhibit 19; https://blogs.cisco.com/enterprise/cisco-traffic-analysis-encrypted-threat-analytics, attached hereto as Exhibit 38; https://communities.cisco.com/docs/DOC-76964, attached hereto as Exhibit 39; https://www.cisco.com/c/en/us/support/security/stealthwatch/tsd-products-support-series-home.html, attached hereto as Exhibit 40; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-guides-list.html, attached hereto as Exhibit 41; https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/hardware/installation/SW_6_9_1_Hardware_Installation_DV_1_2.pdf, attached hereto as Exhibit 42; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-and-configuration-guides-list.html, attached hereto as Exhibit 43; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-programming-reference-

guides-list.html, attached hereto as Exhibit 44; https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-routing-switching.html, attached hereto as Exhibit 45.

130. These documents provide instructions, directions and/or require others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '176 Patent, where all the steps of the method claims are performed by either Cisco, its customers, purchasers, users or developers, or some combination thereof. For example, Cisco includes the Stealthwatch System Hardware Installation Guide, which provides instructions and recommendations on how to install and deploy the Accused '176 Products in an infringing manner as shown below.

Placement Considerations

As shown in the figure below, Stealthwatch system products can be strategically deployed to provide optimal coverage of key network segments throughout the network, whether in the internal network, at the perimeter, or in the DMZ.



Placing the SMC

As the management device, the Stealthwatch Management Console (SMC) should be installed at a location on your network that is accessible to all the devices sending data to it.

If you have a failover pair of SMCs, it is recommended that you install the primary SMC and the secondary SMC in separate physical locations. This strategy will enhance a disaster recovery effort should it become necessary.

Placing the Stealthwatch Flow Collector

As collection and monitoring devices, the Stealthwatch Flow Collector for NetFlow appliance and the Stealthwatch Flow Collector for sFlow appliance should be installed at a location on your network that is accessible to the NetFlow or sFlow devices sending the data to a Flow Collector, as well as any devices you plan to use to access the management interface.

Note: When you place a Flow Collector outside a firewall, Lancope recommends that you turn off the setting "Accept traffic from any exporter."

Placing the Stealthwatch Flow Sensor

As a passive monitoring device, the Stealthwatch Flow Sensor can sit at multiple points on your network to observe and record IP activity, thereby protecting network integrity and detecting security breaches. The Flow Sensor features integrated Web-based management systems that facilitate either centralized or remote management and administration.

The Flow Sensor appliance is most effective when placed at critical segments of your corporate network as follows:

- Inside your firewall to monitor traffic and determine if a firewall breach has occurred
- Outside your firewall, monitoring traffic flow to analyze who is threatening your firewall
- At sensitive segments of your network, offering protection from disgruntled employees or hackers with root access
- At remote office locations that constitute vulnerable network extensions
- On your business network for protocol use management (for example, on your transaction services subnet to determine if a hacker is running Telnet or FTP and compromising your customers' financial data)

Placing Other Stealthwatch Products

The only requirement for the placement of other Stealthwatch products, such as the Stealthwatch UDP Director (also known as FlowReplicator), or a VM server containing a Stealthwatch Flow Sensor Virtual Edition (VE), is that they have an unobstructed communication path to the rest of your Stealthwatch products as applicable.

Exhibit 42 at 11-12.

131. As such, Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the '176 Patent.

FIFTH CAUSE OF ACTION
(Direct Infringement of the '077 Patent pursuant to 35 U.S.C. § 271(a))

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

133. Cisco has infringed and continues to infringe Claims 1-20 of the '077 Patent in violation of 35 U.S.C. § 271(a).

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

135. Cisco'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.

136. Cisco's infringement includes the manufacture, use, sale, importation and/or offer for sale of Cisco's products and services, including but not limited to the Accused Catalyst Products, the Accused Router Products, and the Accused Stealthwatch Products, alone or in conjunction with one another (collectively, the "Accused '077 Products").

137. The Accused '077 Products embody the patented invention of the '077 Patent and infringe the '077 Patent because they practice a method comprising:

provisioning, each device of a plurality of devices, with one or more rules generated based on a boundary of a network protected by the plurality of devices with one or more networks other than the network protected by the plurality of devices at which the device is configured to be located; and

configuring, each device of the plurality of devices, to:

receive packets via a communication interface that does not have a network-layer address;

responsive to a determination by the device that a portion of the packets received from or destined for a host located in the network protected by the plurality of devices corresponds to criteria specified by the one or more rules, drop the portion of the packets; and

modify a switching matrix of a local area network (LAN) switch associated with the device such that the LAN switch is configured to drop the portion of the packets responsive to the determination by the device.

'077 Patent, Claim 1.

138. As shown below, the Accused '077 Products perform the step of "provisioning, each device of a plurality of devices, with one or more rules generated based on a boundary of a network protected by the plurality of devices with one or more networks other than the network protected by the plurality of devices at which the device is configured to be located; and configuring, each device of the plurality of devices." As shown below, the Accused '077 Products include "policy-based automation from edge to cloud with foundational capabilities":

The Cisco® Digital Network Architecture (DNA) with Software Defined Access (SD-Access) is the network fabric that powers business. Cisco DNA is an open and extensible, software-driven architecture that accelerates and simplifies your enterprise network operations. The programmable architecture frees your IT staff from time consuming, repetitive network configuration tasks so they can focus instead on innovation that positively transforms your business. SD-Access enables policy-based automation from edge to cloud with foundational capabilities. These include:

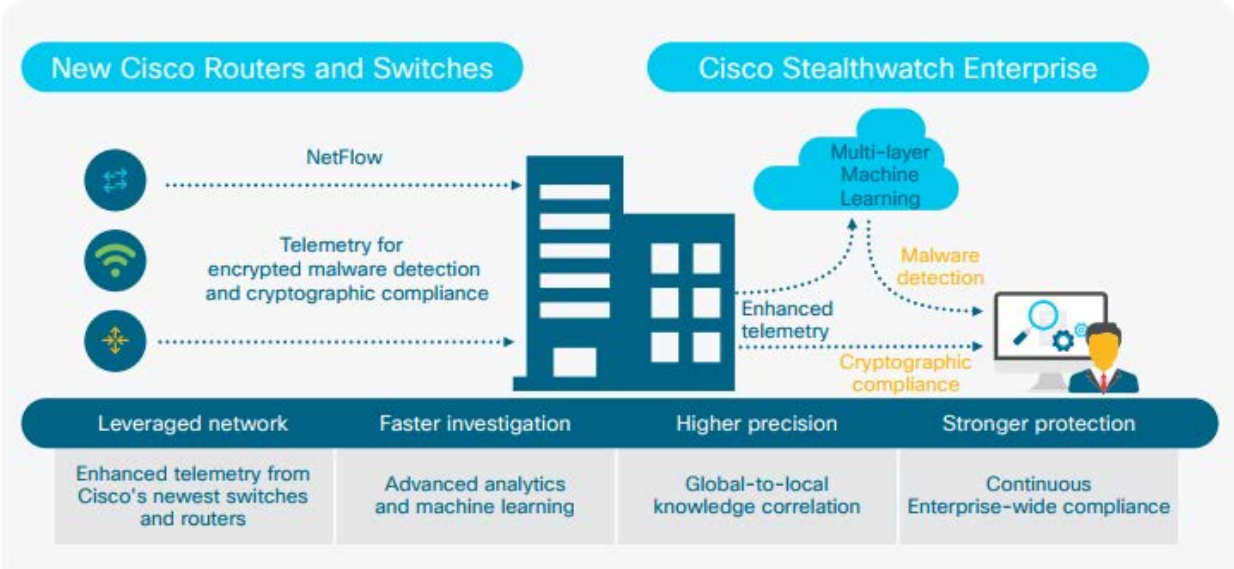
- Simplified device deployment
- Unified management of wired and wireless networks
- Network virtualization and segmentation
- Group-based policies
- Context-based analytics

(Cisco Catalyst Data Sheet). https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/datasheet-c78-739053.pdf, attached hereto as Exhibit 17, at 1.

139. The Accused '077 Products "receive packets via a communication interface that does not have a network-layer address." As shown below, the Accused '077 Products include

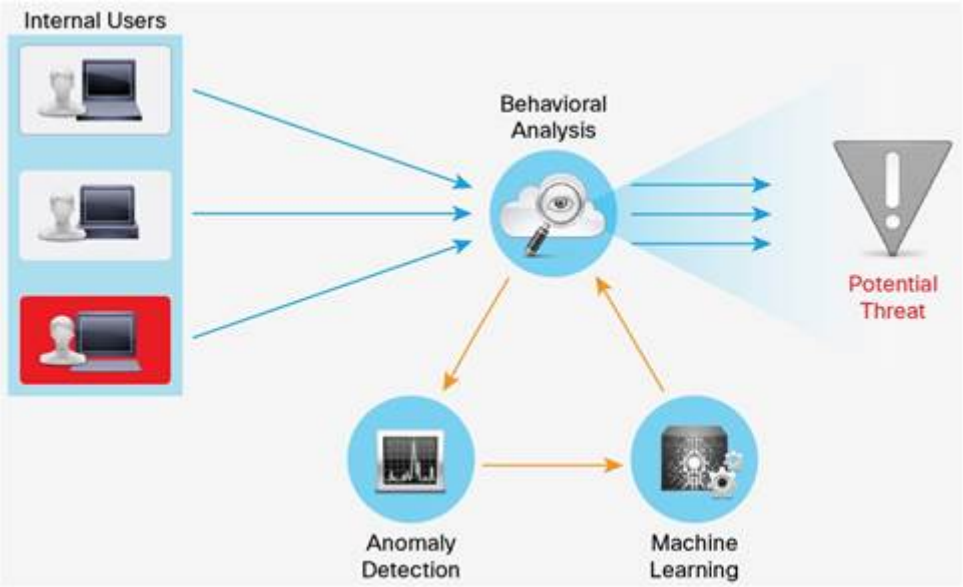
Multi-layer Machine Learning to receive packets at multiple OSI layers:

Figure 2. Encrypted Traffic Analytics – technical solution overview



(Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at 3.

140. The Accused '077 Products include Cognitive Threat Analytics ("CTA"). CTA "[a]nalyz[es] more than 10 billion web requests daily, [and] finds malicious activity that has bypassed security controls, or entered through unmonitored channels (including removable media), and is operating inside an organization's environment. Cognitive Threat Analytics is a cloud-based product that uses machine learning and statistical modeling of networks. It creates a baseline of the traffic in your network and identifies anomalies. It analyzes user and device behavior, and web traffic, to discover command-and-control communications, data exfiltration, and potentially unwanted applications operating in your infrastructure (Figure 1)."



https://www.cisco.com/c/en/us/products/collateral/security/cognitive-threat-analytics/datasheet-c78-736557.html, attached hereto as Exhibit 29, at 1.

141. CTA "is integrated with Cisco AMP Threat Grid. When CTA independently detects command-and-control communication in the web channel, it queries the AMP Threat Grid database and correlates the indicators of compromise with the millions of malware artifacts seen by AMP Threat Grid to identify the malware that caused the anomaly." *Id.* at 2. CTA also provides Automated Response and "integrates with existing security monitoring technologies, including Security Information and Event Management (SIEM) platforms. Organizations can integrate and automate their response with an established workflow." *Id.*

142. The Accused '077 Products, "responsive to a determination by the device that a portion of the packets received from or destined for a host located in the network protected by the plurality of devices corresponds to criteria specified by the one or more rules, drop the portion of the packets; and modify a switching matrix of a local area network (LAN) switch associated with the device such that the LAN switch is configured to drop the portion of the packets responsive to the determination by the device." As shown below, the Accused '077

Products "turns the network into an end-to-end sensor and enforcer that detects, contains and prevents emerging sophisticated security threats":

Conclusion

In summary, the network is now an even more advanced security sensor, capable of detecting threats in encrypted traffic. A Cisco Digital Network Architecture-ready infrastructure turns the network into an end-to-end sensor and enforcer that detects, contains and prevents emerging, sophisticated security threats.

(Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at 8.

143. As shown below, the Accused '077 Products include "policy-based automation from edge to cloud with foundational capabilities":

The Cisco® Digital Network Architecture (DNA) with Software Defined Access (SD-Access) is the network fabric that powers business. Cisco DNA is an open and extensible, software-driven architecture that accelerates and simplifies your enterprise network operations. The programmable architecture frees your IT staff from time consuming, repetitive network configuration tasks so they can focus instead on innovation that positively transforms your business. SD-Access enables policy-based automation from edge to cloud with foundational capabilities. These include:

- Simplified device deployment
- Unified management of wired and wireless networks
- Network virtualization and segmentation
- Group-based policies
- Context-based analytics

(Cisco Catalyst Data Sheet). https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/datasheet-c78-739053.pdf, attached hereto as Exhibit 17, at 1.

144. As a result of Cisco'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.

145. Cisco's infringement of the '077 Patent has injured and continues to injure Centripetal in an amount to be proven at trial.

146. Cisco has willfully infringed each of the Asserted Patents. Centripetal is

informed and believes that Cisco had knowledge of the Asserted Patents through various channels and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

147. On or around 2014, Centripetal partnered with ThreatGRID, a company which included threat intelligence technology which Centripetal integrated with their patented products that used some of the Asserted Patents. Cisco later acquired ThreatGRID in 2016. Centripetal is informed and believes that Cisco gained increased exposure to Centripetal's patented technology as a result of the acquisition of ThreatGRID. https://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/threatgrid.html, attached hereto as Exhibit 31.

148. Centripetal is further informed and believes that, on or around January 2016, Cisco requested an introduction to Centripetal through a third party, Granite Hill Capital Partners. Later, Centripetal received a point of contact introduction to Cisco from Granite Hill Capital Partners.

149. In 2016, Cisco invited Centripetal to participate in Cisco Live, which is Cisco's partner conference – in which Centripetal was asked to demonstrate its technology in Cisco's "Security Partner Village" booth. On or around June 2016, Centripetal attended the Cisco Live conference and demonstrated its patented technology, including the RuleGATE Threat Intelligence Gateway product which encompasses at least some of the Asserted Patents. Cisco currently lists Centripetal on its website located at www.cisco.com, as part of a "partner ecosystem" whose "[t]hreat intelligence platforms" use Threat Grid. https://www.cisco.com/c/en/us/products/security/threat-grid/integrations.html#~stickynav=2, attached hereto as Exhibit 32, at 3.

150. Cisco thus knew or, in the alternative, was willfully blind to Centripetal's technology and its Asserted Patents. Cisco's infringement of the '077 Patent is egregious because despite this knowledge, Centripetal is informed and believes that Cisco deliberately copied Centripetal's patented technology, which it implemented into its products and services, such as Centripetal's CleanINTERNET service and Threat Intelligence Gateway, including the RuleGATE 2000. The blatant copying of Centripetal's patented technology and disregard for Centripetal's patent rights with an objectively high likelihood of infringement is egregious behavior warranting a finding of willful infringement and enhanced damages.

151. Centripetal is informed and believes that Cisco has undertaken no efforts to design these products or services around the '077 Patent to avoid infringement despite Cisco's knowledge and understanding that its products and services infringe the '077 Patent. As such, Cisco has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '077 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.

SIXTH CAUSE OF ACTION
(Indirect Infringement of the '077 Patent pursuant to 35 U.S.C. § 271(b))

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

153. Cisco has induced and continues to induce infringement of one or more claims of the '077 Patent under 35 U.S.C. § 271(b).

154. In addition to directly infringing the '077 Patent, Cisco indirectly infringes the '077 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to perform one or more of the steps

of the method claims, either literally or under the doctrine of equivalents, of the '077 Patent, where all the steps of the method claims are performed by either Cisco, its customers, purchasers, users or developers, or some combination thereof. Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the '077 Patent, including Claims 1-6 and 19-20.

155. Cisco knowingly and actively aided and abetted the direct infringement of the '077 Patent by instructing and encouraging its customers, purchasers, users and developers to use the '077 Accused Products. Such instructions and encouragement include, but are not limited to, advising third parties to use the '077 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '077 Patent, specifically through the use of the Accused Catalyst Products, the Accused Router Products, and the Accused Stealthwatch Products, alone or in conjunction with one another, and by advertising and promoting the use of the '077 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '077 Accused Products in an infringing manner.

156. Cisco updates and maintains an HTTP site with Cisco's quick start guides, administration guides, user guides, operating instructions, blogs, white papers, data sheets and training certification programs which cover in depth aspects of operating Cisco's offerings. *See* https://www.cisco.com/c/en/us/support/switches/catalyst-9300-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 34; https://www.cisco.com/c/en/us/support/switches/catalyst-9400-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 35;

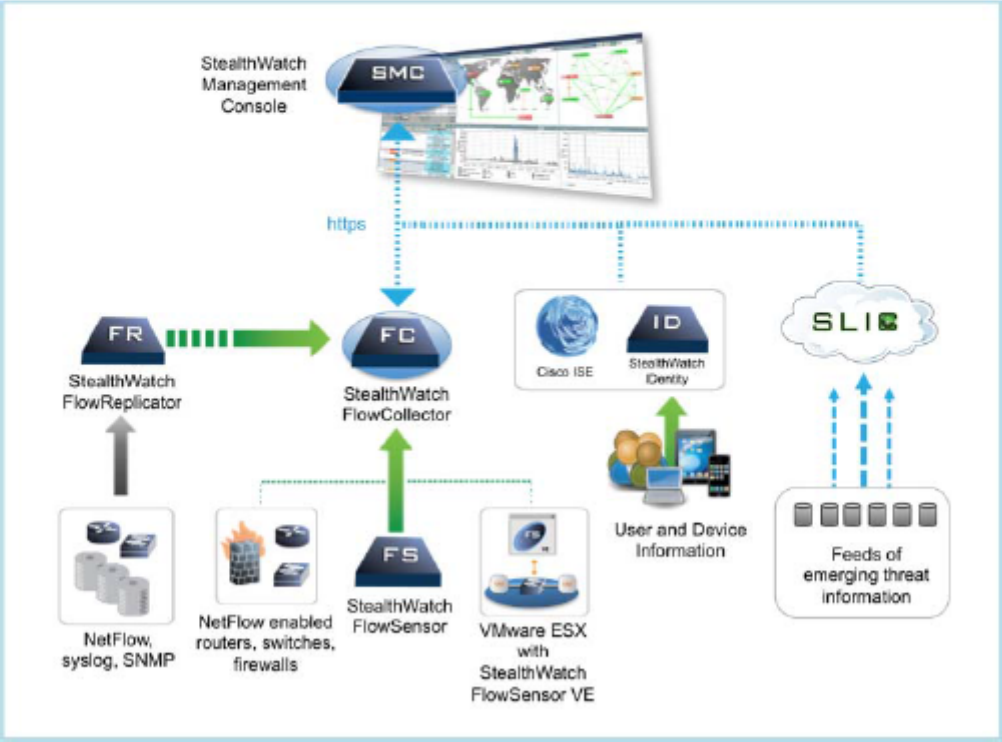
https://www.cisco.com/c/en/us/support/switches/catalyst-9500-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 36; https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.pdf, attached hereto as Exhibit 16; *see also* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/datasheet-c78-739053.pdf, attached hereto as Exhibit 17; https://www.cisco.com/c/en/us/support/routers/index.html, attached hereto as Exhibit 37; *see also* https://www.cisco.com/c/dam/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/at-a-glance-c45-612993.pdf, attached hereto as Exhibit 18; *see also* https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/datasheet-c78-732542.pdf, attached hereto as Exhibit 19; https://blogs.cisco.com/enterprise/cisco-traffic-analysis-encrypted-threat-analytics, attached hereto as Exhibit 38; https://communities.cisco.com/docs/DOC-76964, attached hereto as Exhibit 39; https://www.cisco.com/c/en/us/support/security/stealthwatch/tsd-products-support-series-home.html, attached hereto as Exhibit 40; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-guides-list.html, attached hereto as Exhibit 41; https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/hardware/installation/SW_6_9_1_Hardware_Installation_DV_1_2.pdf, attached hereto as Exhibit 42; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-and-configuration-guides-list.html, attached hereto as Exhibit 43; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-programming-reference-guides-list.html, attached hereto as Exhibit 44; https://www.cisco.com/c/en/us/training-

events/training-certifications/certifications/associate/ccna-routing-switching.html, attached hereto as Exhibit 45.

157. These documents provide instructions, directions and/or require others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '077 Patent, where all the steps of the method claims are performed by either Cisco, its customers, purchasers, users or developers, or some combination thereof. For example, Cisco includes the Stealthwatch System Hardware Installation Guide, which provides instructions and recommendations on how to install and deploy the Accused '077 Products in an infringing manner as shown below.

Placement Considerations

As shown in the figure below, Stealthwatch system products can be strategically deployed to provide optimal coverage of key network segments throughout the network, whether in the internal network, at the perimeter, or in the DMZ.



Placing the SMC

As the management device, the Stealthwatch Management Console (SMC) should be installed at a location on your network that is accessible to all the devices sending data to it.

If you have a failover pair of SMCs, it is recommended that you install the primary SMC and the secondary SMC in separate physical locations. This strategy will enhance a disaster recovery effort should it become necessary.

Placing the Stealthwatch Flow Collector

As collection and monitoring devices, the Stealthwatch Flow Collector for NetFlow appliance and the Stealthwatch Flow Collector for sFlow appliance should be installed at a location on your network that is accessible to the NetFlow or sFlow devices sending the data to a Flow Collector, as well as any devices you plan to use to access the management interface.

Note: When you place a Flow Collector outside a firewall, Lancope recommends that you turn off the setting "Accept traffic from any exporter."

Placing the Stealthwatch Flow Sensor

As a passive monitoring device, the Stealthwatch Flow Sensor can sit at multiple points on your network to observe and record IP activity, thereby protecting network integrity and detecting security breaches. The Flow Sensor features integrated Web-based management systems that facilitate either centralized or remote management and administration.

The Flow Sensor appliance is most effective when placed at critical segments of your corporate network as follows:

- Inside your firewall to monitor traffic and determine if a firewall breach has occurred
- Outside your firewall, monitoring traffic flow to analyze who is threatening your firewall
- At sensitive segments of your network, offering protection from disgruntled employees or hackers with root access
- At remote office locations that constitute vulnerable network extensions
- On your business network for protocol use management (for example, on your transaction services subnet to determine if a hacker is running Telnet or FTP and compromising your customers' financial data)

Placing Other Stealthwatch Products

The only requirement for the placement of other Stealthwatch products, such as the Stealthwatch UDP Director (also known as FlowReplicator), or a VM server containing a Stealthwatch Flow Sensor Virtual Edition (VE), is that they have an unobstructed communication path to the rest of your Stealthwatch products as applicable.

Exhibit 42 at 11-12.

158. As such, Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the '077 Patent.

SEVENTH CAUSE OF ACTION
(Direct Infringement of the '722 Patent pursuant to 35 U.S.C. § 271(a))

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

160. Cisco has infringed and continues to infringe Claims 1-20 of the '722 Patent in violation of 35 U.S.C. § 271(a).

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

162. Cisco'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.

163. Cisco's infringement includes the manufacture, use, sale, importation and/or offer for sale of Cisco's products and services, including but not limited to the Accused Catalyst Products and the Accused Router Products (collectively, the "Accused '722 Products").

164. The Accused '722 Products embody the patented invention of the '722 Patent and infringe the '722 Patent because they practice a method comprising:

> receiving, by a packet-filtering device, a plurality of packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators;
>
> receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet;
>
> responsive to a determination by the packet-filtering device that the first packet

satisfies one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more network-threat indicators of the plurality of network-threat indicators:

applying, by the packet-filtering device and to the first packet, an operator specified by the packet-filtering rule and configured to cause the packet-filtering device to allow the first packet to continue toward a destination of the first packet;

communicating, by the packet-filtering device, information from the packet-filtering rule that identifies the one or more network-threat indicators, and data indicative that the first packet was allowed to continue toward the destination of the first packet;

causing, by the packet-filtering device and 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;

receiving, by the packet-filtering device, an instruction generated in response to a user invoking an element in the at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators; and

responsive to receiving the instruction:

modifying, by the packet-filtering device, at least one operator specified by the packet-filtering rule to reconfigure the packet-filtering device to prevent packets corresponding to the one or more criteria from continuing toward their respective destinations; and

responsive to a determination by the packet-filtering device that the second packet corresponds to the one or more criteria:

preventing, by the packet-filtering device, the second packet from continuing toward a destination of the second packet;

communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet; and

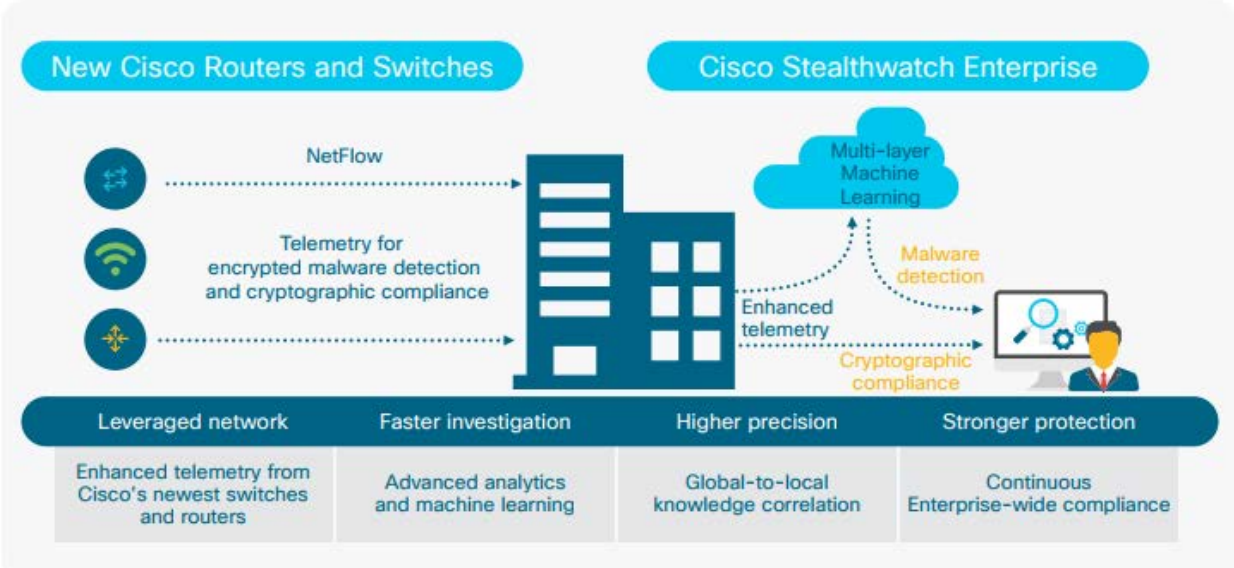
causing, by the packet-filtering device and in the interface, display of the data indicative that the second packet was prevented from continuing toward the destination of the second packet.

‘722 Patent, Claim 1.

165. The Accused ‘722 Products perform the steps of “receiving, by a packet-filtering device, a plurality of packet-filtering rules configured to cause the packet-filtering

device to identify packets corresponding to at least one of a plurality of network-threat indicators" and "receiving, by the packet-filtering device, a plurality of packets, wherein the plurality of packets comprises a first packet and a second packet." As shown below, the Accused '722 Products collect, store, and analyze both traditional flow data and intraflow metadata and "[o]btain contextual threat intelligence with real-time analysis correlated with user and device information." (Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf., attached hereto as Exhibit 25, at 2-4.

Figure 2. Encrypted Traffic Analytics – technical solution overview

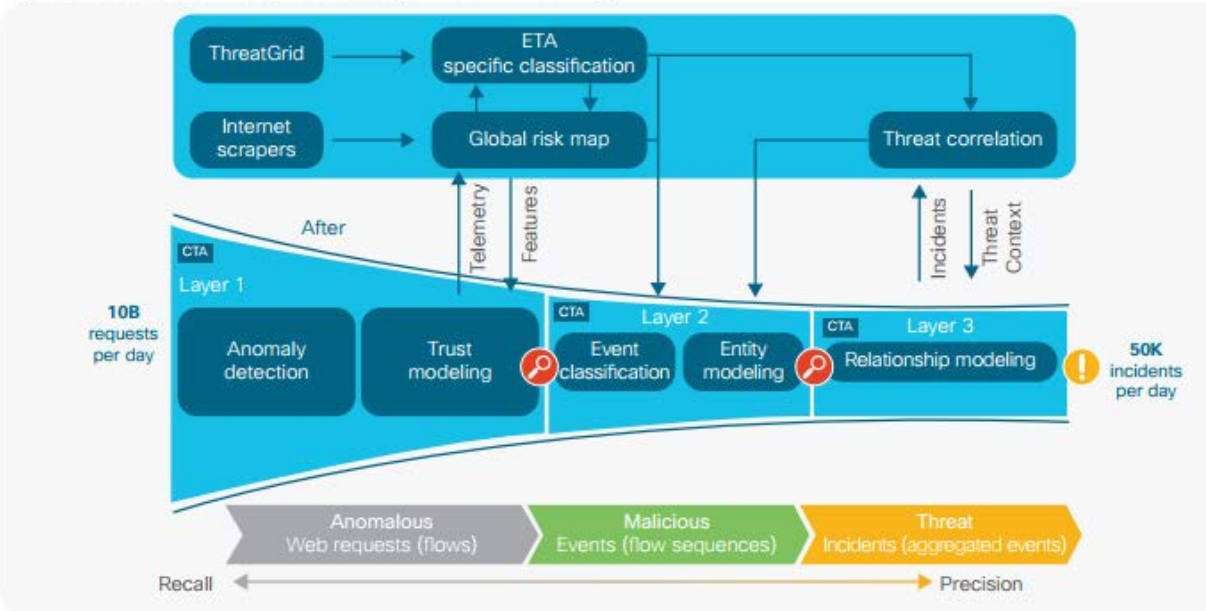


Id. at 3.

166. The Accused '722 Products perform the steps of "responsive to a determination by the packet-filtering device that the first packet satisfies one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more network-threat indicators of the plurality of network-threat indicators," "applying, by the packet-filtering device and to the first packet, an operator specified by the packet-filtering rule

and configured to cause the packet-filtering device to allow the first packet to continue toward a destination of the first packet," and "communicating, by the packet-filtering device, information from the packet-filtering rule that identifies the one or more network-threat indicators, and data indicative that the first packet was allowed to continue toward the destination of the first packet." As shown below, the Accused '722 Products "correlate traffic with global threat behaviors to automatically identify infected hosts, command and control communication and suspicious traffic":

Figure 3. Stealtwatch Enterprise Multi-layer Machine Learning



Id. at 5.

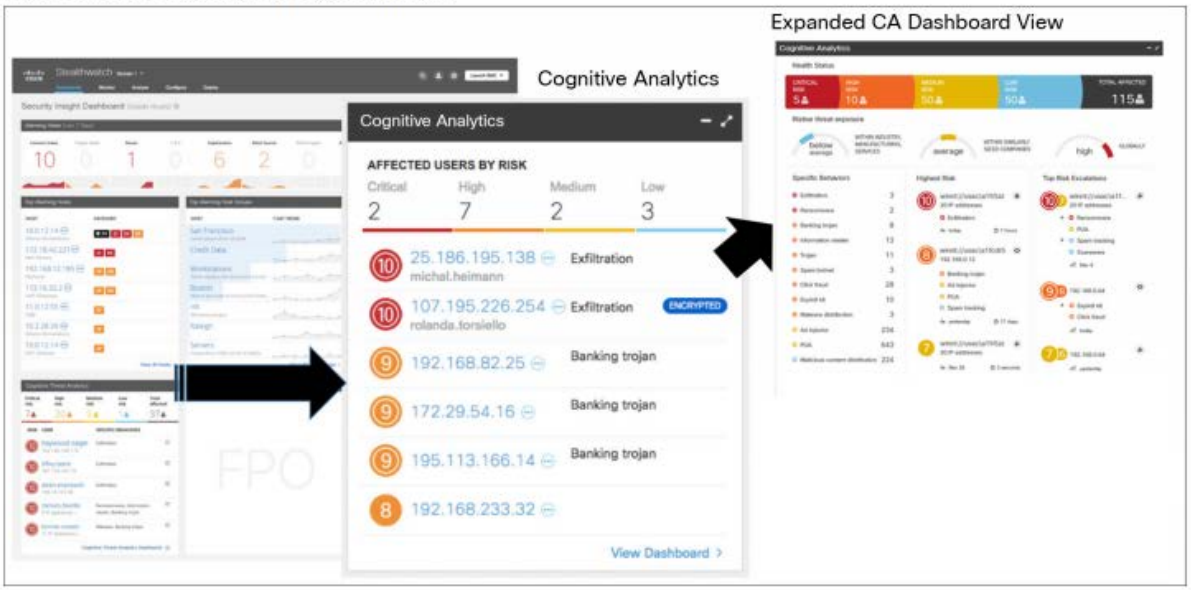
167. The Accused '722 Products use "NetFlow, proxy servers, endpoint telemetry, policy and access engines, traffic segmentation and more to establish baseline "normal" behavior for hosts and users across the enterprise. Stealthwatch can correlate traffic with global threat behaviors to automatically identify infected hosts, command and control communication and suspicious traffic. Stealthwatch maintains a global risk map – a very broad behavioral profile about servers on the Internet, identifying servers that are related to attacks, may be

exploited, or may be used as a part of an attack in the future (Figure 3). This is not a blacklist, but a holistic picture from a security perspective. Stealthwatch analyzes the new encrypted traffic data elements in enhanced NetFlow by applying machine learning and statistical modeling. The global risk map and Encrypted Traffic Analytics data elements reinforce using advance security analytics. Rather than decrypting the traffic, Stealthwatch uses machine learning algorithms to pinpoint malicious patterns in encrypted traffic to help identify threats and improve incident response." *Id*.

168. The Accused '722 Products perform the steps of "causing, by the packet-filtering device and 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" and "receiving, by the packet-filtering device, an instruction generated in response to a user invoking an element in the at least one portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators." As shown below, the Accused '722 Products' "Security Insight dashboard… provides a view of affected users identified by risk type. An expanded dashboard provides detailed information regarding the top risk escalations and relative threat exposure":

The Security Insight dashboard on the Stealthwatch Management Console (SMC) provides a view of affected users identified by risk type. An expanded dashboard provides detailed information regarding the top risk escalations and relative threat exposure. Table 3 lists some high-risk threats that use encrypted command and control communications.

Figure 4. Stealthwatch security insight dashboard



Id. at 7.

169. The Accused '722 Products perform the steps of "responsive to receiving the instruction: modifying, by the packet-filtering device, at least one operator specified by the packet-filtering rule to reconfigure the packet-filtering device to prevent packets corresponding to the one or more criteria from continuing toward their respective destinations" and "responsive to a determination by the packet-filtering device that the second packet corresponds to the one or more criteria: preventing, by the packet-filtering device, the second packet from continuing toward a destination of the second packet; communicating, by the packet-filtering device, data indicative that the second packet was prevented from continuing toward the destination of the second packet." As shown below, the Accused '722 Products "turns the network into an end-to-end sensor and enforcer that detects, contains and prevents emerging sophisticated security threats":

Conclusion

In summary, the network is now an even more advanced security sensor, capable of detecting threats in encrypted traffic. A Cisco Digital Network Architecture-ready infrastructure turns the network into an end-to-end sensor and enforcer that detects, contains and prevents emerging, sophisticated security threats.

Id. at 8.

170. "Upon discovery, a malicious encrypted flow can be blocked or quarantined by Stealthwatch. Policy-driven remediation actions via pxGrid using Cisco Identity Services Engine (ISE) with Cisco TrustSec® and Software-Defined Access (SD-Access) simplify and accelerate network security operations." *Id.* at 6.

171. As a result of Cisco'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.

172. Cisco's infringement of the '722 Patent has injured and continues to injure Centripetal in an amount to be proven at trial.

173. Cisco has willfully infringed each of the Asserted Patents. Centripetal is informed and believes that Cisco had knowledge of the Asserted Patents through various channels and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

174. On or around 2014, Centripetal partnered with ThreatGRID, a company which included threat intelligence technology which Centripetal integrated with their patented products that used some of the Asserted Patents. Cisco later acquired ThreatGRID in 2016. Centripetal is informed and believes that Cisco gained increased exposure to Centripetal's patented technology as a result of the acquisition of ThreatGRID. https://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/threatgrid.html, attached hereto as Exhibit 31.

175. Centripetal is further informed and believes that, on or around January 2016, Cisco requested an introduction to Centripetal through a third party, Granite Hill Capital Partners. Later, Centripetal received a point of contact introduction to Cisco from Granite Hill Capital Partners.

176. In 2016, Cisco invited Centripetal to participate in Cisco Live, which is Cisco's partner conference – in which Centripetal was asked to demonstrate its technology in Cisco's "Security Partner Village" booth. On or around June 2016, Centripetal attended the Cisco Live conference and demonstrated its patented technology, including the RuleGATE Threat Intelligence Gateway product which encompasses at least some of the Asserted Patents. Cisco currently lists Centripetal on its website located at www.cisco.com, as part of a "partner ecosystem" whose "[t]hreat intelligence platforms" use Threat Grid. https://www.cisco.com/c/en/us/products/security/threat-grid/integrations.html#~stickynav=2, attached hereto as Exhibit 32, at 3.

177. Cisco thus knew or, in the alternative, was willfully blind to Centripetal's technology and its Asserted Patents. Cisco's infringement of the '722 Patent is egregious because despite this knowledge, Centripetal is informed and believes that Cisco deliberately copied Centripetal's patented technology, which it implemented into its products and services, such as Centripetal's CleanINTERNET service and Threat Intelligence Gateway, including the RuleGATE 2000. The blatant copying of Centripetal's patented technology and disregard for Centripetal's patent rights with an objectively high likelihood of infringement is egregious behavior warranting a finding of willful infringement and enhanced damages.

178. Centripetal is informed and believes that Cisco has undertaken no efforts to design these products or services around the '722 Patent to avoid infringement despite Cisco's

knowledge and understanding that its products and services infringe the '722 Patent. As such, Cisco has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '722 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.

EIGHTH CAUSE OF ACTION
(Indirect Infringement of the '722 Patent pursuant to 35 U.S.C. § 271(b))

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

180. Cisco has induced and continues to induce infringement of one or more claims of the '722 Patent under 35 U.S.C. § 271(b).

181. In addition to directly infringing the '722 Patent, Cisco indirectly infringes the '722 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '722 Patent, where all the steps of the method claims are performed by either Cisco, its customers, purchasers, users or developers, or some combination thereof. Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the '722 Patent, including Claims 1-25.

182. Cisco knowingly and actively aided and abetted the direct infringement of the '722 Patent by instructing and encouraging its customers, purchasers, users and developers to use the '722 Accused Products. Such instructions and encouragement include, but are not limited to, advising third parties to use the '722 Accused Products in an infringing manner,

providing a mechanism through which third parties may infringe the '722 Patent, specifically through the use of the Accused Catalyst Products, the Accused Router Products, and the Accused Stealthwatch Products, alone or in conjunction with one another, and by advertising and promoting the use of the '722 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '722 Accused Products in an infringing manner.

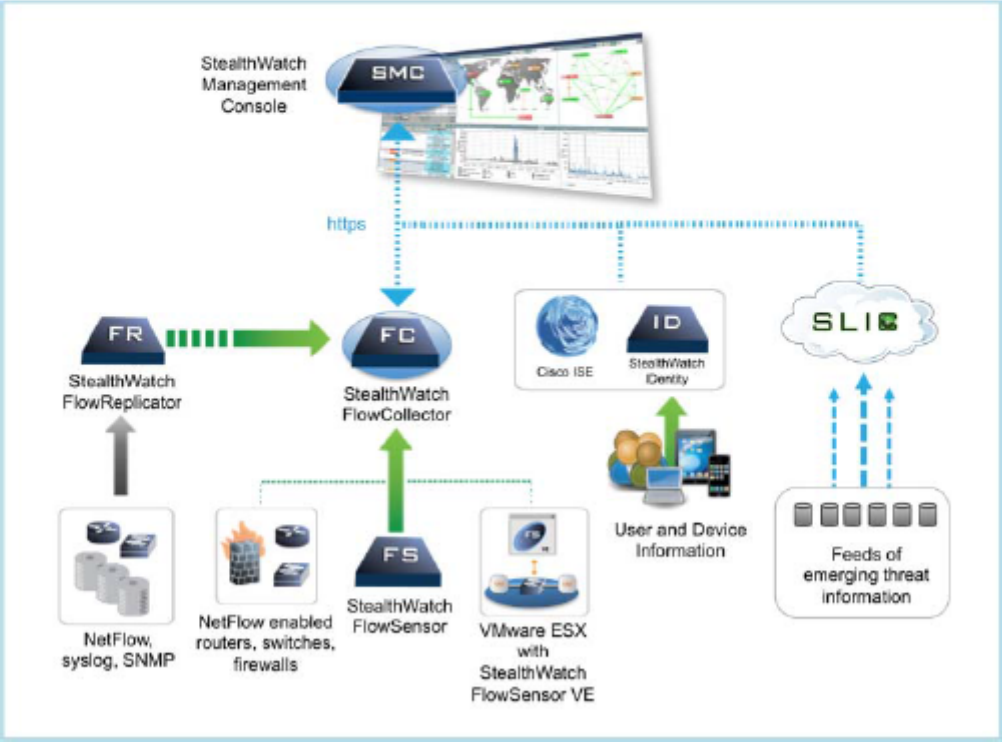
183. Cisco updates and maintains an HTTP site with Cisco's quick start guides, administration guides, user guides, operating instructions, blogs, white papers, data sheets and training certification programs which cover in depth aspects of operating Cisco's offerings. *See* https://www.cisco.com/c/en/us/support/switches/catalyst-9300-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 34; https://www.cisco.com/c/en/us/support/switches/catalyst-9400-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 35; https://www.cisco.com/c/en/us/support/switches/catalyst-9500-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 36; https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.pdf, attached hereto as Exhibit 16; *see also* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/datasheet-c78-739053.pdf, attached hereto as Exhibit 17; https://www.cisco.com/c/en/us/support/routers/index.html, attached hereto as Exhibit 37; *see also* https://www.cisco.com/c/dam/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/at-a-glance-c45-612993.pdf, attached hereto as Exhibit 18; *see also* https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-

routers-isr/datasheet-c78-732542.pdf, attached hereto as Exhibit 19; https://blogs.cisco.com/enterprise/cisco-traffic-analysis-encrypted-threat-analytics, attached hereto as Exhibit 38; https://communities.cisco.com/docs/DOC-76964, attached hereto as Exhibit 39; https://www.cisco.com/c/en/us/support/security/stealthwatch/tsd-products-support-series-home.html, attached hereto as Exhibit 40; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-guides-list.html, attached hereto as Exhibit 41; https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/hardware/installation/SW_6_9_1_Hardware_Installation_DV_1_2.pdf, attached hereto as Exhibit 42; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-and-configuration-guides-list.html, attached hereto as Exhibit 43; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-programming-reference-guides-list.html, attached hereto as Exhibit 44; https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-routing-switching.html, attached hereto as Exhibit 45.

184. These documents provide instructions, directions and/or require others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '722 Patent, where all the steps of the method claims are performed by either Cisco, its customers, purchasers, users or developers, or some combination thereof. For example, Cisco includes the Stealthwatch System Hardware Installation Guide, which provides instructions and recommendations on how to install and deploy the Accused '722 Products in an infringing manner as shown below.

Placement Considerations

As shown in the figure below, Stealthwatch system products can be strategically deployed to provide optimal coverage of key network segments throughout the network, whether in the internal network, at the perimeter, or in the DMZ.



Placing the SMC

As the management device, the Stealthwatch Management Console (SMC) should be installed at a location on your network that is accessible to all the devices sending data to it.

If you have a failover pair of SMCs, it is recommended that you install the primary SMC and the secondary SMC in separate physical locations. This strategy will enhance a disaster recovery effort should it become necessary.

Placing the Stealthwatch Flow Collector

As collection and monitoring devices, the Stealthwatch Flow Collector for NetFlow appliance and the Stealthwatch Flow Collector for sFlow appliance should be installed at a location on your network that is accessible to the NetFlow or sFlow devices sending the data to a Flow Collector, as well as any devices you plan to use to access the management interface.

Note: When you place a Flow Collector outside a firewall, Lancope recommends that you turn off the setting "Accept traffic from any exporter."

Placing the Stealthwatch Flow Sensor

As a passive monitoring device, the Stealthwatch Flow Sensor can sit at multiple points on your network to observe and record IP activity, thereby protecting network integrity and detecting security breaches. The Flow Sensor features integrated Web-based management systems that facilitate either centralized or remote management and administration.

The Flow Sensor appliance is most effective when placed at critical segments of your corporate network as follows:

- Inside your firewall to monitor traffic and determine if a firewall breach has occurred
- Outside your firewall, monitoring traffic flow to analyze who is threatening your firewall
- At sensitive segments of your network, offering protection from disgruntled employees or hackers with root access
- At remote office locations that constitute vulnerable network extensions
- On your business network for protocol use management (for example, on your transaction services subnet to determine if a hacker is running Telnet or FTP and compromising your customers' financial data)

Placing Other Stealthwatch Products

The only requirement for the placement of other Stealthwatch products, such as the Stealthwatch UDP Director (also known as FlowReplicator), or a VM server containing a Stealthwatch Flow Sensor Virtual Edition (VE), is that they have an unobstructed communication path to the rest of your Stealthwatch products as applicable.

Exhibit 42 at 11-12.

185. As such, Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the '722 Patent.

NINTH CAUSE OF ACTION
(Direct Infringement of the '806 Patent pursuant to 35 U.S.C. § 271(a))

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

187. Cisco has infringed and continues to infringe Claims 1-24 of the '806 Patent in violation of 35 U.S.C. § 271(a).

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

189. Cisco'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.

190. Cisco's infringement includes the manufacture, use, sale, importation and/or offer for sale of Cisco's products and services, including but not limited to the Accused Catalyst Products, the Accused Router Products, the Accused ASA Products, and the Accused Stealthwatch Products, alone or in conjunction with one another (collectively, the "Accused '806 Products").

191. The Accused '806 Products embody the patented invention of the '806 Patent and infringe the '806 Patent because they practice a method comprising:

receiving, by a network protection device, a first rule set and a second rule set;

preprocessing, by the network protection device, the first rule set and the second rule set to optimize performance of the network protection device for processing packets in accordance with at least one of the first rule set or the second rule set;

configuring at least two processors of the network protection device to process packets in accordance with the first rule set;

after the preprocessing and the configuring, receiving, by the network protection device, a plurality of packets;

processing, by the network protection device and in accordance with the first rule set, a portion of the plurality of packets;

signaling, each processor of the at least two processors, to process packets in accordance with the second rule set; and

configuring, each processor of the at least two processors, to responsive to the signaling to process packets in accordance with the second rule set:

cease processing of one or more packets;

cache the one or more packets;

reconfigure to process packets in accordance with the second rule set;

signal completion of reconfiguration to process packets in accordance with the second rule set; and

responsive to receiving signaling that each other processor of the at least two processors has completed reconfiguration to process packets in accordance with the second rule set, process, in accordance with the second rule set, the one or more packets.

'806 Patent, Claim 1.

192. The Accused '806 Products perform the steps of "receiving, by a network protection device, a first rule set and a second rule set; preprocessing, by the network protection device, the first rule set and the second rule set to optimize performance of the network protection device for processing packets in accordance with at least one of the first rule set or the second rule set; configuring at least two processors of the network protection device to process packets in accordance with the first rule set." As shown below, the Accused '806 Products "enables policy-based automation from edge to cloud with foundational capabilities," including "Simplified device deployment, Unified management of wired and

wireless networks, Network virtualization and segmentation, Group-based policies, and Context-based analytics."

The Foundation of Software-Defined Access

Advanced persistent security threats. The exponential growth of Internet of Things (IoT) devices. Mobility everywhere. Cloud adoption. All of these require a network fabric that integrates advanced hardware and software innovations to automate, secure, and simplify customer networks. The goal of this network fabric is to enable customer revenue growth by accelerating the rollout of business services.

The Cisco Digital Network Architecture (Cisco DNA™) with SD-Access is the network fabric that powers business. It is an open and extensible, software-driven architecture that accelerates and simplifies your enterprise network operations. The programmable architecture frees your IT staff from time-consuming, repetitive network configuration tasks so they can focus instead on innovation that positively transforms your business. SD-Access enables policy-based automation from edge to cloud with foundational capabilities. These include:

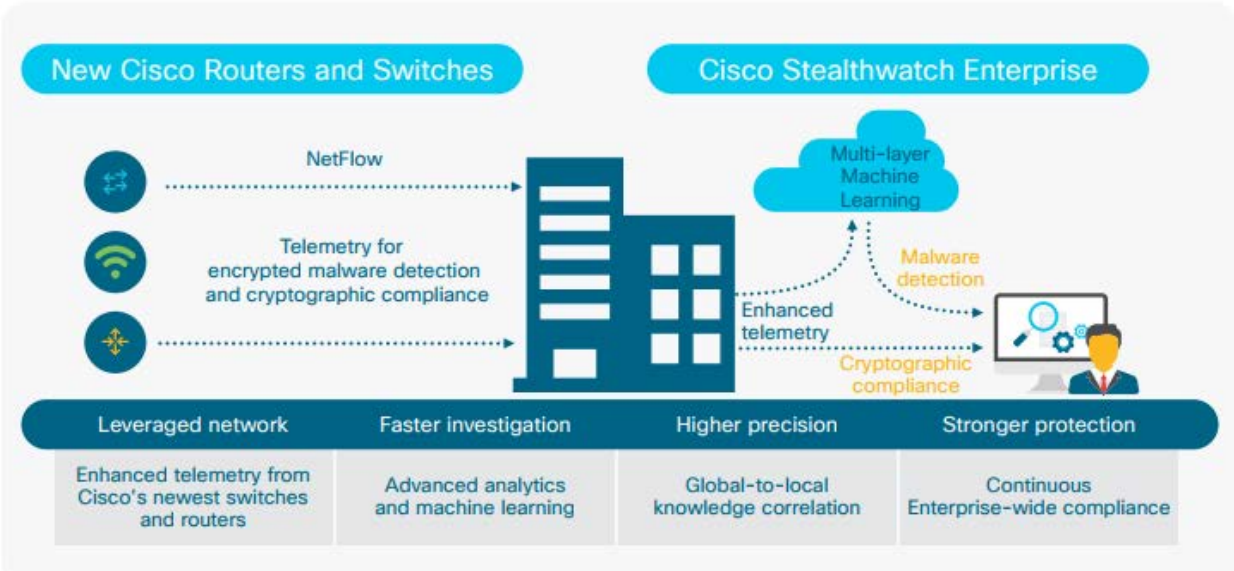
- Simplified device deployment
- Unified management of wired and wireless networks
- Network virtualization and segmentation
- Group-based policies
- Context-based analytics

(Cisco Catalyst 9300 Series Switches). https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.pdf, attached hereto as Exhibit 16, at 1.

193. The Accused '806 Products perform the steps of "after the preprocessing and the configuring, receiving, by the network protection device, a plurality of packets; processing, by the network protection device and in accordance with the first rule set, a portion of the plurality of packets; signaling, each processor of the at least two processors, to process packets in accordance with the second rule set." As shown below, the Accused '806 Products collect, store, and analyze both traditional flow data and intraflow metadata and "[o]btain contextual threat intelligence with real-time analysis correlated with user and device information." (Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at 2-

4.

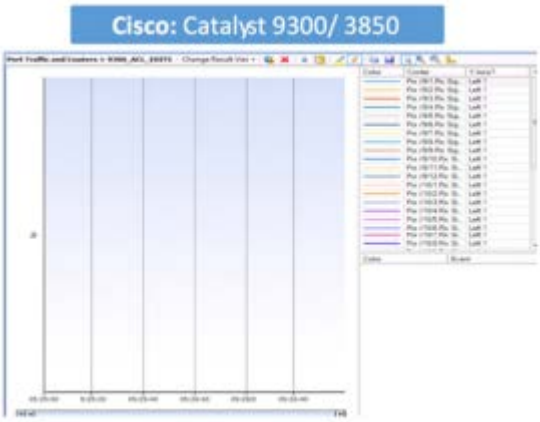
Figure 2. Encrypted Traffic Analytics – technical solution overview



Id. at 3.

194. The Accused '806 Products perform the steps of "configuring, each processor of the at least two processors, to responsive to the signaling to process packets in accordance with the second rule set: cease processing of one or more packets; cache the one or more packets; reconfigure to process packets in accordance with the second rule set; signal completion of reconfiguration to process packets in accordance with the second rule set; and responsive to receiving signaling that each other processor of the at least two processors has completed reconfiguration to process packets in accordance with the second rule set, process, in accordance with the second rule set, the one or more packets." As shown below, the Accused '806 Products "support high-speed policy edits (Adds/Deletes) with efficient resource allocation for scale, and secure implementation. With features such as 'ACL Label-Sharing' and 'Hitless ACL updates,' the switches demonstrated programming of policy to the network without being compromised. A table-stakes requirement for dynamic policy based automation." https://blogs.cisco.com/enterprise/wired-infrastructure-optimized-and-secure-

switching-resources, attached hereto as Exhibit 46, at 5.



(Miercom-Report-Cisco-vs-Huawei-Network-Architecture-DR170921G.pdf, attached hereto as Exhibit 23, at 22.

195. The Accused '806 Products support "UADP 2.0 Application-Specific Integrated Circuit (ASIC) with programmable pipeline and microengine capabilities, along with template-based, configurable allocation of Layer 2 and Layer 3 forwarding, Access Control Lists (ACLs), and Quality of Service (QoS) entries." https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.pdf, attached hereto as Exhibit 16, at 2.

196. The Accused '806 Products "are based on UADP 2.0 the second generation of UADP ASIC that comprises of 7.46 Billion transistors – one for every human being on this planet! In addition to programmability improvements of the ASIC pipeline, we have also introduced flexible tables on UADP 2.0 to enable universal deployments of the Catalyst 9000 Switches. UADP 2.0 turns Catalyst 9K into a Swiss Army Knife style Switch by customization of available table (SRAM/TCAM) resources based on customer deployment requirements. Cisco currently offers four fully tested templates to cover the all places in the network." https://communities.cisco.com/community/technology/enterprise_networks/blog/2017/06/20/ci

sco-catalyst-9000-series-of-switches-maximize-your-network-mileage, attached hereto as Exhibit 47 at 1.

197. The Accused '806 Products includes Transactional-Commit Modeling, which is "a new feature for rule updation" of ACL rules. With Transactional-Commit Modeling, "a rule update is applied after the rule compilation is completed; without affecting the rule matching performance. With the legacy model, rule updates take effect immediately but rule matching slows down during the rule compilation period. This feature is useful to prevent potential packet drops during large compilation of rules under high traffic conditions."

Transactional-Commit Model

The ASA rule-engine supports a new feature for rule updation called the Transactional-Commit Model. When this feature is enabled, a rule update is applied after the rule compilation is completed; without affecting the rule matching performance. With the legacy model, rule updates take effect immediately but rule matching slows down during the rule compilation period. This feature is useful to prevent potential packet drops during large compilation of rules under high traffic conditions. This feature is also useful to reduce the rule compilation time under two specific patterns of configurations:

- Preventing packet drops while compiling large rules during high traffic rates.
- Reducing rule compilation time while updating a large number of similar rules.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/firewall/asa_91_firewall_config/access_rules.html, attached hereto as Exhibit 30, at 6-4.

198. As a result of Cisco'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.

199. Cisco's infringement of the '806 Patent has injured and continues to injure Centripetal in an amount to be proven at trial.

200. Cisco has willfully infringed each of the Asserted Patents. Centripetal is informed and believes that Cisco had knowledge of the Asserted Patents through various channels and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

201. On or around 2014, Centripetal partnered with ThreatGRID, a company which included threat intelligence technology which Centripetal integrated with their patented

products that used some of the Asserted Patents. Cisco later acquired ThreatGRID in 2016. Centripetal is informed and believes that Cisco gained increased exposure to Centripetal's patented technology as a result of the acquisition of ThreatGRID. https://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/threatgrid.html, attached hereto as Exhibit 31.

202. Centripetal is further informed and believes that, on or around January 2016, Cisco requested an introduction to Centripetal through a third party, Granite Hill Capital Partners. Later, Centripetal received a point of contact introduction to Cisco from Granite Hill Capital Partners.

203. In 2016, Cisco invited Centripetal to participate in Cisco Live, which is Cisco's partner conference – in which Centripetal was asked to demonstrate its technology in Cisco's "Security Partner Village" booth. On or around June 2016, Centripetal attended the Cisco Live conference and demonstrated its patented technology, including the RuleGATE Threat Intelligence Gateway product which encompasses at least some of the Asserted Patents. Cisco currently lists Centripetal on its website located at www.cisco.com, as part of a "partner ecosystem" whose "[t]hreat intelligence platforms" use Threat Grid. https://www.cisco.com/c/en/us/products/security/threat-grid/integrations.html#~stickynav=2), attached hereto as Exhibit 32, at 3.

204. Cisco thus knew or, in the alternative, was willfully blind to Centripetal's technology and its Asserted Patents. Cisco's infringement of the '806 Patent is egregious because despite this knowledge, Centripetal is informed and believes that Cisco deliberately copied Centripetal's patented technology, which it implemented into its products and services, such as Centripetal's CleanINTERNET service and Threat Intelligence Gateway, including the

RuleGATE 2000. The blatant copying of Centripetal's patented technology and disregard for Centripetal's patent rights with an objectively high likelihood of infringement is egregious behavior warranting a finding of willful infringement and enhanced damages.

205. Centripetal is informed and believes that Cisco has undertaken no efforts to design these products or services around the '806 Patent to avoid infringement despite Cisco's knowledge and understanding that its products and services infringe the '806 Patent. As such, Cisco has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '806 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.

TENTH CAUSE OF ACTION
(Indirect Infringement of the '806 Patent pursuant to 35 U.S.C. § 271(b))

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

207. Cisco has induced and continues to induce infringement of one or more claims of the '806 Patent under 35 U.S.C. § 271(b).

208. In addition to directly infringing the '806 Patent, Cisco indirectly infringes the '806 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '806 Patent, where all the steps of the method claims are performed by either Cisco, its customers, purchasers, users or developers, or some combination thereof. Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or

more method claims of the '806 Patent, including Claims 1-8.

209. Cisco knowingly and actively aided and abetted the direct infringement of the '806 Patent by instructing and encouraging its customers, purchasers, users and developers to use the '806 Accused Products. Such instructions and encouragement include, but are not limited to, advising third parties to use the '806 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '806 Patent, specifically through the use of the Accused Catalyst Products, the Accused Router Products, and the Accused Stealthwatch Products, alone or in conjunction with one another, and by advertising and promoting the use of the '806 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '806 Accused Products in an infringing manner.

210. Cisco updates and maintains an HTTP site with Cisco's quick start guides, administration guides, user guides, operating instructions, blogs, white papers, data sheets and training certification programs which cover in depth aspects of operating Cisco's offerings. *See* https://www.cisco.com/c/en/us/support/switches/catalyst-9300-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 34; https://www.cisco.com/c/en/us/support/switches/catalyst-9400-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 35; https://www.cisco.com/c/en/us/support/switches/catalyst-9500-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 36; https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.pdf, attached hereto as Exhibit 16; *see also* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/datasheet-c78-739053.pdf, attached hereto as Exhibit 17;

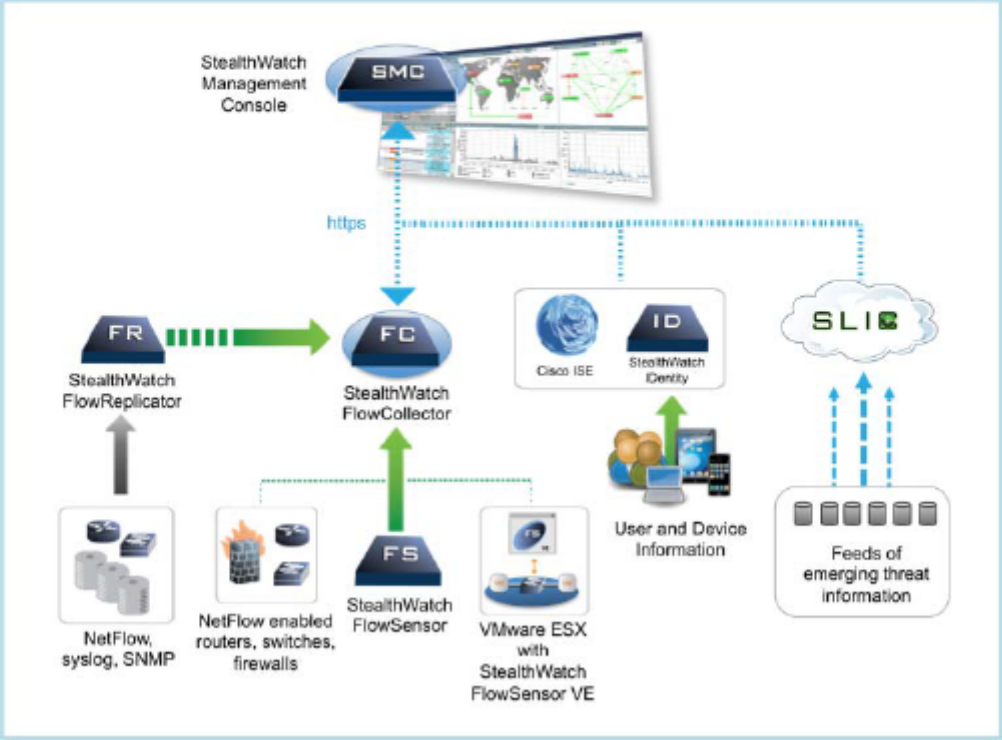
https://www.cisco.com/c/en/us/support/routers/index.html, attached hereto as Exhibit 37; *see also* https://www.cisco.com/c/dam/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/at-a-glance-c45-612993.pdf, attached hereto as Exhibit 18; *see also* https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/datasheet-c78-732542.pdf, attached hereto as Exhibit 19; https://blogs.cisco.com/enterprise/cisco-traffic-analysis-encrypted-threat-analytics, attached hereto as Exhibit 38; https://communities.cisco.com/docs/DOC-76964, attached hereto as Exhibit 39; https://www.cisco.com/c/en/us/support/security/stealthwatch/tsd-products-support-series-home.html, attached hereto as Exhibit 40; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-guides-list.html, attached hereto as Exhibit 41; https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/hardware/installation/SW_6_9_1_Hardware_Installation_DV_1_2.pdf, attached hereto as Exhibit 42; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-and-configuration-guides-list.html, attached hereto as Exhibit 43; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-programming-reference-guides-list.html, attached hereto as Exhibit 44; https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-routing-switching.html, attached hereto as Exhibit 45.

211. These documents provide instructions, directions and/or require others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the ‘806 Patent, where all the steps of the method claims are performed by either Cisco, its customers,

purchasers, users or developers, or some combination thereof. For example, Cisco includes the Stealthwatch System Hardware Installation Guide, which provides instructions and recommendations on how to install and deploy the Accused '806 Products in an infringing manner as shown below.

Placement Considerations

As shown in the figure below, Stealthwatch system products can be strategically deployed to provide optimal coverage of key network segments throughout the network, whether in the internal network, at the perimeter, or in the DMZ.



Placing the SMC

As the management device, the Stealthwatch Management Console (SMC) should be installed at a location on your network that is accessible to all the devices sending data to it.

If you have a failover pair of SMCs, it is recommended that you install the primary SMC and the secondary SMC in separate physical locations. This strategy will enhance a disaster recovery effort should it become necessary.

Placing the Stealthwatch Flow Collector

As collection and monitoring devices, the Stealthwatch Flow Collector for NetFlow appliance and the Stealthwatch Flow Collector for sFlow appliance should be installed at a location on your network that is accessible to the NetFlow or sFlow devices sending the data to a Flow Collector, as well as any devices you plan to use to access the management interface.

Note: When you place a Flow Collector outside a firewall, Lancope recommends that you turn off the setting "Accept traffic from any exporter."

Placing the Stealthwatch Flow Sensor

As a passive monitoring device, the Stealthwatch Flow Sensor can sit at multiple points on your network to observe and record IP activity, thereby protecting network integrity and detecting security breaches. The Flow Sensor features integrated Web-based management systems that facilitate either centralized or remote management and administration.

The Flow Sensor appliance is most effective when placed at critical segments of your corporate network as follows:

- Inside your firewall to monitor traffic and determine if a firewall breach has occurred
- Outside your firewall, monitoring traffic flow to analyze who is threatening your firewall
- At sensitive segments of your network, offering protection from disgruntled employees or hackers with root access
- At remote office locations that constitute vulnerable network extensions
- On your business network for protocol use management (for example, on your transaction services subnet to determine if a hacker is running Telnet or FTP and compromising your customers' financial data)

Placing Other Stealthwatch Products

The only requirement for the placement of other Stealthwatch products, such as the Stealthwatch UDP Director (also known as FlowReplicator), or a VM server containing a Stealthwatch Flow Sensor Virtual Edition (VE), is that they have an unobstructed communication path to the rest of your Stealthwatch products as applicable.

Exhibit 42 at 11-12.

212. As such, Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the '806 Patent.

ELEVENTH CAUSE OF ACTION
(Direct Infringement of the '713 Patent pursuant to 35 U.S.C. § 271(a))

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

214. Cisco has infringed and continues to infringe Claims 1-20 of the '713 Patent in violation of 35 U.S.C. § 271(a).

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

216. Cisco'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.

217. Cisco's infringement includes the manufacture, use, sale, importation and/or offer for sale of Cisco's products and services, including but not limited to the Accused Catalyst Products, the Accused Router Products, and the Accused Stealthwatch Products, alone or in conjunction with one another (collectively, the "Accused '713 Products").

218. The Accused '713 Products embody the patented invention of the '713 Patent and infringe the '713 Patent because they practice a method comprising:

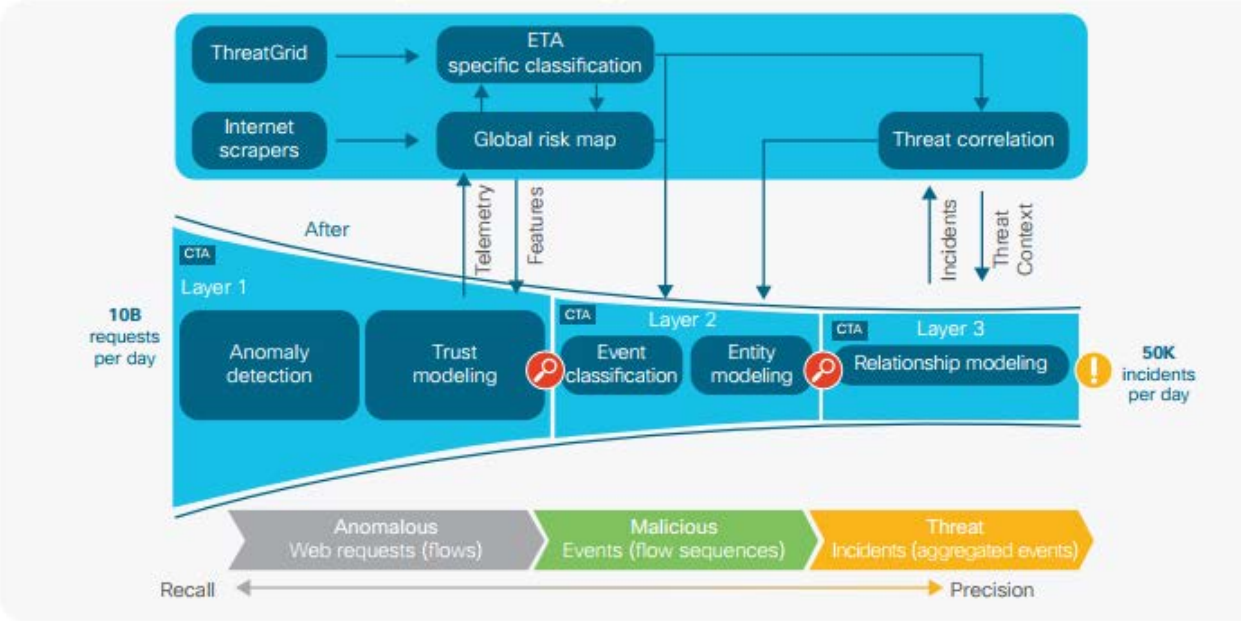
> receiving, by a computing system provisioned with a plurality of packet-filtering rules, a first packet and a second packet;
>
> responsive to a determination by the computing system that the first packet comprises data corresponding to a transport layer security (TLS)-version value for which one or more packet-filtering rules of the plurality of packet-filtering rules indicate packets should be forwarded toward their respective destinations, forwarding, by the computing system, the first packet toward its destination; and

responsive to a determination by the computing system that the second packet comprises data corresponding to a TLS-version value for which the one or more packet-filtering rules indicate packets should be blocked from continuing toward their respective destinations, dropping, by the computing system, the second packet.

'713 Patent, Claim 1.

219. The Accused '713 Products perform the steps of "receiving, by a computing system provisioned with a plurality of packet-filtering rules, a first packet and a second packet." As shown below, the Accused '713 Products "correlate traffic with global threat behaviors to automatically identify infected hosts, command and control communication and suspicious traffic":

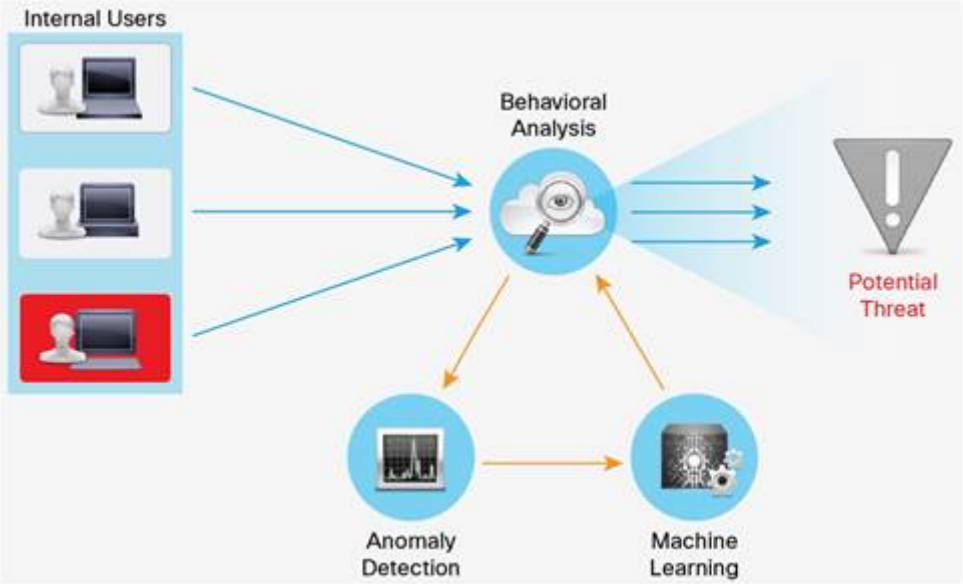
Figure 3. Stealtwatch Enterprise Multi-layer Machine Learning



(Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at 5.

220. The Accused '713 Products include Cognitive Threat Analytics ("CTA"). CTA "[a]nalyz[es] more than 10 billion web requests daily, [and] finds malicious activity that has bypassed security controls, or entered through unmonitored channels (including removable

media), and is operating inside an organization's environment. Cognitive Threat Analytics is a cloud-based product that uses machine learning and statistical modeling of networks. It creates a baseline of the traffic in your network and identifies anomalies. It analyzes user and device behavior, and web traffic, to discover command-and-control communications, data exfiltration, and potentially unwanted applications operating in your infrastructure (Figure 1)."



https://www.cisco.com/c/en/us/products/collateral/security/cognitive-threat-analytics/datasheet-c78-736557.html, attached hereto as Exhibit 29, at 1.

221. CTA "is integrated with Cisco AMP Threat Grid. When CTA independently detects command-and-control communication in the web channel, it queries the AMP Threat Grid database and correlates the indicators of compromise with the millions of malware artifacts seen by AMP Threat Grid to identify the malware that caused the anomaly." *Id.* at 2. CTA also provides Automated Response and "integrates with existing security monitoring technologies, including Security Information and Event Management (SIEM) platforms. Organizations can integrate and automate their response with an established workflow." *Id.*

222. The Accused '713 Products perform the steps of "responsive to a determination by the computing system that the first packet comprises data corresponding to a transport layer

security (TLS)-version value for which one or more packet-filtering rules of the plurality of packet-filtering rules indicate packets should be forwarded toward their respective destinations, forwarding, by the computing system, the first packet toward its destination." The Accused '713 Products "extract[] four main data elements: the sequence of packet lengths and times, the byte distribution, TLS-specific features and the initial data packet. Cisco's unique Application-Specific Integrated Circuit (ASIC) architecture provides the ability to extract these data elements without slowing down the data network," which includes the Initial Data Packet ("IDP"). (Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at 4. "IDP is used to obtain packet data from the first packet of a flow. It allows extraction of interesting data such as an HTTP URL, DNS hostname/address and other data elements. The TLS handshake is composed of several messages that contain interesting, unencrypted metadata used to extract data elements such as cipher suites, TLS versions and the client's public key length." *Id.*

Appendix A

Data Elements Extracted by Encrypted Traffic Analytics.

Data Element Name	Description
Sequence of Packet Lengths and Times (SPLT)	An array of LENGTH values followed by an array of INTERARRIVAL TIME values describing the first N packets of a flow that carry application payload. Each LENGTH is encoded as a 16-bit integer to form a 20-byte array. Immediately following this, each INTERARRIVAL TIME is encoded as a 16-bit integer to form another 20-byte array.
Byte distribution	A histogram giving the frequency of occurrence for each byte value or (range of values) in the first N bytes of application payload for a flow. Each "frequency of occurrence" is represented as a 16-bit integer.
Initial Data Packet (IDP)	The content of the first packet of this flow that contains actual payload data, starting at the beginning of the IP header.
TLS records	An array of LENGTH values, followed by an array of INTERARRIVAL TIME values, followed by an array of CONTENT TYPE values, followed by an array of HANDSHAKE TYPE values. These arrays describe the first N records of a TLS flow.
TLS record lengths	A sequence of record lengths for up to the first N records of a TLS flow.
TLS record times	A sequence of TLS interarrival times for up to the first N records of a TLS flow.
TLS content types	A sequence of ContentType values for up to the first N records of a TLS flow.
TLS handshake types	A sequence of HandshakeType values for up to the first N records of a TLS flow.
TLS cipher suites	A list of up to N cipher suites offered by the client, or selected by the server in a TLS flow.

Data Element Name	Description
TLS extensions	An array of LENGTH values followed by an array of EXTENSION TYPE values describing the TLS extensions observed in the Hello message for a TLS flow.
TLS extension lengths	A list of extension lengths for up to the first N TLS extensions observed in the TLS Hello message for a flow.
TLS extension types	A list of extension types for up to the first N TLS extensions observed in the TLS Hello message for a flow.
TLS version	The TLS version number observed in the TLS Hello message for a flow.
TLS key length	The length of the client key observed in the TLS ClientKeyExchange message.
TLS session ID	The session ID value observed (if any) in the TLS Hello message for a flow.
TLS random	The random value observed in the TLS Hello message for this flow.

Id. at 8-9.

223. The Accused '713 Products perform the steps of "responsive to a determination by the computing system that the second packet comprises data corresponding to a TLS-version value for which the one or more packet-filtering rules indicate packets should be blocked from continuing toward their respective destinations, dropping, by the computing system, the second packet." As shown below, the Accused '713 Products "turns the network into an end-to-end sensor and enforcer that detects, contains and prevents emerging sophisticated security threats":

Conclusion

In summary, the network is now an even more advanced security sensor, capable of detecting threats in encrypted traffic. A Cisco Digital Network Architecture-ready infrastructure turns the network into an end-to-end sensor and enforcer that detects, contains and prevents emerging, sophisticated security threats.

Id. at 8.

224. "Upon discovery, a malicious encrypted flow can be blocked or quarantined by Stealthwatch. Policy-driven remediation actions via pxGrid using Cisco Identity Services Engine (ISE) with Cisco TrustSec® and Software-Defined Access (SD-Access) simplify and accelerate network security operations." *Id.* at 6.

225. As a result of Cisco'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.

226. Cisco's infringement of the '713 Patent has injured and continues to injure Centripetal in an amount to be proven at trial.

227. Cisco has willfully infringed each of the Asserted Patents. Centripetal is informed and believes that Cisco had knowledge of the Asserted Patents through various channels and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

228. On or around 2014, Centripetal partnered with ThreatGRID, a company which included threat intelligence technology which Centripetal integrated with their patented products that used some of the Asserted Patents. Cisco later acquired ThreatGRID in 2016. Centripetal is informed and believes that Cisco gained increased exposure to Centripetal's patented technology as a result of the acquisition of ThreatGRID. https://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/threatgrid.html, attached hereto as Exhibit 31.

229. Centripetal is further informed and believes that, on or around January 2016, Cisco requested an introduction to Centripetal through a third party, Granite Hill Capital Partners. Later, Centripetal received a point of contact introduction to Cisco from Granite Hill Capital Partners.

230. In 2016, Cisco invited Centripetal to participate in Cisco Live, which is Cisco's partner conference – in which Centripetal was asked to demonstrate its technology in Cisco's "Security Partner Village" booth. On or around June 2016, Centripetal attended the Cisco Live conference and demonstrated its patented technology, including the RuleGATE Threat Intelligence Gateway product which encompasses at least some of the Asserted Patents. Cisco currently lists Centripetal on its website located at www.cisco.com, as part of a "partner ecosystem" whose "[t]hreat intelligence platforms" use Threat Grid. https://www.cisco.com/c/en/us/products/security/threat-grid/integrations.html#~stickynav=2, attached hereto as Exhibit 32, at 3.

231. Cisco thus knew or, in the alternative, was willfully blind to Centripetal's technology and its Asserted Patents. Cisco's infringement of the '713 Patent is egregious because despite this knowledge, Centripetal is informed and believes that Cisco deliberately

copied Centripetal's patented technology, which it implemented into its products and services, such as Centripetal's CleanINTERNET service and Threat Intelligence Gateway, including the RuleGATE 2000. The blatant copying of Centripetal's patented technology and disregard for Centripetal's patent rights with an objectively high likelihood of infringement is egregious behavior warranting a finding of willful infringement and enhanced damages.

232. Centripetal is informed and believes that Cisco has undertaken no efforts to design these products or services around the '713 Patent to avoid infringement despite Cisco's knowledge and understanding that its products and services infringe the '713 Patent. As such, Cisco has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '713 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.

TWELFTH CAUSE OF ACTION
(Indirect Infringement of the '713 Patent pursuant to 35 U.S.C. § 271(b))

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

234. Cisco has induced and continues to induce infringement of one or more claims of the '713 Patent under 35 U.S.C. § 271(b).

235. In addition to directly infringing the '713 Patent, Cisco indirectly infringes the '713 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '713 Patent, where all the steps of the method claims are performed by either Cisco, its customers, purchasers, users or developers, or some combination thereof. Cisco knew or was willfully

blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the '713 Patent, including Claims 1-7.

236. Cisco knowingly and actively aided and abetted the direct infringement of the '713 Patent by instructing and encouraging its customers, purchasers, users and developers to use the '713 Accused Products. Such instructions and encouragement include, but are not limited to, advising third parties to use the '713 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '713 Patent, specifically through the use of the Accused Catalyst Products, the Accused Router Products, and the Accused Stealthwatch Products, alone or in conjunction with one another, and by advertising and promoting the use of the '713 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '713 Accused Products in an infringing manner.

237. Cisco updates and maintains an HTTP site with Cisco's quick start guides, administration guides, user guides, operating instructions, blogs, white papers, data sheets and training certification programs which cover in depth aspects of operating Cisco's offerings. *See* https://www.cisco.com/c/en/us/support/switches/catalyst-9300-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 34; https://www.cisco.com/c/en/us/support/switches/catalyst-9400-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 35; https://www.cisco.com/c/en/us/support/switches/catalyst-9500-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 36; https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.pdf, attached hereto as Exhibit 16; *see also*

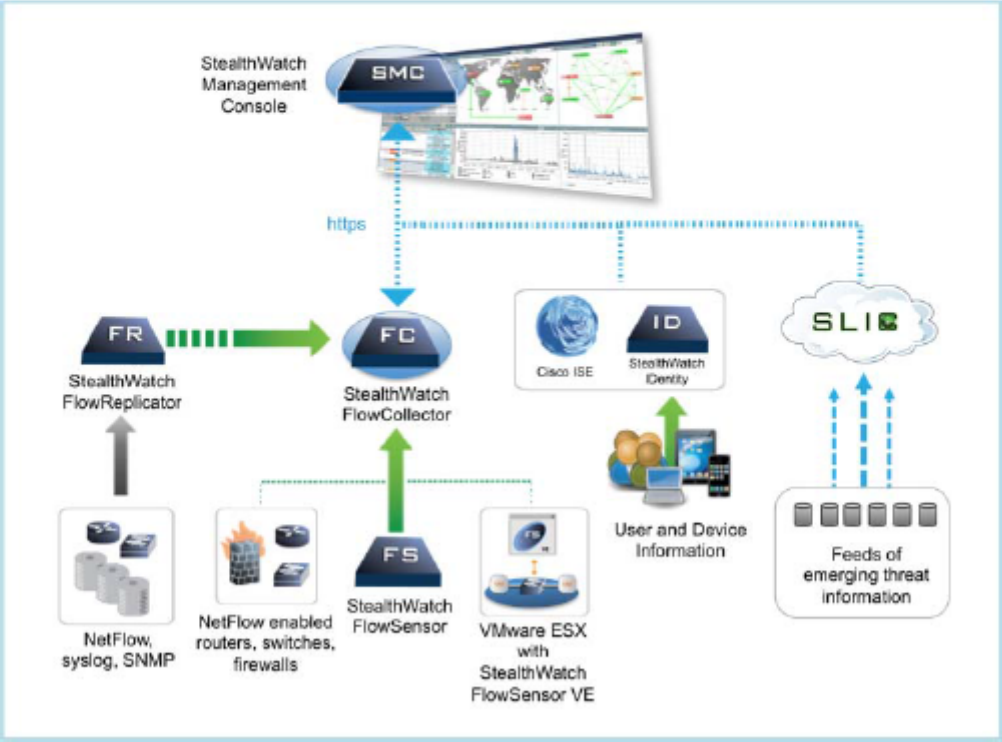
https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/datasheet-c78-739053.pdf, attached hereto as Exhibit 17; https://www.cisco.com/c/en/us/support/routers/index.html, attached hereto as Exhibit 37; *see also* https://www.cisco.com/c/dam/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/at-a-glance-c45-612993.pdf, attached hereto as Exhibit 18; *see also* https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/datasheet-c78-732542.pdf, attached hereto as Exhibit 19; https://blogs.cisco.com/enterprise/cisco-traffic-analysis-encrypted-threat-analytics, attached hereto as Exhibit 38; https://communities.cisco.com/docs/DOC-76964, attached hereto as Exhibit 39; https://www.cisco.com/c/en/us/support/security/stealthwatch/tsd-products-support-series-home.html, attached hereto as Exhibit 40; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-guides-list.html, attached hereto as Exhibit 41; https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/hardware/installation/SW_6_9_1_Hardware_Installation_DV_1_2.pdf, attached hereto as Exhibit 42; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-and-configuration-guides-list.html, attached hereto as Exhibit 43; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-programming-reference-guides-list.html, attached hereto as Exhibit 44; https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-routing-switching.html, attached hereto as Exhibit 45.

238. These documents provide instructions, directions and/or require others, including its customers, purchasers, users, and developers, to perform one or more of the steps

of the method claims, either literally or under the doctrine of equivalents, of the '713 Patent, where all the steps of the method claims are performed by either Cisco, its customers, purchasers, users or developers, or some combination thereof. For example, Cisco includes the Stealthwatch System Hardware Installation Guide, which provides instructions and recommendations on how to install and deploy the Accused '713 Products in an infringing manner as shown below.

Placement Considerations

As shown in the figure below, Stealthwatch system products can be strategically deployed to provide optimal coverage of key network segments throughout the network, whether in the internal network, at the perimeter, or in the DMZ.



Placing the SMC

As the management device, the Stealthwatch Management Console (SMC) should be installed at a location on your network that is accessible to all the devices sending data to it.

If you have a failover pair of SMCs, it is recommended that you install the primary SMC and the secondary SMC in separate physical locations. This strategy will enhance a disaster recovery effort should it become necessary.

Placing the Stealthwatch Flow Collector

As collection and monitoring devices, the Stealthwatch Flow Collector for NetFlow appliance and the Stealthwatch Flow Collector for sFlow appliance should be installed at a location on your network that is accessible to the NetFlow or sFlow devices sending the data to a Flow Collector, as well as any devices you plan to use to access the management interface.

Note: When you place a Flow Collector outside a firewall, Lancope recommends that you turn off the setting "Accept traffic from any exporter."

Placing the Stealthwatch Flow Sensor

As a passive monitoring device, the Stealthwatch Flow Sensor can sit at multiple points on your network to observe and record IP activity, thereby protecting network integrity and detecting security breaches. The Flow Sensor features integrated Web-based management systems that facilitate either centralized or remote management and administration.

The Flow Sensor appliance is most effective when placed at critical segments of your corporate network as follows:

- Inside your firewall to monitor traffic and determine if a firewall breach has occurred
- Outside your firewall, monitoring traffic flow to analyze who is threatening your firewall
- At sensitive segments of your network, offering protection from disgruntled employees or hackers with root access
- At remote office locations that constitute vulnerable network extensions
- On your business network for protocol use management (for example, on your transaction services subnet to determine if a hacker is running Telnet or FTP and compromising your customers' financial data)

Placing Other Stealthwatch Products

The only requirement for the placement of other Stealthwatch products, such as the Stealthwatch UDP Director (also known as FlowReplicator), or a VM server containing a Stealthwatch Flow Sensor Virtual Edition (VE), is that they have an unobstructed communication path to the rest of your Stealthwatch products as applicable.

Exhibit 42 at 11-12.

239. As such, Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the '713 Patent.

THIRTEENTH CAUSE OF ACTION
(Direct Infringement of the '552 Patent pursuant to 35 U.S.C. § 271(a))

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

241. Cisco has infringed and continues to infringe Claims 1-21 of the '552 Patent in violation of 35 U.S.C. § 271(a).

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

243. Cisco'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.

244. Cisco's infringement includes the manufacture, use, sale, importation and/or offer for sale of Cisco's products and services, including but not limited to the Accused Catalyst Products, the Accused Router Products, and the Accused Stealthwatch Products, alone or in conjunction with one another (collectively, the "Accused '552 Products").

245. The Accused '552 Products embody the patented invention of the '552 Patent and infringe the '552 Patent because they practice a method comprising:

at a computing device comprising at least one processor, a memory, and a communication interface:

receiving, via the communication interface, a plurality of hypertext transfer protocol secure (HTTPS) packets;

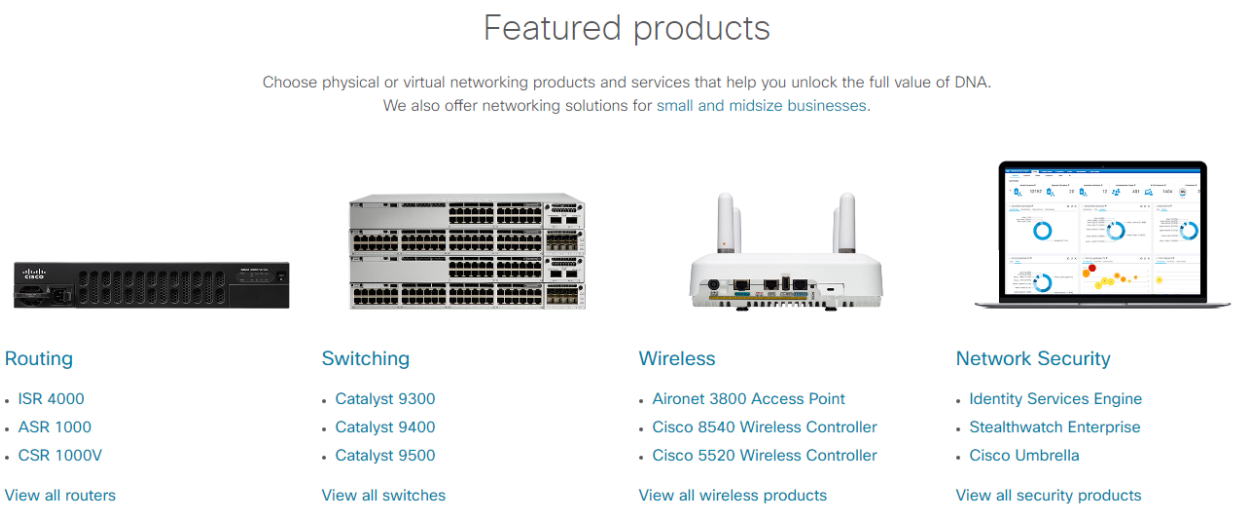
responsive to a determination by the at least one processor that at least a portion of the plurality of HTTPS packets have packet-header-field values corresponding to a

packet filtering rule stored in the memory, applying, by the at least one processor, an operator specified by the packet-filtering rule to the at least a portion of the plurality of HTTPS packets, wherein the operator specifies one or more application-header-field-value criteria identifying one or more transport layer security (TLS)-version values for which packets should be blocked from continuing toward their respective destinations; and

responsive to a determination by the at least one processor that one or more packets, of the at least a portion of the plurality of HTTPS packets, have one or more application-header-field values corresponding to one or more TLS-version values of the one or more TLS-version values for which packets should be blocked from continuing toward their respective destinations, applying, by the at least one processor, at least one packet-transformation function specified by the operator to the one or more packets to block each packet of the one or more packets from continuing toward its respective destination.

'552 Patent, Claim 1.

246. The Accused '552 Products are computing devices which perform the steps of the method of the '552 Patent. As shown below, the Accused '552 Products include "a computing device comprising at least one processor, a memory, and a communication interface."



(Cisco Featured Products). https://www.cisco.com/c/en/us/solutions/enterprise-networks/index.html#~stickynav=1, attached hereto as Exhibit 48.

247. As shown below, the Accused '552 Products include "Intel® x86 CPU complex

with 8-GB memory, and 16 GB of flash and external USB 3.0 SSD pluggable storage slot to host containers,"

Product Overview: Features

Product Highlights

- Highest wireless scale with Wave 2 access points supported on a single switch with select models
- UADP 2.0 Application-Specific Integrated Circuit (ASIC) with programmable pipeline and microengine capabilities, along with template-based, configurable allocation of Layer 2 and Layer 3 forwarding, Access Control Lists (ACLs), and Quality of Service (QoS) entries
- Intel® x86 CPU complex with 8-GB memory, and 16 GB of flash and external USB 3.0 SSD pluggable storage slot to host containers
- USB 2.0 slot to load system images and set configurations
- Up to 480 Gbps of local stackable switching bandwidth
- Flexible and dense uplink offerings with 1G, Multigigabit, 10G, and 40G, with platform readiness for 25G
- Flexible downlink options with 1G and Multigigabit links
- Leading PoE capabilities with up to 384 ports of PoE per stack, 60W Cisco UPOE, and PoE+

(Cisco Catalyst 9300 Series Switches). https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.pdf, attached hereto as Exhibit 16, at 2.

248. As shown below, the Accused '552 Products include many configurations, all of which include communications ports.

Table 1. Cisco Catalyst 9300 Series Switch Configurations

Model	Total 10/100/1000 or Multigigabit copper ports	Default AC power supply	Available PoE power	Cisco StackWise-480	Cisco StackPower
C9300-24T	24	350W AC		Yes	Yes
C9300-48T	48	350W AC		Yes	Yes
C9300-24P	24 POE+	715W AC	445W	Yes	Yes
C9300-48P	48 POE+	715W AC	437W	Yes	Yes
C9300-24U	24 Cisco UPOE	1100W AC	830W	Yes	Yes
C9300-48U	48 Cisco UPOE	1100W AC	822W	Yes	Yes
C9300-24UX	24 Multigigabit Cisco UPOE (100 Mbps or 1, 2.5, 5, or 10 Gbps)	1100W AC	560W	Yes	Yes
C9300-48UXM	48x 2.5G ports (12 mGig – 100 Mbps or 1, 2.5, 5, or 10 Gbps)	1100W AC	490W	Yes	Yes

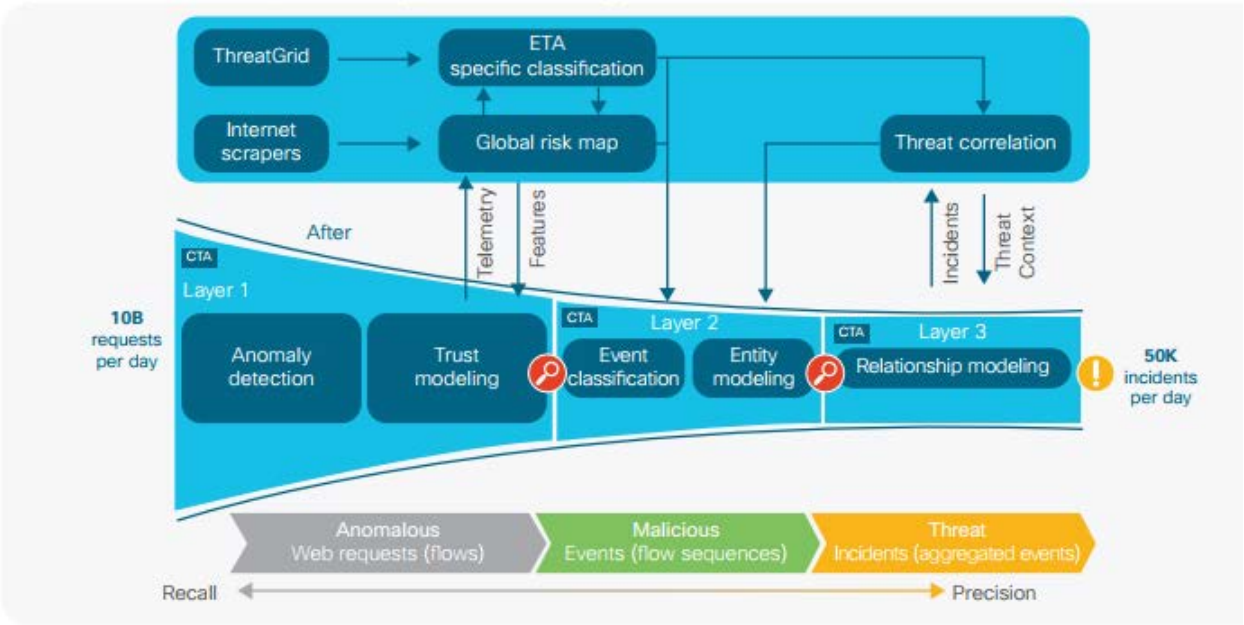
Id. at 3.

249. The Accused '552 Products perform the steps of "receiving, via the

communication interface, a plurality of hypertext transfer protocol secure (HTTPS) packets; responsive to a determination by the at least one processor that at least a portion of the plurality of HTTPS packets have packet-header-field values corresponding to a packet filtering rule stored in the memory."

250. As shown below, the Accused '552 Products "correlate traffic with global threat behaviors to automatically identify infected hosts, command and control communication and suspicious traffic":

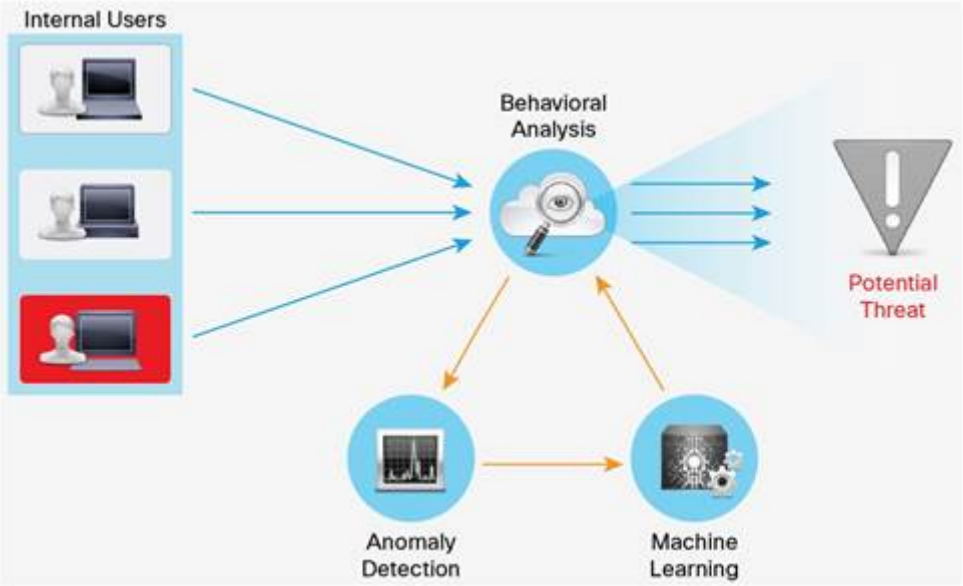
Figure 3. Stealtwatch Enterprise Multi-layer Machine Learning



(Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at 5.

251. The Accused '552 Products include Cognitive Threat Analytics ("CTA"). CTA "[a]nalyz[es] more than 10 billion web requests daily, [and] finds malicious activity that has bypassed security controls, or entered through unmonitored channels (including removable media), and is operating inside an organization's environment. Cognitive Threat Analytics is a cloud-based product that uses machine learning and statistical modeling of networks. It creates

a baseline of the traffic in your network and identifies anomalies. It analyzes user and device behavior, and web traffic, to discover command-and-control communications, data exfiltration, and potentially unwanted applications operating in your infrastructure (Figure 1)."



https://www.cisco.com/c/en/us/products/collateral/security/cognitive-threat-analytics/datasheet-c78-736557.html, attached hereto as Exhibit 29, at 1.

252. CTA "is integrated with Cisco AMP Threat Grid. When CTA independently detects command-and-control communication in the web channel, it queries the AMP Threat Grid database and correlates the indicators of compromise with the millions of malware artifacts seen by AMP Threat Grid to identify the malware that caused the anomaly." *Id.* at 2. CTA also provides Automated Response and "integrates with existing security monitoring technologies, including Security Information and Event Management (SIEM) platforms. Organizations can integrate and automate their response with an established workflow." *Id.*

253. The Accused '552 Products perform the steps of "applying, by the at least one processor, an operator specified by the packet-filtering rule to the at least a portion of the plurality of HTTPS packets, wherein the operator specifies one or more application-header-

field-value criteria identifying one or more transport layer security (TLS)-version values for which packets should be blocked from continuing toward their respective destinations." The Accused '552 Products "extract[] four main data elements: the sequence of packet lengths and times, the byte distribution, TLS-specific features and the initial data packet. Cisco's unique Application-Specific Integrated Circuit (ASIC) architecture provides the ability to extract these data elements without slowing down the data network," which includes the Initial Data Packet ("IDP"). (Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at 4. "IDP is used to obtain packet data from the first packet of a flow. It allows extraction of interesting data such as an HTTP URL, DNS hostname/address and other data elements. The TLS handshake is composed of several messages that contain interesting, unencrypted metadata used to extract data elements such as cipher suites, TLS versions and the client's public key length." *Id.*

Appendix A

Data Elements Extracted by Encrypted Traffic Analytics.

Data Element Name	Description
Sequence of Packet Lengths and Times (SPLT)	An array of LENGTH values followed by an array of INTERARRIVAL TIME values describing the first N packets of a flow that carry application payload. Each LENGTH is encoded as a 16-bit integer to form a 20-byte array. Immediately following this, each INTERARRIVAL TIME is encoded as a 16-bit integer to form another 20-byte array.
Byte distribution	A histogram giving the frequency of occurrence for each byte value or (range of values) in the first N bytes of application payload for a flow. Each "frequency of occurrence" is represented as a 16-bit integer.
Initial Data Packet (IDP)	The content of the first packet of this flow that contains actual payload data, starting at the beginning of the IP header.
TLS records	An array of LENGTH values, followed by an array of INTERARRIVAL TIME values, followed by an array of CONTENT TYPE values, followed by an array of HANDSHAKE TYPE values. These arrays describe the first N records of a TLS flow.
TLS record lengths	A sequence of record lengths for up to the first N records of a TLS flow.
TLS record times	A sequence of TLS interarrival times for up to the first N records of a TLS flow.
TLS content types	A sequence of ContentType values for up to the first N records of a TLS flow.
TLS handshake types	A sequence of HandshakeType values for up to the first N records of a TLS flow.
TLS cipher suites	A list of up to N cipher suites offered by the client, or selected by the server in a TLS flow.

Data Element Name	Description
TLS extensions	An array of LENGTH values followed by an array of EXTENSION TYPE values describing the TLS extensions observed in the Hello message for a TLS flow.
TLS extension lengths	A list of extension lengths for up to the first N TLS extensions observed in the TLS Hello message for a flow.
TLS extension types	A list of extension types for up to the first N TLS extensions observed in the TLS Hello message for a flow.
TLS version	The TLS version number observed in the TLS Hello message for a flow.
TLS key length	The length of the client key observed in the TLS ClientKeyExchange message.
TLS session ID	The session ID value observed (if any) in the TLS Hello message for a flow.
TLS random	The random value observed in the TLS Hello message for this flow.

Id. at 8-9.

254. The Accused '552 Products perform the steps of "responsive to a determination by the at least one processor that one or more packets, of the at least a portion of the plurality of HTTPS packets, have one or more application-header-field values corresponding to one or more TLS-version values of the one or more TLS-version values for which packets should be blocked from continuing toward their respective destinations, applying, by the at least one processor, at least one packet-transformation function specified by the operator to the one or more packets to block each packet of the one or more packets from continuing toward its respective destination." As shown below, the Accused '552 Products "turns the network into an end-to-end sensor and enforcer that detects, contains and prevents emerging sophisticated security threats":

Conclusion

In summary, the network is now an even more advanced security sensor, capable of detecting threats in encrypted traffic. A Cisco Digital Network Architecture-ready infrastructure turns the network into an end-to-end sensor and enforcer that detects, contains and prevents emerging, sophisticated security threats.

Id. at 8.

255. As a result of Cisco'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.

256. Cisco's infringement of the '552 Patent has injured and continues to injure Centripetal in an amount to be proven at trial.

257. Cisco has willfully infringed each of the Asserted Patents. Centripetal is informed and believes that Cisco had knowledge of the Asserted Patents through various channels and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

258. On or around 2014, Centripetal partnered with ThreatGRID, a company which

included threat intelligence technology which Centripetal integrated with their patented products that used some of the Asserted Patents. Cisco later acquired ThreatGRID in 2016. Centripetal is informed and believes that Cisco gained increased exposure to Centripetal's patented technology as a result of the acquisition of ThreatGRID. https://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/threatgrid.html, attached hereto as Exhibit 31.

259. Centripetal is further informed and believes that, on or around January 2016, Cisco requested an introduction to Centripetal through a third party, Granite Hill Capital Partners. Later, Centripetal received a point of contact introduction to Cisco from Granite Hill Capital Partners.

260. In 2016, Cisco invited Centripetal to participate in Cisco Live, which is Cisco's partner conference – in which Centripetal was asked to demonstrate its technology in Cisco's "Security Partner Village" booth. On or around June 2016, Centripetal attended the Cisco Live conference and demonstrated its patented technology, including the RuleGATE Threat Intelligence Gateway product which encompasses at least some of the Asserted Patents. Cisco currently lists Centripetal on its website located at www.cisco.com, as part of a "partner ecosystem" whose "[t]hreat intelligence platforms" use Threat Grid. https://www.cisco.com/c/en/us/products/security/threat-grid/integrations.html#~stickynav=2, attached hereto as Exhibit 32, at 3.

261. Cisco thus knew or, in the alternative, was willfully blind to Centripetal's technology and its Asserted Patents. Cisco's infringement of the '552 Patent is egregious because despite this knowledge, Centripetal is informed and believes that Cisco deliberately copied Centripetal's patented technology, which it implemented into its products and services,

such as Centripetal's CleanINTERNET service and Threat Intelligence Gateway, including the RuleGATE 2000. The blatant copying of Centripetal's patented technology and disregard for Centripetal's patent rights with an objectively high likelihood of infringement is egregious behavior warranting a finding of willful infringement and enhanced damages.

262. Centripetal is informed and believes that Cisco has undertaken no efforts to design these products or services around the '552 Patent to avoid infringement despite Cisco's knowledge and understanding that its products and services infringe the '552 Patent. As such, Cisco has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '552 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.

FOURTEENTH CAUSE OF ACTION
(Indirect Infringement of the '552 Patent pursuant to 35 U.S.C. § 271(b))

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

264. Cisco has induced and continues to induce infringement of one or more claims of the '552 Patent under 35 U.S.C. § 271(b).

265. In addition to directly infringing the '552 Patent, Cisco indirectly infringes the '552 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '552 Patent, where all the steps of the method claims are performed by either Cisco, its customers, purchasers, users or developers, or some combination thereof. Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or

developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the '552 Patent, including Claims 1-7.

266. Cisco knowingly and actively aided and abetted the direct infringement of the '552 Patent by instructing and encouraging its customers, purchasers, users and developers to use the '552 Accused Products. Such instructions and encouragement include, but are not limited to, advising third parties to use the '552 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '552 Patent, specifically through the use of the Accused Catalyst Products, the Accused Router Products, and the Accused Stealthwatch Products, alone or in conjunction with one another, and by advertising and promoting the use of the '552 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '552 Accused Products in an infringing manner.

267. Cisco updates and maintains an HTTP site with Cisco's quick start guides, administration guides, user guides, operating instructions, blogs, white papers, data sheets and training certification programs which cover in depth aspects of operating Cisco's offerings. *See* https://www.cisco.com/c/en/us/support/switches/catalyst-9300-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 34; https://www.cisco.com/c/en/us/support/switches/catalyst-9400-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 35; https://www.cisco.com/c/en/us/support/switches/catalyst-9500-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 36; https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.pdf, attached hereto as Exhibit 16; *see also* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-

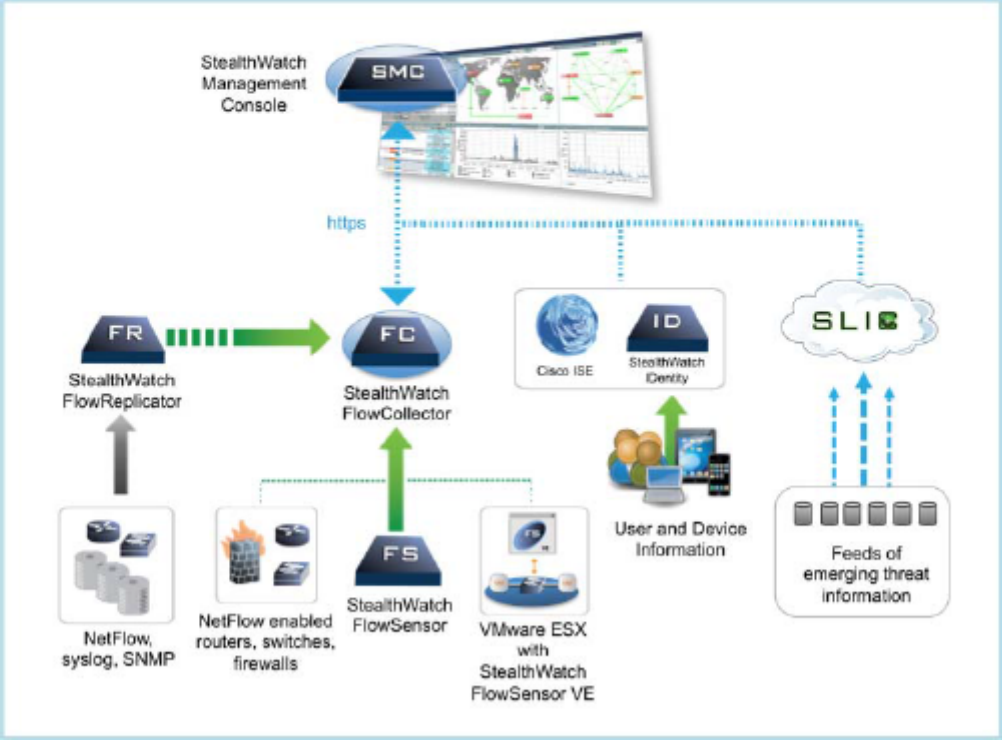
switches/datasheet-c78-739053.pdf, attached hereto as Exhibit 17; https://www.cisco.com/c/en/us/support/routers/index.html, attached hereto as Exhibit 37; *see also* https://www.cisco.com/c/dam/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/at-a-glance-c45-612993.pdf, attached hereto as Exhibit 18; *see also* https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/datasheet-c78-732542.pdf, attached hereto as Exhibit 19; https://blogs.cisco.com/enterprise/cisco-traffic-analysis-encrypted-threat-analytics, attached hereto as Exhibit 38; https://communities.cisco.com/docs/DOC-76964, attached hereto as Exhibit 39; https://www.cisco.com/c/en/us/support/security/stealthwatch/tsd-products-support-series-home.html, attached hereto as Exhibit 40; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-guides-list.html, attached hereto as Exhibit 41; https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/hardware/installation/SW_6_9_1_Hardware_Installation_DV_1_2.pdf, attached hereto as Exhibit 42; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-and-configuration-guides-list.html, attached hereto as Exhibit 43; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-programming-reference-guides-list.html, attached hereto as Exhibit 44; https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-routing-switching.html, attached hereto as Exhibit 45.

268. These documents provide instructions, directions and/or require others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the ‘552 Patent,

where all the steps of the method claims are performed by either Cisco, its customers, purchasers, users or developers, or some combination thereof. For example, Cisco includes the Stealthwatch System Hardware Installation Guide, which provides instructions and recommendations on how to install and deploy the Accused '552 Products in an infringing manner as shown below.

Placement Considerations

As shown in the figure below, Stealthwatch system products can be strategically deployed to provide optimal coverage of key network segments throughout the network, whether in the internal network, at the perimeter, or in the DMZ.



Placing the SMC

As the management device, the Stealthwatch Management Console (SMC) should be installed at a location on your network that is accessible to all the devices sending data to it.

If you have a failover pair of SMCs, it is recommended that you install the primary SMC and the secondary SMC in separate physical locations. This strategy will enhance a disaster recovery effort should it become necessary.

Placing the Stealthwatch Flow Collector

As collection and monitoring devices, the Stealthwatch Flow Collector for NetFlow appliance and the Stealthwatch Flow Collector for sFlow appliance should be installed at a location on your network that is accessible to the NetFlow or sFlow devices sending the data to a Flow Collector, as well as any devices you plan to use to access the management interface.

Note: When you place a Flow Collector outside a firewall, Lancope recommends that you turn off the setting "Accept traffic from any exporter."

Placing the Stealthwatch Flow Sensor

As a passive monitoring device, the Stealthwatch Flow Sensor can sit at multiple points on your network to observe and record IP activity, thereby protecting network integrity and detecting security breaches. The Flow Sensor features integrated Web-based management systems that facilitate either centralized or remote management and administration.

The Flow Sensor appliance is most effective when placed at critical segments of your corporate network as follows:

- Inside your firewall to monitor traffic and determine if a firewall breach has occurred
- Outside your firewall, monitoring traffic flow to analyze who is threatening your firewall
- At sensitive segments of your network, offering protection from disgruntled employees or hackers with root access
- At remote office locations that constitute vulnerable network extensions
- On your business network for protocol use management (for example, on your transaction services subnet to determine if a hacker is running Telnet or FTP and compromising your customers' financial data)

Placing Other Stealthwatch Products

The only requirement for the placement of other Stealthwatch products, such as the Stealthwatch UDP Director (also known as FlowReplicator), or a VM server containing a Stealthwatch Flow Sensor Virtual Edition (VE), is that they have an unobstructed communication path to the rest of your Stealthwatch products as applicable.

Exhibit 42 at 11-12.

269. As such, Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the '552 Patent.

FIFTEENTH CAUSE OF ACTION
(Direct Infringement of the '213 Patent pursuant to 35 U.S.C. § 271(a))

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

271. Cisco has infringed and continues to infringe Claims 1-16 of the '213 Patent in violation of 35 U.S.C. § 271(a).

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

273. Cisco'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.

274. Cisco's infringement includes the manufacture, use, sale, importation and/or offer for sale of Cisco's products and services, including but not limited to the Accused Catalyst Products, the Accused Router Products, and the Accused Stealthwatch Products, alone or in conjunction with one another (collectively, the "Accused '213 Products").

275. The Accused '213 Products embody the patented invention of the '213 Patent and infringe the '213 Patent because they practice a method comprising:

> receiving, by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server, a dynamic security policy that comprises at least one rule specifying application-layer packet-header information and a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information;
>
> receiving, by a packet security gateway of the plurality of packet security gateways,

packets associated with a network protected by the packet security gateway;

identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets comprising the application-layer packet-header information;

performing, by the packet security gateway and on a packet-by-packet basis, the packet transformation function on each of the one or more packets comprising the application-layer packet-header information, wherein the performing the packet transformation function comprises

identifying a subset of information specified by the packet digest logging function for each of the one or more packets comprising the application-layer packet-header information;

generating, for each of the one or more packets comprising the application-layer packet-header information, a record comprising the subset of information specified by the packet digest logging function; and

reformatting, for each of the one or more packets comprising the application-layer packet-header information, the subset of information specified by the packet digest logging function in accordance with a logging system standard; and

routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the application-layer packet-header information in response to the performing the packet transformation function.

'213 Patent, Claim 1.

276. The Accused '213 Products perform the step of "receiving, by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server, a dynamic security policy that comprises at least one rule specifying application-layer packet-header information and a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information." As shown below, the Accused '213 Products "enables policy-based automation from edge to cloud with foundational capabilities," including "Simplified device deployment, Unified management of wired and wireless networks, Network virtualization and segmentation, Group-based policies, and Context-based analytics."

The Foundation of Software-Defined Access

Advanced persistent security threats. The exponential growth of Internet of Things (IoT) devices. Mobility everywhere. Cloud adoption. All of these require a network fabric that integrates advanced hardware and software innovations to automate, secure, and simplify customer networks. The goal of this network fabric is to enable customer revenue growth by accelerating the rollout of business services.

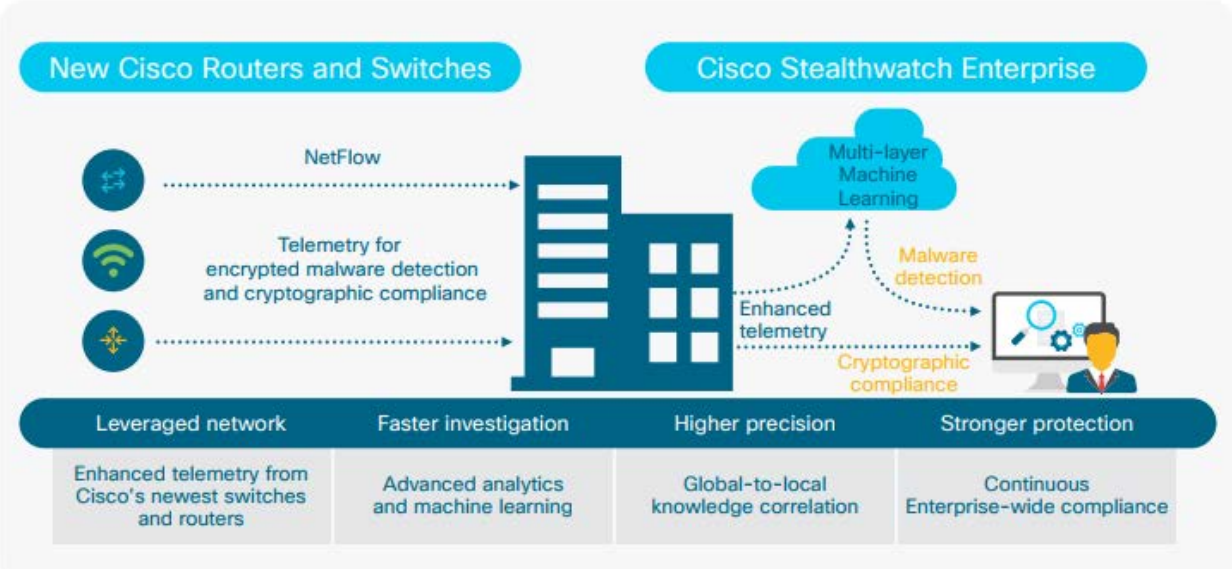
The Cisco Digital Network Architecture (Cisco DNA™) with SD-Access is the network fabric that powers business. It is an open and extensible, software-driven architecture that accelerates and simplifies your enterprise network operations. The programmable architecture frees your IT staff from time-consuming, repetitive network configuration tasks so they can focus instead on innovation that positively transforms your business. SD-Access enables policy-based automation from edge to cloud with foundational capabilities. These include:

- Simplified device deployment
- Unified management of wired and wireless networks
- Network virtualization and segmentation
- Group-based policies
- Context-based analytics

(Cisco Catalyst 9300 Series Switches). https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.pdf, attached hereto as Exhibit 16, at 1.

277. The Accused '213 Products perform the steps of "receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway," and "identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets comprising the application-layer packet-header information":

Figure 2. Encrypted Traffic Analytics – technical solution overview

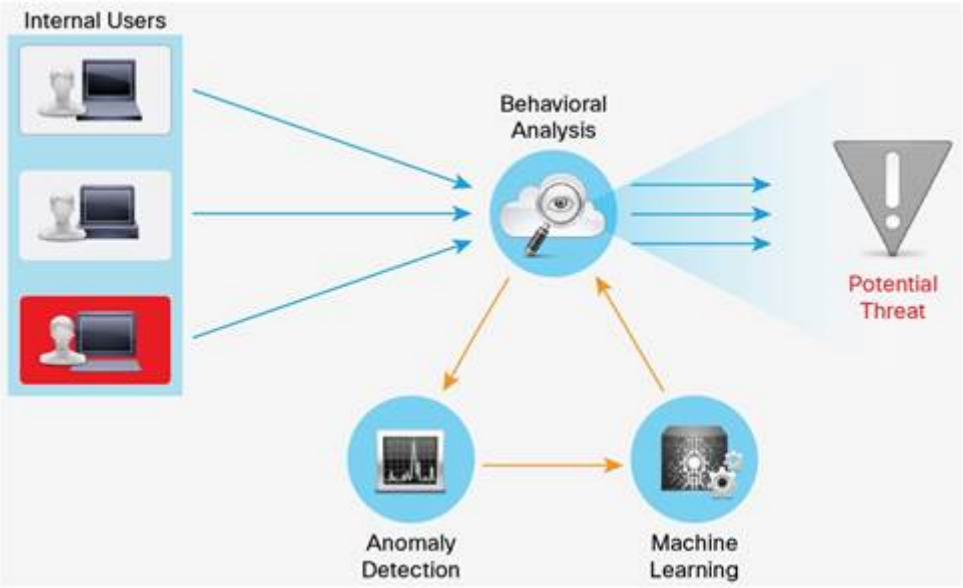


(Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at 3.

278. The Accused '213 Products perform the steps of "performing, by the packet security gateway and on a packet-by-packet basis, the packet transformation function on each of the one or more packets comprising the application-layer packet-header information, wherein the performing the packet transformation function comprises," "identifying a subset of information specified by the packet digest logging function for each of the one or more packets comprising the application-layer packet-header information," "generating, for each of the one or more packets comprising the application-layer packet-header information, a record comprising the subset of information specified by the packet digest logging function," and "reformatting, for each of the one or more packets comprising the application-layer packet-header information, the subset of information specified by the packet digest logging function in accordance with a logging system standard."

279. The Accused '213 Products include Cognitive Threat Analytics ("CTA"). CTA "[a]nalyz[es] more than 10 billion web requests daily, [and] finds malicious activity that has

bypassed security controls, or entered through unmonitored channels (including removable media), and is operating inside an organization's environment. Cognitive Threat Analytics is a cloud-based product that uses machine learning and statistical modeling of networks. It creates a baseline of the traffic in your network and identifies anomalies. It analyzes user and device behavior, and web traffic, to discover command-and-control communications, data exfiltration, and potentially unwanted applications operating in your infrastructure (Figure 1)."

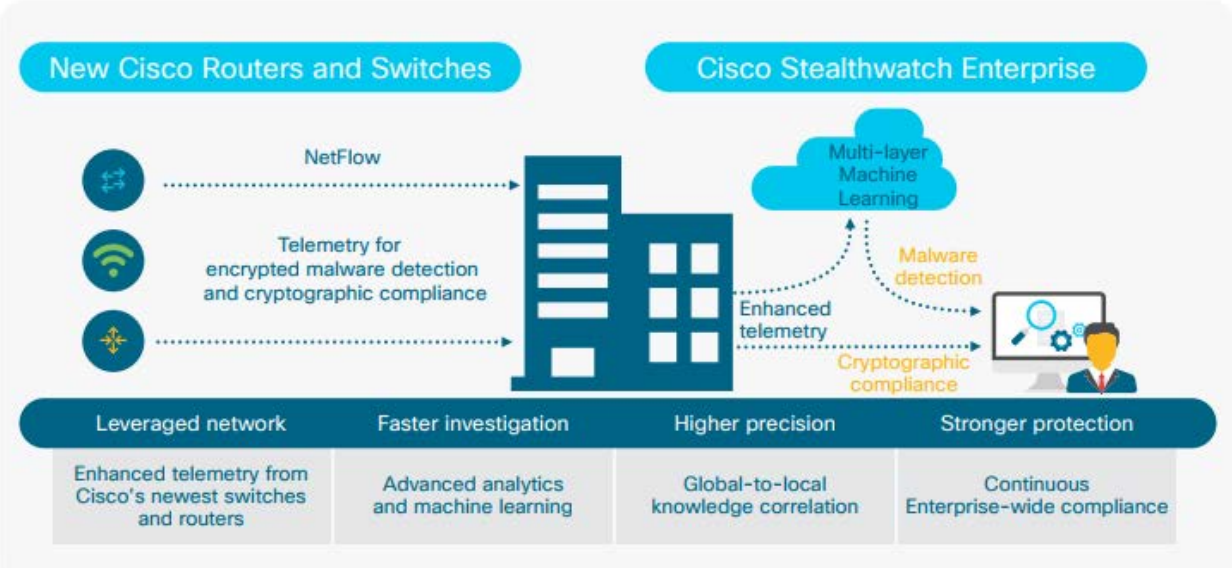


https://www.cisco.com/c/en/us/products/collateral/security/cognitive-threat-analytics/datasheet-c78-736557.html, attached hereto as Exhibit 29, at 1.

280. CTA "is integrated with Cisco AMP Threat Grid. When CTA independently detects command-and-control communication in the web channel, it queries the AMP Threat Grid database and correlates the indicators of compromise with the millions of malware artifacts seen by AMP Threat Grid to identify the malware that caused the anomaly." *Id.* at 2. CTA also provides Automated Response and "integrates with existing security monitoring technologies, including Security Information and Event Management (SIEM) platforms. Organizations can integrate and automate their response with an established workflow." *Id.*

281. As shown below, the Accused '213 Products collect, store, and analyze both traditional flow data and intraflow metadata and "[o]btain contextual threat intelligence with real-time analysis correlated with user and device information." (Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at 2-4.

Figure 2. Encrypted Traffic Analytics – technical solution overview

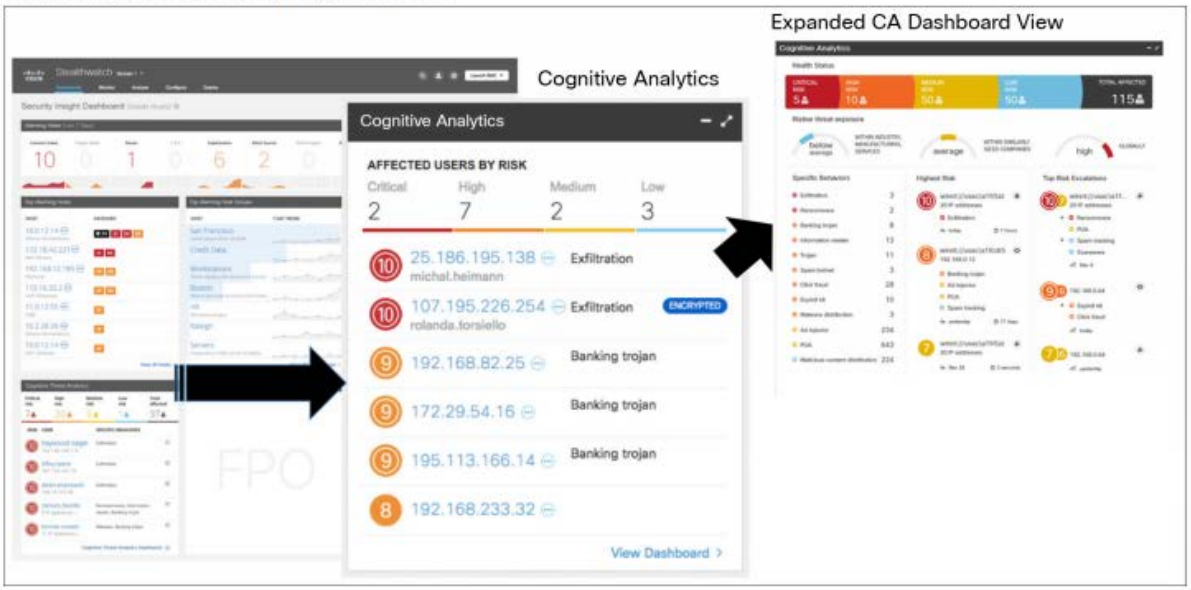


Id. at 3.

282. As shown below, the Accused '213 Products' "Security Insight dashboard . . . provides a view of affected users identified by risk type. An expanded dashboard provides detailed information regarding the top risk escalations and relative threat exposure":

The Security Insight dashboard on the Stealthwatch Management Console (SMC) provides a view of affected users identified by risk type. An expanded dashboard provides detailed information regarding the top risk escalations and relative threat exposure. Table 3 lists some high-risk threats that use encrypted command and control communications.

Figure 4. Stealthwatch security insight dashboard



Id. at 6.

283. The Accused '213 Products perform the step of "routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the application-layer packet-header information in response to the performing the packet transformation function."

284. As shown below, the Accused '213 Products include "policy-based automation from edge to cloud with foundational capabilities":

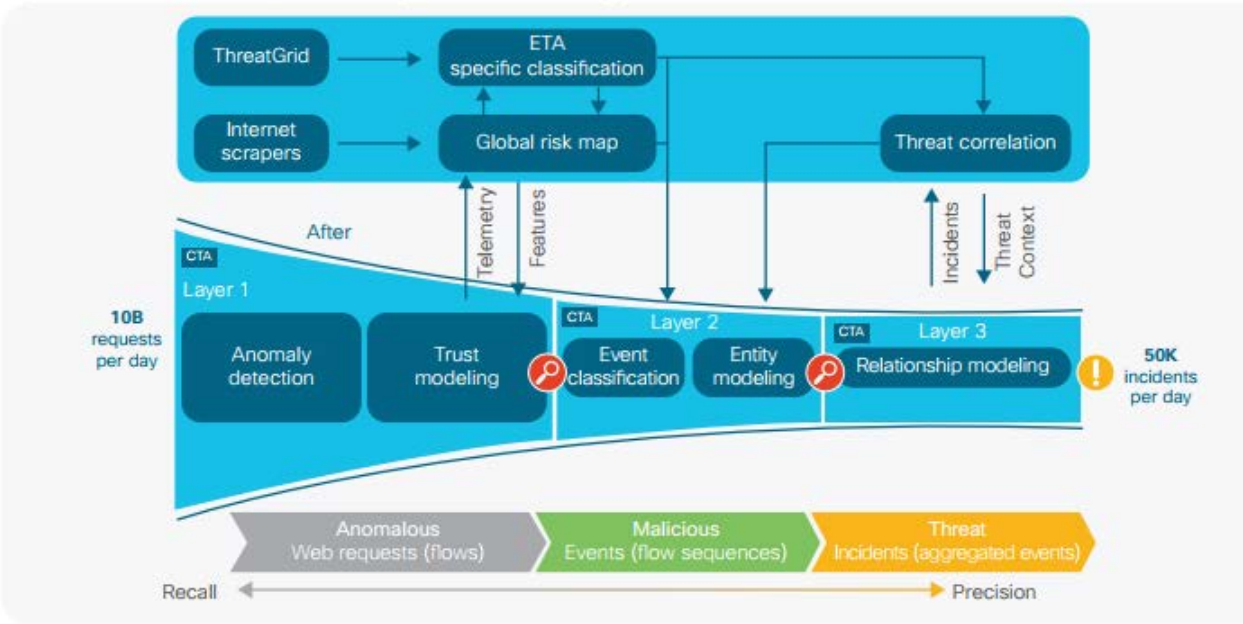
The Cisco® Digital Network Architecture (DNA) with Software Defined Access (SD-Access) is the network fabric that powers business. Cisco DNA is an open and extensible, software-driven architecture that accelerates and simplifies your enterprise network operations. The programmable architecture frees your IT staff from time consuming, repetitive network configuration tasks so they can focus instead on innovation that positively transforms your business. SD-Access enables policy-based automation from edge to cloud with foundational capabilities. These include:

- Simplified device deployment
- Unified management of wired and wireless networks
- Network virtualization and segmentation
- Group-based policies
- Context-based analytics

(Cisco Catalyst Data Sheet). https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/datasheet-c78-739053.pdf, attached hereto as Exhibit 17, at 1.

285. As shown below, the Accused '213 Products "correlate traffic with global threat behaviors to automatically identify infected hosts, command and control communication and suspicious traffic":

Figure 3. Stealtwatch Enterprise Multi-layer Machine Learning



(Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at 5.

286. As a result of Cisco'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.

287. Cisco's infringement of the '213 Patent has injured and continues to injure Centripetal in an amount to be proven at trial.

288. Cisco has willfully infringed each of the Asserted Patents. Centripetal is informed and believes that Cisco had knowledge of the Asserted Patents through various channels and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

289. On or around 2014, Centripetal partnered with ThreatGRID, a company which included threat intelligence technology which Centripetal integrated with their patented products that used some of the Asserted Patents. Cisco later acquired ThreatGRID in 2016. Centripetal is informed and believes that Cisco gained increased exposure to Centripetal's patented technology as a result of the acquisition of ThreatGRID. https://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/threatgrid.html, attached hereto as Exhibit 31.

290. Centripetal is further informed and believes that, on or around January 2016, Cisco requested an introduction to Centripetal through a third party, Granite Hill Capital Partners. Later, Centripetal received a point of contact introduction to Cisco from Granite Hill Capital Partners.

291. In 2016, Cisco invited Centripetal to participate in Cisco Live, which is Cisco's partner conference – in which Centripetal was asked to demonstrate its technology in Cisco's "Security Partner Village" booth. On or around June 2016, Centripetal attended the Cisco Live

conference and demonstrated its patented technology, including the RuleGATE Threat Intelligence Gateway product which encompasses at least some of the Asserted Patents. Cisco currently lists Centripetal on its website located at www.cisco.com, as part of a "partner ecosystem" whose "[t]hreat intelligence platforms" use Threat Grid. https://www.cisco.com/c/en/us/products/security/threat-grid/integrations.html#~stickynav=2, attached hereto as Exhibit 32, at 3.

292. Cisco thus knew or, in the alternative, was willfully blind to Centripetal's technology and its Asserted Patents. Cisco's infringement of the '213 Patent is egregious because despite this knowledge, Centripetal is informed and believes that Cisco deliberately copied Centripetal's patented technology, which it implemented into its products and services, such as Centripetal's CleanINTERNET service and Threat Intelligence Gateway, including the RuleGATE 2000. The blatant copying of Centripetal's patented technology and disregard for Centripetal's patent rights with an objectively high likelihood of infringement is egregious behavior warranting a finding of willful infringement and enhanced damages.

293. Centripetal is informed and believes that Cisco has undertaken no efforts to design these products or services around the '213 Patent to avoid infringement despite Cisco's knowledge and understanding that its products and services infringe the '213 Patent. As such, Cisco has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '213 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.

SIXTEENTH CAUSE OF ACTION
(Indirect Infringement of the '213 Patent pursuant to 35 U.S.C. § 271(b))

294. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth

herein, the allegations of the preceding paragraphs, as set forth above.

295. Cisco has induced and continues to induce infringement of one or more claims of the '213 Patent under 35 U.S.C. § 271(b).

296. In addition to directly infringing the '213 Patent, Cisco indirectly infringes the '213 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '213 Patent, where all the steps of the method claims are performed by either Cisco, its customers, purchasers, users or developers, or some combination thereof. Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the '213 Patent, including Claims 1-16.

297. Cisco knowingly and actively aided and abetted the direct infringement of the '213 Patent by instructing and encouraging its customers, purchasers, users and developers to use the '213 Accused Products. Such instructions and encouragement include, but are not limited to, advising third parties to use the '213 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '213 Patent, specifically through the use of the Accused Catalyst Products, the Accused Router Products, and the Accused Stealthwatch Products, alone or in conjunction with one another, and by advertising and promoting the use of the '213 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '213 Accused Products in an infringing manner.

298. Cisco updates and maintains an HTTP site with Cisco's quick start guides,

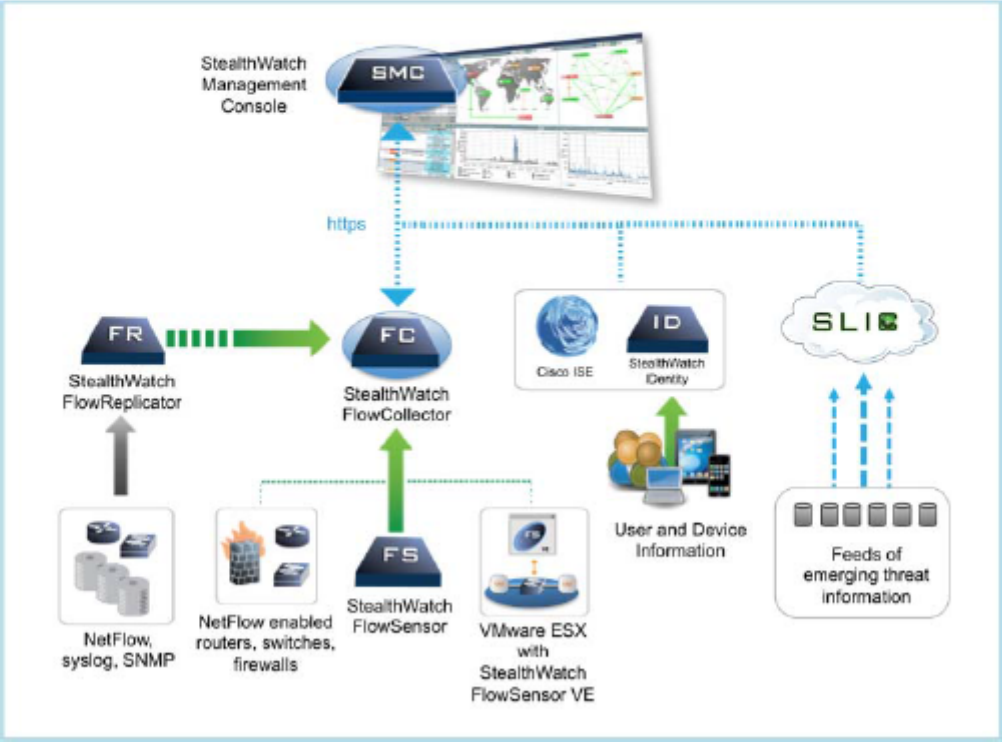
administration guides, user guides, operating instructions, blogs, white papers, data sheets and training certification programs which cover in depth aspects of operating Cisco's offerings. *See* https://www.cisco.com/c/en/us/support/switches/catalyst-9300-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 34; https://www.cisco.com/c/en/us/support/switches/catalyst-9400-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 35; https://www.cisco.com/c/en/us/support/switches/catalyst-9500-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 36; https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.pdf, attached hereto as Exhibit 16; *see also* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/datasheet-c78-739053.pdf, attached hereto as Exhibit 17; https://www.cisco.com/c/en/us/support/routers/index.html, attached hereto as Exhibit 37; *see also* https://www.cisco.com/c/dam/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/at-a-glance-c45-612993.pdf, attached hereto as Exhibit 18; *see also* https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/datasheet-c78-732542.pdf, attached hereto as Exhibit 19; https://blogs.cisco.com/enterprise/cisco-traffic-analysis-encrypted-threat-analytics, attached hereto as Exhibit 38; https://communities.cisco.com/docs/DOC-76964, attached hereto as Exhibit 39; https://www.cisco.com/c/en/us/support/security/stealthwatch/tsd-products-support-series-home.html, attached hereto as Exhibit 40; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-guides-list.html, attached hereto as Exhibit 41;

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/hardware/installation/SW_6_9_1_Hardware_Installation_DV_1_2.pdf, attached hereto as Exhibit 42; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-and-configuration-guides-list.html, attached hereto as Exhibit 43; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-programming-reference-guides-list.html, attached hereto as Exhibit 44; https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-routing-switching.html, attached hereto as Exhibit 45.

299. These documents provide instructions, directions and/or require others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '213 Patent, where all the steps of the method claims are performed by either Cisco, its customers, purchasers, users or developers, or some combination thereof. For example, Cisco includes the Stealthwatch System Hardware Installation Guide, which provides instructions and recommendations on how to install and deploy the Accused '213 Products in an infringing manner as shown below.

Placement Considerations

As shown in the figure below, Stealthwatch system products can be strategically deployed to provide optimal coverage of key network segments throughout the network, whether in the internal network, at the perimeter, or in the DMZ.



Placing the SMC

As the management device, the Stealthwatch Management Console (SMC) should be installed at a location on your network that is accessible to all the devices sending data to it.

If you have a failover pair of SMCs, it is recommended that you install the primary SMC and the secondary SMC in separate physical locations. This strategy will enhance a disaster recovery effort should it become necessary.

Placing the Stealthwatch Flow Collector

As collection and monitoring devices, the Stealthwatch Flow Collector for NetFlow appliance and the Stealthwatch Flow Collector for sFlow appliance should be installed at a location on your network that is accessible to the NetFlow or sFlow devices sending the data to a Flow Collector, as well as any devices you plan to use to access the management interface.

Note: When you place a Flow Collector outside a firewall, Lancope recommends that you turn off the setting "Accept traffic from any exporter."

Placing the Stealthwatch Flow Sensor

As a passive monitoring device, the Stealthwatch Flow Sensor can sit at multiple points on your network to observe and record IP activity, thereby protecting network integrity and detecting security breaches. The Flow Sensor features integrated Web-based management systems that facilitate either centralized or remote management and administration.

The Flow Sensor appliance is most effective when placed at critical segments of your corporate network as follows:

- Inside your firewall to monitor traffic and determine if a firewall breach has occurred
- Outside your firewall, monitoring traffic flow to analyze who is threatening your firewall
- At sensitive segments of your network, offering protection from disgruntled employees or hackers with root access
- At remote office locations that constitute vulnerable network extensions
- On your business network for protocol use management (for example, on your transaction services subnet to determine if a hacker is running Telnet or FTP and compromising your customers' financial data)

Placing Other Stealthwatch Products

The only requirement for the placement of other Stealthwatch products, such as the Stealthwatch UDP Director (also known as FlowReplicator), or a VM server containing a Stealthwatch Flow Sensor Virtual Edition (VE), is that they have an unobstructed communication path to the rest of your Stealthwatch products as applicable.

Exhibit 42 at 11-12.

300. As such, Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the '213 Patent.

SEVENTEENTH CAUSE OF ACTION
(Direct Infringement of the '205 Patent pursuant to 35 U.S.C. § 271(a))

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

302. Cisco has infringed and continues to infringe Claims 1-96 of the '205 Patent in violation of 35 U.S.C. § 271(a).

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

304. Cisco'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.

305. Cisco's infringement includes the manufacture, use, sale, importation and/or offer for sale of Cisco's products and services, including but not limited to the Accused Catalyst Products, the Accused Router Products, and the Accused Stealthwatch Products, alone or in conjunction with one another (collectively, the "Accused '205 Products").

306. The Accused '205 Products embody the patented invention of the '205 Patent and infringe the '205 Patent because they practice a method comprising:

at each packet security gateway of one or more packet security gateways associated with a security policy management server:

receiving a plurality of dynamic security policies from the security policy management server, wherein receiving the plurality of dynamic security policies comprises:

receiving at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets

associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped;

receiving, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded;

receiving, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should be forwarded; and

receiving, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses;

receiving packets associated with a network protected by the packet security gateway; and

performing, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the packet security gateway, wherein performing the at least one of the multiple packet transformation functions specified by the plurality of dynamic security policies on the packets comprises performing at least one packet transformation function other than forwarding or dropping the packets.

‘205 Patent, Claim 1.

307. The Accused ‘205 Products perform the steps of “at each packet security gateway of one or more packet security gateways associated with a security policy management server: receiving a plurality of dynamic security policies from the security policy management server, wherein receiving the plurality of dynamic security policies comprises:” “receiving at least one rule specifying a set of network addresses for which associated packets should be forwarded and at least one rule specifying that all packets associated with network addresses outside the set of network addresses for which packets should be forwarded should be dropped,” “receiving, at a first time, a dynamic security policy specifying a first set of network addresses for which packets should be forwarded,” “receiving, at a second time, a dynamic security policy specifying a second set of network addresses for which packets should

be forwarded," and "receiving, at a third time, a dynamic security policy specifying a third set of network addresses for which packets should be forwarded, the second time being after the first time, the third time being after the second time, the second set of network addresses including more network addresses than the first set of network addresses, and the third set of network addresses including more network addresses than the second set of network addresses." As shown below, the Accused '205 Products "enables policy-based automation from edge to cloud with foundational capabilities," including "Simplified device deployment, Unified management of wired and wireless networks, Network virtualization and segmentation, Group-based policies, and Context-based analytics."

The Foundation of Software-Defined Access

Advanced persistent security threats. The exponential growth of Internet of Things (IoT) devices. Mobility everywhere. Cloud adoption. All of these require a network fabric that integrates advanced hardware and software innovations to automate, secure, and simplify customer networks. The goal of this network fabric is to enable customer revenue growth by accelerating the rollout of business services.

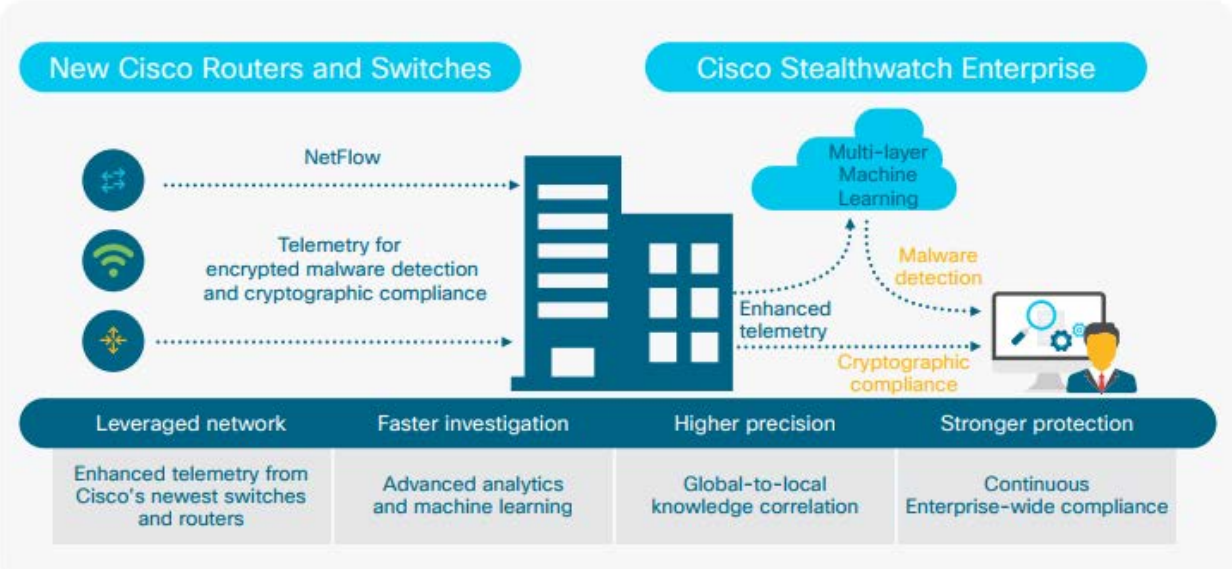
The Cisco Digital Network Architecture (Cisco DNA™) with SD-Access is the network fabric that powers business. It is an open and extensible, software-driven architecture that accelerates and simplifies your enterprise network operations. The programmable architecture frees your IT staff from time-consuming, repetitive network configuration tasks so they can focus instead on innovation that positively transforms your business. SD-Access enables policy-based automation from edge to cloud with foundational capabilities. These include:

- Simplified device deployment
- Unified management of wired and wireless networks
- Network virtualization and segmentation
- Group-based policies
- Context-based analytics

(Cisco Catalyst 9300 Series Switches). https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.pdf, attached hereto as Exhibit 16, at 1.

308. The Accused '205 Products perform the step of "receiving packets associated with a network protected by the packet security gateway."

Figure 2. Encrypted Traffic Analytics – technical solution overview



(Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at 3.

309. The Accused '205 Products perform the step of "performing, on a packet by packet basis, at least one of multiple packet transformation functions specified by the plurality of dynamic security policies on the packets associated with the network protected by the packet security gateway, wherein performing the at least one of the multiple packet transformation functions specified by the plurality of dynamic security policies on the packets comprises performing at least one packet transformation function other than forwarding or dropping the packets."

310. As shown below, the Accused '205 Products include "policy-based automation from edge to cloud with foundational capabilities":

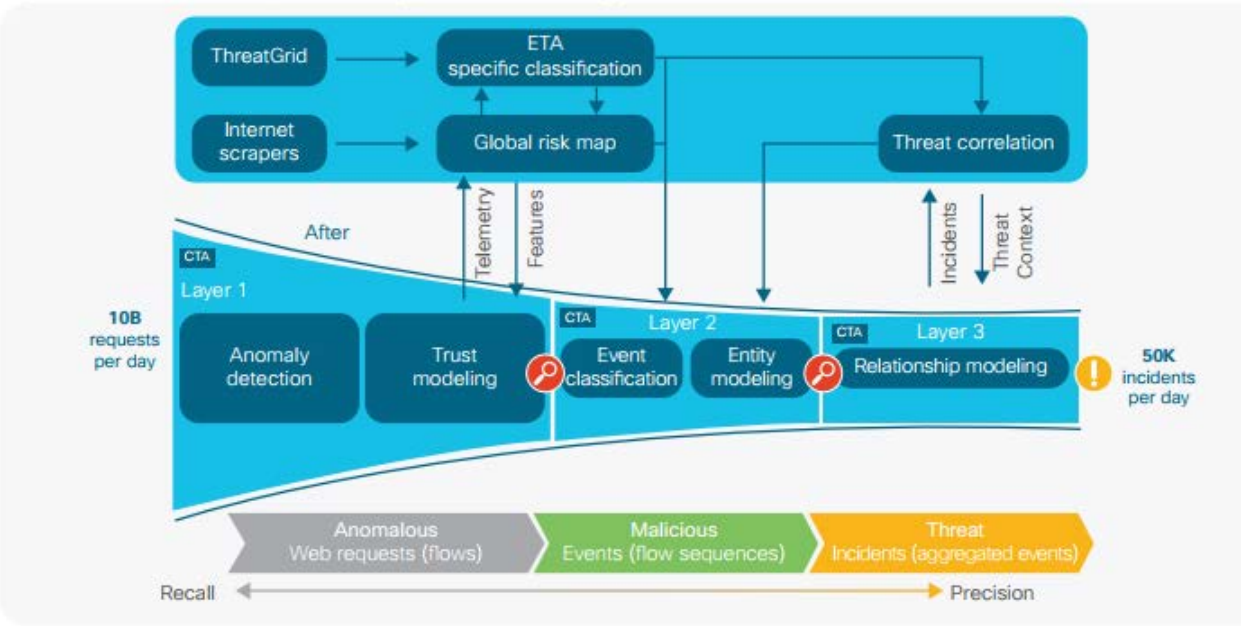
The Cisco® Digital Network Architecture (DNA) with Software Defined Access (SD-Access) is the network fabric that powers business. Cisco DNA is an open and extensible, software-driven architecture that accelerates and simplifies your enterprise network operations. The programmable architecture frees your IT staff from time consuming, repetitive network configuration tasks so they can focus instead on innovation that positively transforms your business. SD-Access enables policy-based automation from edge to cloud with foundational capabilities. These include:

- Simplified device deployment
- Unified management of wired and wireless networks
- Network virtualization and segmentation
- Group-based policies
- Context-based analytics

(Cisco Catalyst Data Sheet). https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/datasheet-c78-739053.pdf, attached hereto as Exhibit 17, at 1.

311. As shown below, the Accused '205 Products "correlate traffic with global threat behaviors to automatically identify infected hosts, command and control communication and suspicious traffic":

Figure 3. Stealtwatch Enterprise Multi-layer Machine Learning



(Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at

5.

312. As a result of Cisco'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.

313. Cisco's infringement of the '205 Patent has injured and continues to injure Centripetal in an amount to be proven at trial.

314. Cisco has willfully infringed each of the Asserted Patents. Centripetal is informed and believes that Cisco had knowledge of the Asserted Patents through various channels and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

315. On or around 2014, Centripetal partnered with ThreatGRID, a company which included threat intelligence technology which Centripetal integrated with their patented products that used some of the Asserted Patents. Cisco later acquired ThreatGRID in 2016. Centripetal is informed and believes that Cisco gained increased exposure to Centripetal's patented technology as a result of the acquisition of ThreatGRID. https://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/threatgrid.html, attached hereto as Exhibit 31.

316. Centripetal is further informed and believes that, on or around January 2016, Cisco requested an introduction to Centripetal through a third party, Granite Hill Capital Partners. Later, Centripetal received a point of contact introduction to Cisco from Granite Hill Capital Partners.

317. In 2016, Cisco invited Centripetal to participate in Cisco Live, which is Cisco's partner conference – in which Centripetal was asked to demonstrate its technology in Cisco's "Security Partner Village" booth. On or around June 2016, Centripetal attended the Cisco Live

conference and demonstrated its patented technology, including the RuleGATE Threat Intelligence Gateway product which encompasses at least some of the Asserted Patents. Cisco currently lists Centripetal on its website located at www.cisco.com, as part of a "partner ecosystem" whose "[t]hreat intelligence platforms" use Threat Grid. https://www.cisco.com/c/en/us/products/security/threat-grid/integrations.html#~stickynav=2, attached hereto as Exhibit 32, at 3.

318. Cisco thus knew or, in the alternative, was willfully blind to Centripetal's technology and its Asserted Patents. Cisco's infringement of the '205 Patent is egregious because despite this knowledge, Centripetal is informed and believes that Cisco deliberately copied Centripetal's patented technology, which it implemented into its products and services, such as Centripetal's CleanINTERNET service and Threat Intelligence Gateway, including the RuleGATE 2000. The blatant copying of Centripetal's patented technology and disregard for Centripetal's patent rights with an objectively high likelihood of infringement is egregious behavior warranting a finding of willful infringement and enhanced damages.

319. Centripetal is informed and believes that Cisco has undertaken no efforts to design these products or services around the '205 Patent to avoid infringement despite Cisco's knowledge and understanding that its products and services infringe the '205 Patent. As such, Cisco has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '205 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.

EIGHTEENTH CAUSE OF ACTION
(Indirect Infringement of the '205 Patent pursuant to 35 U.S.C. § 271(b))

320. Centripetal repeats, realleges, and incorporates by reference, as if fully set forth

herein, the allegations of the preceding paragraphs, as set forth above.

321. Cisco has induced and continues to induce infringement of one or more claims of the ‘205 Patent under 35 U.S.C. § 271(b).

322. In addition to directly infringing the ‘205 Patent, Cisco indirectly infringes the ‘205 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the ‘205 Patent, where all the steps of the method claims are performed by either Cisco, its customers, purchasers, users or developers, or some combination thereof. Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the ‘205 Patent, including Claims 1-16, 49-62, and 91-96.

323. Cisco knowingly and actively aided and abetted the direct infringement of the ‘205 Patent by instructing and encouraging its customers, purchasers, users and developers to use the ‘205 Accused Products. Such instructions and encouragement include, but are not limited to, advising third parties to use the ‘205 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the ‘205 Patent, specifically through the use of the Accused Catalyst Products, the Accused Router Products, and the Accused Stealthwatch Products, alone or in conjunction with one another, and by advertising and promoting the use of the ‘205 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the ‘205 Accused Products in an infringing manner.

324. Cisco updates and maintains an HTTP site with Cisco’s quick start guides,

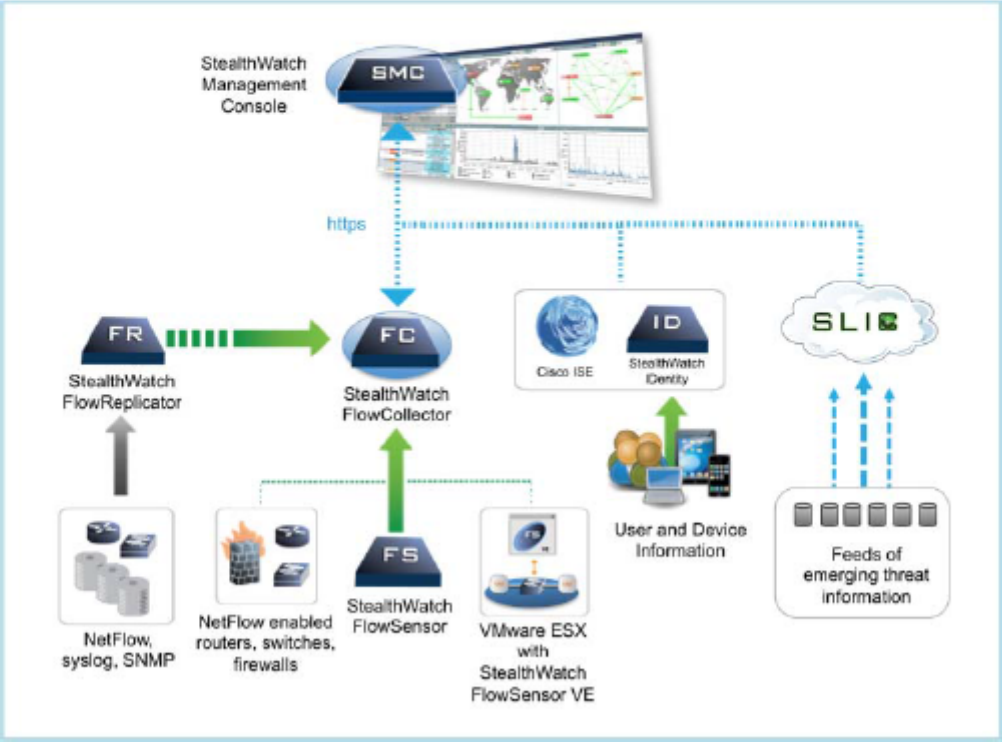
administration guides, user guides, operating instructions, blogs, white papers, data sheets and training certification programs which cover in depth aspects of operating Cisco's offerings. *See* https://www.cisco.com/c/en/us/support/switches/catalyst-9300-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 34; https://www.cisco.com/c/en/us/support/switches/catalyst-9400-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 35; https://www.cisco.com/c/en/us/support/switches/catalyst-9500-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 36; https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.pdf, attached hereto as Exhibit 16; *see also* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/datasheet-c78-739053.pdf, attached hereto as Exhibit 17; https://www.cisco.com/c/en/us/support/routers/index.html, attached hereto as Exhibit 37; *see also* https://www.cisco.com/c/dam/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/at-a-glance-c45-612993.pdf, attached hereto as Exhibit 18; *see also* https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/datasheet-c78-732542.pdf, attached hereto as Exhibit 19; https://blogs.cisco.com/enterprise/cisco-traffic-analysis-encrypted-threat-analytics, attached hereto as Exhibit 38; https://communities.cisco.com/docs/DOC-76964, attached hereto as Exhibit 39; https://www.cisco.com/c/en/us/support/security/stealthwatch/tsd-products-support-series-home.html, attached hereto as Exhibit 40; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-guides-list.html, attached hereto as Exhibit 41;

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/hardware/installation/SW_6_9_1_Hardware_Installation_DV_1_2.pdf, attached hereto as Exhibit 42; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-and-configuration-guides-list.html, attached hereto as Exhibit 43; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-programming-reference-guides-list.html, attached hereto as Exhibit 44; https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-routing-switching.html, attached hereto as Exhibit 45.

325. These documents provide instructions, directions and/or require others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '205 Patent, where all the steps of the method claims are performed by either Cisco, its customers, purchasers, users or developers, or some combination thereof. For example, Cisco includes the Stealthwatch System Hardware Installation Guide, which provides instructions and recommendations on how to install and deploy the Accused '205 Products in an infringing manner as shown below.

Placement Considerations

As shown in the figure below, Stealthwatch system products can be strategically deployed to provide optimal coverage of key network segments throughout the network, whether in the internal network, at the perimeter, or in the DMZ.



Placing the SMC

As the management device, the Stealthwatch Management Console (SMC) should be installed at a location on your network that is accessible to all the devices sending data to it.

If you have a failover pair of SMCs, it is recommended that you install the primary SMC and the secondary SMC in separate physical locations. This strategy will enhance a disaster recovery effort should it become necessary.

Placing the Stealthwatch Flow Collector

As collection and monitoring devices, the Stealthwatch Flow Collector for NetFlow appliance and the Stealthwatch Flow Collector for sFlow appliance should be installed at a location on your network that is accessible to the NetFlow or sFlow devices sending the data to a Flow Collector, as well as any devices you plan to use to access the management interface.

Note: When you place a Flow Collector outside a firewall, Lancope recommends that you turn off the setting "Accept traffic from any exporter."

Placing the Stealthwatch Flow Sensor

As a passive monitoring device, the Stealthwatch Flow Sensor can sit at multiple points on your network to observe and record IP activity, thereby protecting network integrity and detecting security breaches. The Flow Sensor features integrated Web-based management systems that facilitate either centralized or remote management and administration.

The Flow Sensor appliance is most effective when placed at critical segments of your corporate network as follows:

- Inside your firewall to monitor traffic and determine if a firewall breach has occurred
- Outside your firewall, monitoring traffic flow to analyze who is threatening your firewall
- At sensitive segments of your network, offering protection from disgruntled employees or hackers with root access
- At remote office locations that constitute vulnerable network extensions
- On your business network for protocol use management (for example, on your transaction services subnet to determine if a hacker is running Telnet or FTP and compromising your customers' financial data)

Placing Other Stealthwatch Products

The only requirement for the placement of other Stealthwatch products, such as the Stealthwatch UDP Director (also known as FlowReplicator), or a VM server containing a Stealthwatch Flow Sensor Virtual Edition (VE), is that they have an unobstructed communication path to the rest of your Stealthwatch products as applicable.

Exhibit 42 at 11-12.

326. As such, Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the '205 Patent.

NINETEENTH CAUSE OF ACTION
(Direct Infringement of the '148 Patent pursuant to 35 U.S.C. § 271(a))

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

328. Cisco has infringed and continues to infringe Claims 1-24 of the '148 Patent in violation of 35 U.S.C. § 271(a).

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

330. Cisco'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.

331. Cisco's infringement includes the manufacture, use, sale, importation and/or offer for sale of Cisco's products and services, including but not limited to the Accused Catalyst Products, the Accused Router Products, the Accused ASA Products, and the Accused Stealthwatch Products, alone or in conjunction with one another (collectively, the "Accused '148 Products").

332. The Accused '148 Products embody the patented invention of the '148 Patent and infringe the '148 Patent because they practice a method comprising:

preprocessing, by a network device, a first rule set and a second rule set;

configuring the network device to process packets in accordance with the first rule set;

receiving, after the preprocessing and the configuring, by the network device, a plurality of packets;

processing, by the network device, a first portion of the plurality of packets in accordance with the first rule set;

signaling the network device to process packets in accordance with the second rule set; and

responsive to the signaling:

ceasing processing of one or more packets;

caching the one or more packets;

reconfiguring the network device to process packets in accordance with the second rule set;

signaling completion of reconfiguration to process packets in accordance with the second rule set; and

responsive to the signaling completion of reconfiguration, processing the one or more cached packets in accordance with the second rule set.

‘148 Patent, Claim 1.

333. The Accused ‘148 Products perform the steps of “preprocessing, by a network device, a first rule set and a second rule set” and “configuring the network device to process packets in accordance with the first rule set.”

334. As shown below, the Accused ‘148 Products “enables policy-based automation from edge to cloud with foundational capabilities,” including “Simplified device deployment, Unified management of wired and wireless networks, Network virtualization and segmentation, Group-based policies, and Context-based analytics.”

The Foundation of Software-Defined Access

Advanced persistent security threats. The exponential growth of Internet of Things (IoT) devices. Mobility everywhere. Cloud adoption. All of these require a network fabric that integrates advanced hardware and software innovations to automate, secure, and simplify customer networks. The goal of this network fabric is to enable customer revenue growth by accelerating the rollout of business services.

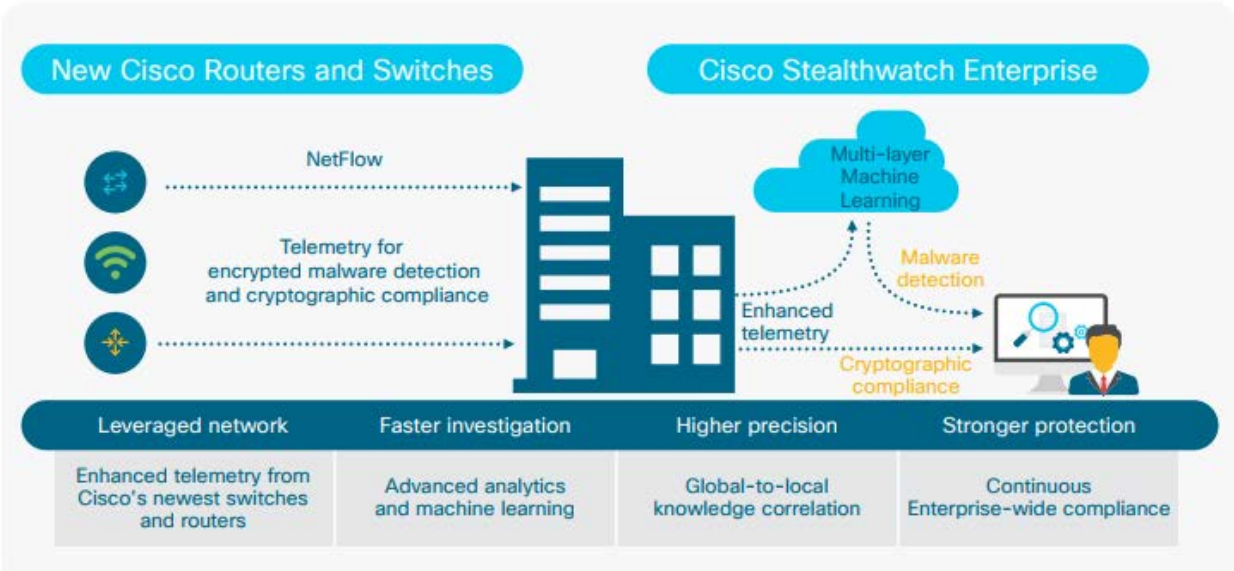
The Cisco Digital Network Architecture (Cisco DNA™) with SD-Access is the network fabric that powers business. It is an open and extensible, software-driven architecture that accelerates and simplifies your enterprise network operations. The programmable architecture frees your IT staff from time-consuming, repetitive network configuration tasks so they can focus instead on innovation that positively transforms your business. SD-Access enables policy-based automation from edge to cloud with foundational capabilities. These include:

- Simplified device deployment
- Unified management of wired and wireless networks
- Network virtualization and segmentation
- Group-based policies
- Context-based analytics

(Cisco Catalyst 9300 Series Switches). https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.pdf, attached hereto as Exhibit 16, at 1.

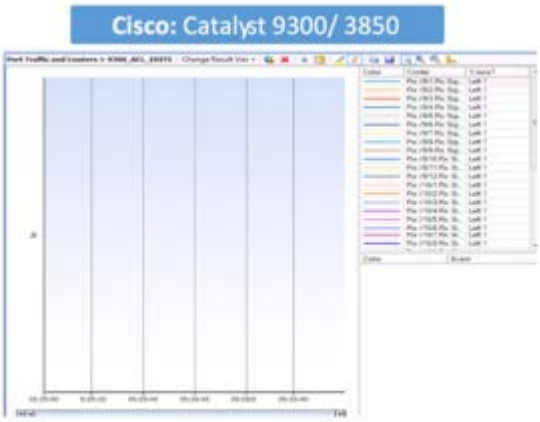
335. The Accused '148 Products perform the steps of "receiving, after the preprocessing and the configuring, by the network device, a plurality of packets" and "processing, by the network device, a first portion of the plurality of packets in accordance with the first rule set." As shown below, the Accused '148 Products collect, store, and analyze both traditional flow data and intraflow metadata and "[o]btain contextual threat intelligence with real-time analysis correlated with user and device information." (Cisco Encrypted Traffic Analytics White Paper). https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25, at 2-4.

Figure 2. Encrypted Traffic Analytics – technical solution overview



Id. at 3.

336. The Accused '148 Products perform the steps of "signaling the network device to process packets in accordance with the second rule set," "responsive to the signaling: ceasing processing of one or more packets; caching the one or more packets; reconfiguring the network device to process packets in accordance with the second rule set; signaling completion of reconfiguration to process packets in accordance with the second rule set," and "responsive to the signaling completion of reconfiguration, processing the one or more cached packets in accordance with the second rule set." As shown below, the Accused '148 Products "support high-speed policy edits (Adds/Deletes) with efficient resource allocation for scale, and secure implementation. With features such as 'ACL Label-Sharing' and 'Hitless ACL updates,' the switches demonstrated programming of policy to the network without being compromised. A table-stakes requirement for dynamic policy based automation." https://blogs.cisco.com/enterprise/wired-infrastructure-optimized-and-secure-switching-resources, attached hereto as Exhibit 46, at 5.



Miercom-Report-Cisco-vs-Huawei-Network-Architecture-DR170921G.pdf, attached hereto as Exhibit 23, at 22.

337. The Accused '148 Products support "UADP 2.0 Application-Specific Integrated Circuit (ASIC) with programmable pipeline and microengine capabilities, along with template-based, configurable allocation of Layer 2 and Layer 3 forwarding, Access Control Lists (ACLs), and Quality of Service (QoS) entries." https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.pdf, attached hereto as Exhibit 16, at 2.

338. The Accused '148 Products "are based on UADP 2.0 the second generation of UADP ASIC that comprises of 7.46 Billion transistors – one for every human being on this planet! In addition to programmability improvements of the ASIC pipeline, we have also introduced flexible tables on UADP 2.0 to enable universal deployments of the Catalyst 9000 Switches. UADP 2.0 turns Catalyst 9K into a Swiss Army Knife style Switch by customization of available table (SRAM/TCAM) resources based on customer deployment requirements. Cisco currently offers four fully tested templates to cover the all places in the network." https://communities.cisco.com/community/technology/enterprise_networks/blog/2017/06/20/cisco-catalyst-9000-series-of-switches-maximize-your-network-mileage, attached hereto as

Exhibit 47, at 1.

339. The Accused '148 Products includes Transactional-Commit Modeling, which is "a new feature for rule updation" of ACL rules. With Transactional-Commit Modeling, "a rule update is applied after the rule compilation is completed; without affecting the rule matching performance. With the legacy model, rule updates take effect immediately but rule matching slows down during the rule compilation period. This feature is useful to prevent potential packet drops during large compilation of rules under high traffic conditions."

Transactional-Commit Model

The ASA rule-engine supports a new feature for rule updation called the Transactional-Commit Model. When this feature is enabled, a rule update is applied after the rule compilation is completed; without affecting the rule matching performance. With the legacy model, rule updates take effect immediately but rule matching slows down during the rule compilation period. This feature is useful to prevent potential packet drops during large compilation of rules under high traffic conditions. This feature is also useful to reduce the rule compilation time under two specific patterns of configurations:

- Preventing packet drops while compiling large rules during high traffic rates.
- Reducing rule compilation time while updating a large number of similar rules.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/firewall/asa_91_firewall_config/access_rules.html, attached hereto as Exhibit 30, at 6-4.

340. As a result of Cisco'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. Cisco's infringement of the '148 Patent has injured and continues to injure Centripetal in an amount to be proven at trial.

342. Cisco has willfully infringed each of the Asserted Patents. Centripetal is informed and believes that Cisco had knowledge of the Asserted Patents through various channels and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

343. On or around 2014, Centripetal partnered with ThreatGRID, a company which included threat intelligence technology which Centripetal integrated with their patented products that used some of the Asserted Patents. Cisco later acquired ThreatGRID in 2016.

Centripetal is informed and believes that Cisco gained increased exposure to Centripetal's patented technology as a result of the acquisition of ThreatGRID. https://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/threatgrid.html, attached hereto as Exhibit 31.

344. Centripetal is further informed and believes that, on or around January 2016, Cisco requested an introduction to Centripetal through a third party, Granite Hill Capital Partners. Later, Centripetal received a point of contact introduction to Cisco from Granite Hill Capital Partners.

345. In 2016, Cisco invited Centripetal to participate in Cisco Live, which is Cisco's partner conference – in which Centripetal was asked to demonstrate its technology in Cisco's "Security Partner Village" booth. On or around June 2016, Centripetal attended the Cisco Live conference and demonstrated its patented technology, including the RuleGATE Threat Intelligence Gateway product which encompasses at least some of the Asserted Patents. Cisco currently lists Centripetal on its website located at www.cisco.com, as part of a "partner ecosystem" whose "[t]hreat intelligence platforms" use Threat Grid. https://www.cisco.com/c/en/us/products/security/threat-grid/integrations.html#~stickynav=2, attached hereto as Exhibit 32, at 3.

346. Cisco thus knew or, in the alternative, was willfully blind to Centripetal's technology and its Asserted Patents. Cisco's infringement of the '148 Patent is egregious because despite this knowledge, Centripetal is informed and believes that Cisco deliberately copied Centripetal's patented technology, which it implemented into its products and services, such as Centripetal's CleanINTERNET service and Threat Intelligence Gateway, including the RuleGATE 2000. The blatant copying of Centripetal's patented technology and disregard for

Centripetal's patent rights with an objectively high likelihood of infringement is egregious behavior warranting a finding of willful infringement and enhanced damages.

347. Centripetal is informed and believes that Cisco has undertaken no efforts to design these products or services around the '148 Patent to avoid infringement despite Cisco's knowledge and understanding that its products and services infringe the '148 Patent. As such, Cisco has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '148 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.

TWENTIENTH CAUSE OF ACTION
(Indirect Infringement of the '148 Patent pursuant to 35 U.S.C. § 271(b))

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. Cisco has induced and continues to induce infringement of one or more claims of the '148 Patent under 35 U.S.C. § 271(b).

350. In addition to directly infringing the '148 Patent, Cisco indirectly infringes the '148 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '148 Patent, where all the steps of the method claims are performed by either Cisco, its customers, purchasers, users or developers, or some combination thereof. Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the '148 Patent, including Claims 1-8.

351. Cisco knowingly and actively aided and abetted the direct infringement of the '148 Patent by instructing and encouraging its customers, purchasers, users and developers to use the '148 Accused Products. Such instructions and encouragement include, but are not limited to, advising third parties to use the '148 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '148 Patent, specifically through the use of the Accused Catalyst Products, the Accused Router Products, and the Accused Stealthwatch Products, alone or in conjunction with one another, and by advertising and promoting the use of the '148 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '148 Accused Products in an infringing manner.

352. Cisco updates and maintains an HTTP site with Cisco's quick start guides, administration guides, user guides, operating instructions, blogs, white papers, data sheets and training certification programs which cover in depth aspects of operating Cisco's offerings. *See* https://www.cisco.com/c/en/us/support/switches/catalyst-9300-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 34; https://www.cisco.com/c/en/us/support/switches/catalyst-9400-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 35; https://www.cisco.com/c/en/us/support/switches/catalyst-9500-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 36; https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.pdf, attached hereto as Exhibit 16; *see also* https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/datasheet-c78-739053.pdf, attached hereto as Exhibit 17;

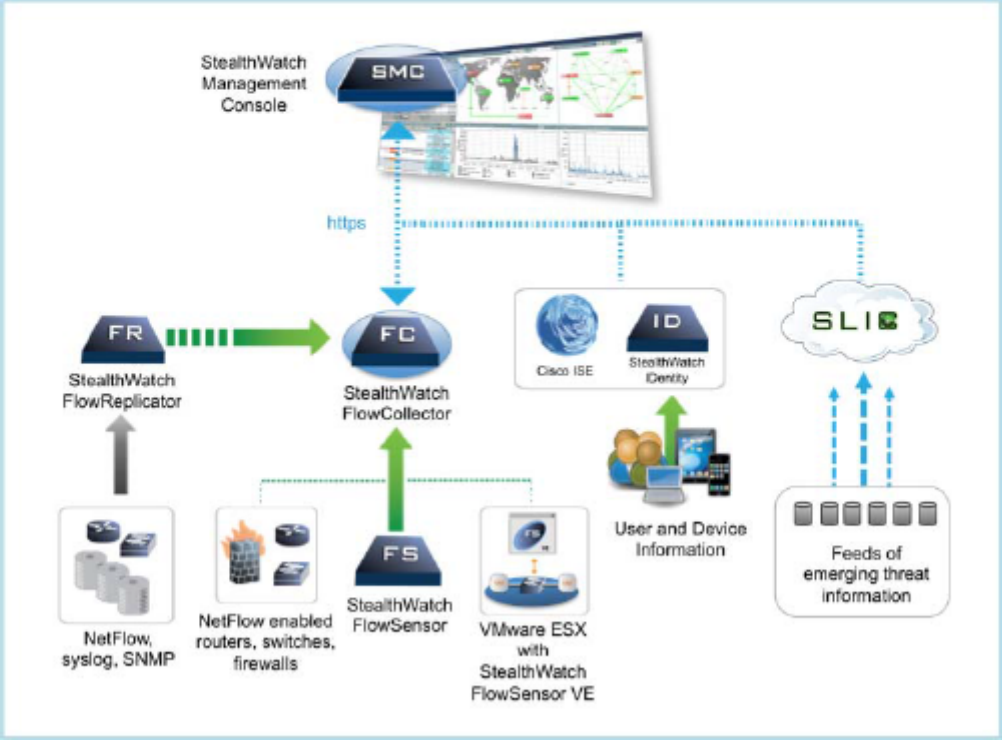
https://www.cisco.com/c/en/us/support/routers/index.html, attached hereto as Exhibit 37; *see also* https://www.cisco.com/c/dam/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/at-a-glance-c45-612993.pdf, attached hereto as Exhibit 18; *see also* https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/datasheet-c78-732542.pdf, attached hereto as Exhibit 19; https://blogs.cisco.com/enterprise/cisco-traffic-analysis-encrypted-threat-analytics, attached hereto as Exhibit 38; https://communities.cisco.com/docs/DOC-76964, attached hereto as Exhibit 39; https://www.cisco.com/c/en/us/support/security/stealthwatch/tsd-products-support-series-home.html, attached hereto as Exhibit 40; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-guides-list.html, attached hereto as Exhibit 41; https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/hardware/installation/SW_6_9_1_Hardware_Installation_DV_1_2.pdf, attached hereto as Exhibit 42; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-and-configuration-guides-list.html, attached hereto as Exhibit 43; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-programming-reference-guides-list.html, attached hereto as Exhibit 44; https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-routing-switching.html, attached hereto as Exhibit 45.

353. These documents provide instructions, directions and/or require others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the ‘148 Patent, where all the steps of the method claims are performed by either Cisco, its customers,

purchasers, users or developers, or some combination thereof. For example, Cisco includes the Stealthwatch System Hardware Installation Guide, which provides instructions and recommendations on how to install and deploy the Accused '148 Products in an infringing manner as shown below.

Placement Considerations

As shown in the figure below, Stealthwatch system products can be strategically deployed to provide optimal coverage of key network segments throughout the network, whether in the internal network, at the perimeter, or in the DMZ.



Placing the SMC

As the management device, the Stealthwatch Management Console (SMC) should be installed at a location on your network that is accessible to all the devices sending data to it.

If you have a failover pair of SMCs, it is recommended that you install the primary SMC and the secondary SMC in separate physical locations. This strategy will enhance a disaster recovery effort should it become necessary.

Placing the Stealthwatch Flow Collector

As collection and monitoring devices, the Stealthwatch Flow Collector for NetFlow appliance and the Stealthwatch Flow Collector for sFlow appliance should be installed at a location on your network that is accessible to the NetFlow or sFlow devices sending the data to a Flow Collector, as well as any devices you plan to use to access the management interface.

Note: When you place a Flow Collector outside a firewall, Lancope recommends that you turn off the setting "Accept traffic from any exporter."

Placing the Stealthwatch Flow Sensor

As a passive monitoring device, the Stealthwatch Flow Sensor can sit at multiple points on your network to observe and record IP activity, thereby protecting network integrity and detecting security breaches. The Flow Sensor features integrated Web-based management systems that facilitate either centralized or remote management and administration.

The Flow Sensor appliance is most effective when placed at critical segments of your corporate network as follows:

- Inside your firewall to monitor traffic and determine if a firewall breach has occurred
- Outside your firewall, monitoring traffic flow to analyze who is threatening your firewall
- At sensitive segments of your network, offering protection from disgruntled employees or hackers with root access
- At remote office locations that constitute vulnerable network extensions
- On your business network for protocol use management (for example, on your transaction services subnet to determine if a hacker is running Telnet or FTP and compromising your customers' financial data)

Placing Other Stealthwatch Products

The only requirement for the placement of other Stealthwatch products, such as the Stealthwatch UDP Director (also known as FlowReplicator), or a VM server containing a Stealthwatch Flow Sensor Virtual Edition (VE), is that they have an unobstructed communication path to the rest of your Stealthwatch products as applicable.

Exhibit 42 at 11-12.

354. As such, Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the '148 Patent.

TWENTY-FIRST CAUSE OF ACTION
(Patent Infringement of the '856 Patent)

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

356. Cisco has infringed and continues to infringe Claims 1-25 of the '856 Patent in violation of 35 U.S.C. § 271(a).

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

358. Cisco'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.

359. Cisco's infringement includes the manufacture, use, sale, importation and/or offer for sale of Cisco's products and services, including but not limited to the Accused Catalyst Products, the Accused Router Products, the Accused ASA Products, and the Accused Stealthwatch Products, alone or in conjunction with one another (collectively, the "Accused '856 Products").

360. For example, Defendants have infringed, and continue to infringe, at least claim 1 of the '856 patent:

> 1. A method, comprising:
>
> receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat

indicators comprises a domain name identified as a network threat;

identifying packets comprising unencrypted data;

identifying packets comprising encrypted data;

determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;

filtering, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:

packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators of the plurality of network-threat indicators; and

the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and

routing, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

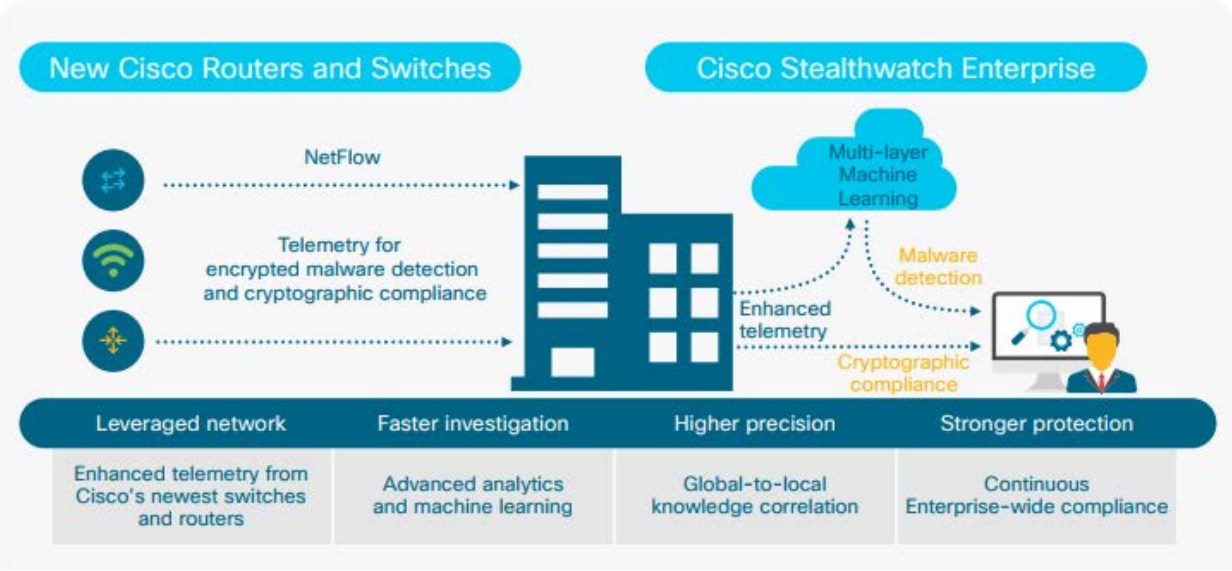
‘856 Patent, Claim 1.

361. The Accused ‘856 Products practice “receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprises a domain name identified as a network threat.”

362. As shown below, the Accused ‘856 Products collect, store, and analyze both traditional flow data and intraflow metadata and “[o]btain contextual threat intelligence with

real-time analysis correlated with user and device information." *See* Cisco Encrypted Traffic Analytics White Paper, available at https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf., attached hereto as Exhibit 25 at 2-4.

Figure 2. Encrypted Traffic Analytics – technical solution overview



Id. at 3.

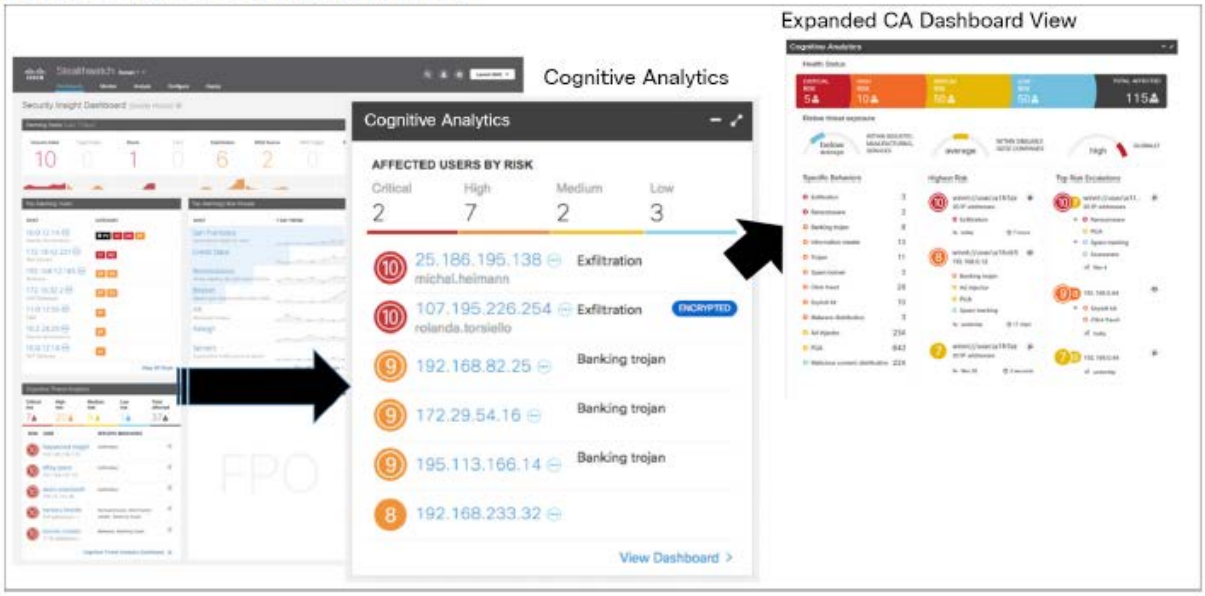
363. The Accused '856 Products "extract[] four main data elements: the sequence of packet lengths and times, the byte distribution, TLS-specific features and the initial data packet. Cisco's unique Application-Specific Integrated Circuit (ASIC) architecture provides the ability to extract these data elements without slowing down the data network," which includes the Initial Data Packet ("IDP"). *See* Cisco Encrypted Traffic Analytics White Paper, available at https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25 at 4. "IDP is used to obtain packet data from the first packet of a flow. It allows extraction of interesting data such as an HTTP URL, DNS hostname/address and other

data elements. The TLS handshake is composed of several messages that contain interesting, unencrypted metadata used to extract data elements such as cipher suites, TLS versions and the client's public key length." *Id.*

364. The Accused '856 Products include the "Stealthwatch Management Console (SMC) [which] provides a view of affected users identified by risk type. An expanded dashboard provides detailed information regarding the top risk escalations and relative threat exposure." As shown below, the information includes domain names identified as threats.

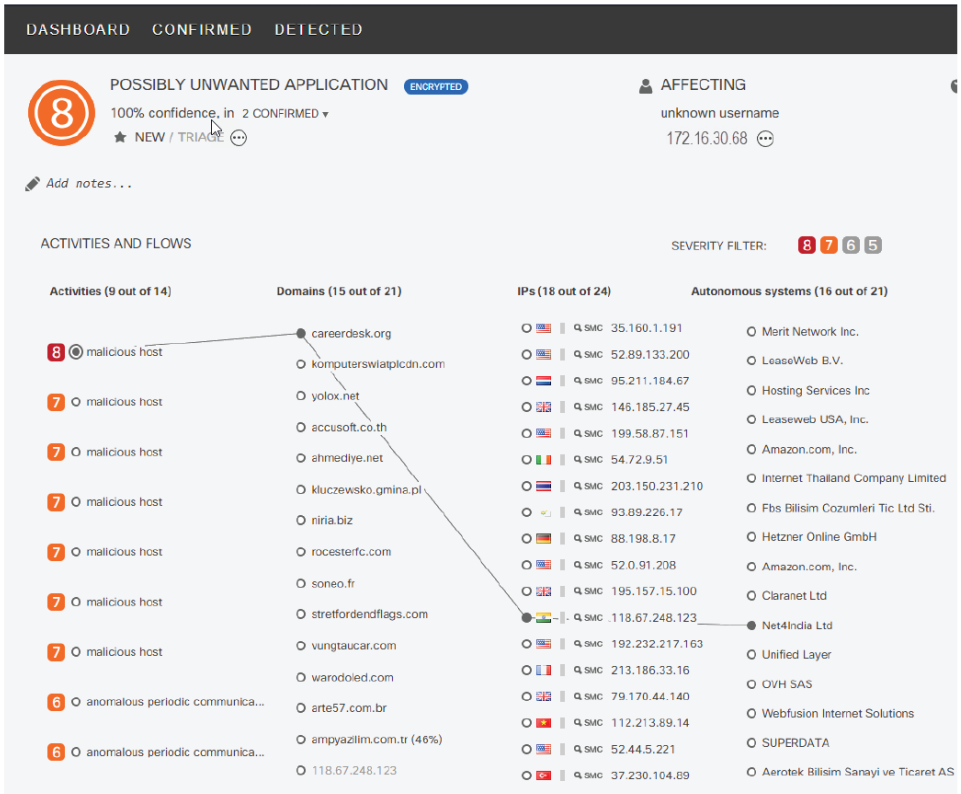
The Security Insight dashboard on the Stealthwatch Management Console (SMC) provides a view of affected users identified by risk type. An expanded dashboard provides detailed information regarding the top risk escalations and relative threat exposure. Table 3 lists some high-risk threats that use encrypted command and control communications.

Figure 4. Stealthwatch security insight dashboard



See Cisco Encrypted Traffic Analytics White Paper, available at https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25 at 6.

Figure 7 *Malware in encrypted medical traffic*



See Encrypted Traffic Analytics Deployment Guide, available at https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Encrypted-Traffic-Analytics-Deployment-Guide-2017DEC.pdf, attached hereto as Exhibit 33 at 14.

365. The Accused '856 Products practice "identifying packets comprising unencrypted data" and "identifying packets comprising encrypted data." As shown below, the Accused '856 Products monitor "all traffic both encrypted and unencrypted… and the ETA and NetFlow data exported to the Stealthwatch Flow Collector and perimeter traffic sent to the Cognitive Threat Analytics cloud for further analysis."

Use Case 1–Branch Crypto Audit & Malware Detection–Internet Edge Only

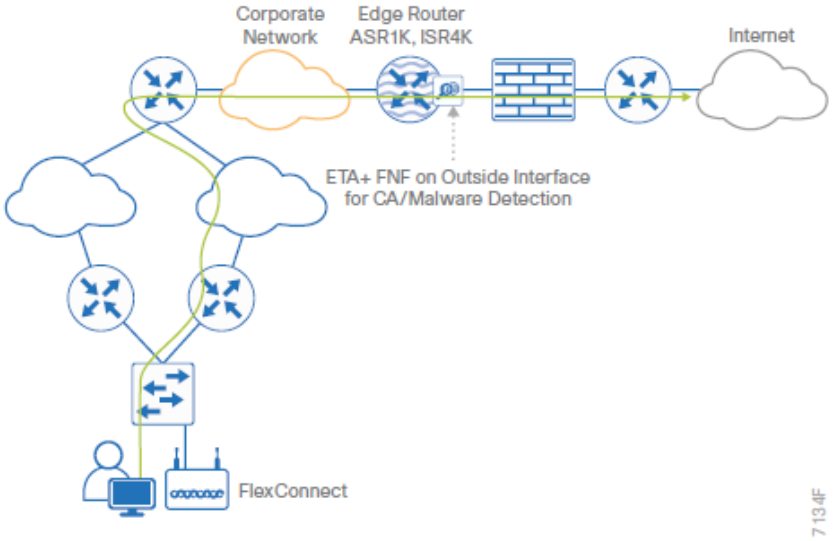
In this deployment scenario in Figure 14, only endpoint traffic that is destined for the Internet is monitored. ETA and FNF are both configured on the Ethernet interface of an ISR4K or more likely, an ASR1K Internet Edge router connected to a corporate firewall. Here, all traffic both encrypted and unencrypted is monitored and the ETA and NetFlow data exported to the Stealthwatch Flow Collector and perimeter traffic sent to the Cognitive Threat Analytics cloud for further analysis.

This use case allows for all Internet bound traffic from the branch as well as campus and data center to be monitored. A cryptographic assessment for all encrypted traffic leaving the enterprise is possible as well as analysis for malware in the Cognitive Threat Analytics cloud. Due to the placement of the ETA and FNF, monitoring and cryptographic assessment of internal traffic between enterprise endpoints and servers is not possible, because monitoring is performed only at the edge.

When considering this deployment model, it will be important to correctly size the Stealthwatch Flow Collector to which the ETA and NetFlow records will be exported as well as ensuring that the Internet Edge Router is correctly sized and capable of processing the required flows per second.

This deployment scenario obviously conserves branch WAN bandwidth, because no ETA exports are occurring at the branch. It also reduces the possible requirement for more Flow Collectors, depending on the number of branches, along with the licensing associated with monitoring all branch flows regardless of destination.

Figure 14 *Branch crypto audit/malware detection at Internet Edge*



Id. at 25.

366. As shown below, "Cisco Stealthwatch harnesses the power of network telemetry—including but not limited to NetFlow, IPFIX, proxy logs, and deep packet inspection on raw packets—in order to provide advanced network visibility, security intelligence, and analytics. This visibility allows a Stealthwatch database record to be maintained for every communication that traverses a network device. This aggregated data can

be analyzed in order to identify hosts with suspicious patterns of activity. Stealthwatch has different alarm categories using many different algorithms watching behavior and identifying suspicious activity. Stealthwatch leverages NetFlow data from network devices throughout all areas of the network—access, distribution, core, data center, and edge—providing a concise view of normal traffic patterns throughout and alerting when policies defining abnormal behavior are matched."

Cisco Stealthwatch

Cisco Stealthwatch harnesses the power of network telemetry—including but not limited to NetFlow, IPFIX, proxy logs, and deep packet inspection on raw packets—in order to provide advanced network visibility, security intelligence, and analytics. This visibility allows a Stealthwatch database record to be maintained for every communication that traverses a network device. This aggregated data can be analyzed in order to identify hosts with suspicious patterns of activity. Stealthwatch has different alarm categories using many different algorithms watching behavior and identifying suspicious activity. Stealthwatch leverages NetFlow data from network devices throughout all areas of the network—access, distribution, core, data center, and edge—providing a concise view of normal traffic patterns throughout and alerting when policies defining abnormal behavior are matched.

For more information, see the Cisco Stealthwatch web page.

Id. at 7.

367. The Accused '856 Products include "intraflow metadata, called *Encrypted Traffic Analytics* (ETA), [which] is derived by using new data elements or telemetry that are independent of protocol details, such as the lengths and arrival times of packets within a flow. These data elements have the property of applying equally well to both encrypted and unencrypted flows. ETA focuses on identifying malware communications in encrypted traffic through passive monitoring, the extraction of relevant data elements, and supervised machine learning with cloud based global visibility. ETA extracts three main data elements: the initial data packet, the sequence of packet length and times, and TLS-specific features." *See* Encrypted Traffic Analytics Deployment Guide, available at CVD-Encrypted-Traffic-Analytics-Deployment-Guide-2017DEC.pdf, attached hereto as Exhibit 33 at 1.

Appendix A: ETA Data Elements

Data Element Name	Description
Sequence of Packet Lengths and Times	An array of LENGTH values followed by an array of INTERARRIVAL TIME values describing the first N packets of a flow that carry application payload. Each LENGTH is encoded as a 16-bit integer to form a 20-byte array. Immediately following this, each INTERARRIVAL TIME is encoded as a 16-bit integer to form another 20-byte array.
Initial data packet	The content of the first packet of this flow that contains actual payload data, starting at the beginning of the IP header.
TLS records	An array of LENGTH values, followed by an array of INTERARRIVAL TIME values, followed by an array of CONTENT TYPE values, followed by an array of HANDSHAKE TYPE values. These arrays describe the first N records of a TLS flow.
TLS record lengths	A sequence of record lengths for up to the first N records of a TLS flow.
TLS record times	A sequence of TLS interarrival times for up to the first N records of a TLS flow.
TLS content types	A sequence of ContentType values for up to the first N records of a TLS flow.
TLS handshake types	A sequence of HandshakeType values for up to the first N records of a TLS flow.
TLS cipher suites	A list of up to N cipher suites offered by the client, or selected by the server in a TLS flow.
TLS extensions	An array of LENGTH values followed by an array of EXTENSION TYPE values describing the TLS extensions observed in the Hello message for a TLS flow.
TLS extension lengths	A list of extension lengths for up to the first N TLS extensions observed in the TLS Hello message for a flow.
TLS extension types	A list of extension types for up to the first N TLS extensions observed in the TLS Hello message for a flow.
TLS version	The TLS version number observed in the TLS Hello message for a flow.
TLS key length	The length of the client key observed in the TLS ClientKeyExchange message.
TLS session ID	The session ID value observed (if any) in the TLS Hello message for a flow.
TLS random	The random value observed in the TLS Hello message for this flow.

Id. at 60.

368. The Accused '856 Products practice "determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators." The Accused '856 Products include Crypto Audit, which "is the capability of viewing/reporting and eventually alerting and alarming on the crypto fields in the Stealthwatch database. The crypto audit functionality provides detailed information about the cipher suites used for TLS communications, including the encryption version, key exchange, key length, cipher suite,

authentication algorithm, and hash used." *See* Encrypted Traffic Analytics Deployment Guide, available at https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Encrypted-Traffic-Analytics-Deployment-Guide-2017DEC.pdf, attached hereto as Exhibit 33 at 4.

369. As shown below, "[w]ith the crypto audit functionality enabled by ETA, the unencrypted metadata in the Client Hello and Client Key Exchange messages provides information that can be used to make inferences about the client's Transport Layer Security (TLS) library and the cipher suites used. The collection of this information begins with the *initial data packet* (IDP), or first packet of the flow, and continues through subsequent messages comprising the TLS handshake. This data is then exported by the device via NetFlow and collected at the Stealthwatch Flow Collector (FC). Once collected, these records can be queried by Stealthwatch Management Console (SMC) for analysis. These flow records can be collected by a Stealthwatch Flow Collector over a period of time and subsequently filtered, searched through, and reported on at the Stealthwatch Management Console for auditing purposes ensuring that the most secure cipher suites are used to secure confidential information as well as providing evidence of regulatory compliance." *Id.* at 4.

Crypto Audit

Crypto audit is the capability of viewing/reporting and eventually alerting and alarming on the crypto fields in the Stealthwatch database. The crypto audit functionality provides detailed information about the cipher suites used for TLS communications, including the encryption version, key exchange, key length, cipher suite, authentication algorithm, and hash used.

With the crypto audit functionality enabled by ETA, the unencrypted metadata in the Client Hello and Client Key Exchange messages provides information that can be used to make inferences about the client's Transport Layer Security (TLS) library and the cipher suites used. The collection of this information begins with the *initial data packet* (IDP), or first packet of the flow, and continues through subsequent messages comprising the TLS handshake. This data is then exported by the device via NetFlow and collected at the Stealthwatch Flow Collector (FC). Once collected, these records can be queried by Stealthwatch Management Console (SMC) for analysis.

These flow records can be collected by a Stealthwatch Flow Collector over a period of time and subsequently filtered, searched through, and reported on at the Stealthwatch Management Console for auditing purposes ensuring that the most secure cipher suites are used to secure confidential information as well as providing evidence of regulatory compliance.

Id. at 4.

370. The Accused '856 Products practice "filtering, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules: packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators of the plurality of network-threat indicators; and the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators."

371. The Accused '856 Products include "intraflow metadata, called *Encrypted Traffic Analytics* (ETA), [which] is derived by using new data elements or telemetry that are independent of protocol details, such as the lengths and arrival times of packets within a flow. These data elements have the property of applying equally well to both encrypted and unencrypted flows. ETA focuses on identifying malware communications in encrypted traffic through passive monitoring, the extraction of relevant data elements, and supervised machine learning with cloud based global visibility. ETA extracts three main data elements: the initial data packet, the sequence of packet length and times, and TLS-specific features." *See* Encrypted Traffic Analytics Deployment Guide, available at https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Encrypted-Traffic-Analytics-Deployment-Guide-2017DEC.pdf, attached hereto as Exhibit 33 at 1.

Appendix A: ETA Data Elements

Data Element Name	Description
Sequence of Packet Lengths and Times	An array of LENGTH values followed by an array of INTERARRIVAL TIME values describing the first N packets of a flow that carry application payload. Each LENGTH is encoded as a 16-bit integer to form a 20-byte array. Immediately following this, each INTERARRIVAL TIME is encoded as a 16-bit integer to form another 20-byte array.
Initial data packet	The content of the first packet of this flow that contains actual payload data, starting at the beginning of the IP header.
TLS records	An array of LENGTH values, followed by an array of INTERARRIVAL TIME values, followed by an array of CONTENT TYPE values, followed by an array of HANDSHAKE TYPE values. These arrays describe the first N records of a TLS flow.
TLS record lengths	A sequence of record lengths for up to the first N records of a TLS flow.
TLS record times	A sequence of TLS interarrival times for up to the first N records of a TLS flow.
TLS content types	A sequence of ContentType values for up to the first N records of a TLS flow.
TLS handshake types	A sequence of HandshakeType values for up to the first N records of a TLS flow.
TLS cipher suites	A list of up to N cipher suites offered by the client, or selected by the server in a TLS flow.
TLS extensions	An array of LENGTH values followed by an array of EXTENSION TYPE values describing the TLS extensions observed in the Hello message for a TLS flow.
TLS extension lengths	A list of extension lengths for up to the first N TLS extensions observed in the TLS Hello message for a flow.
TLS extension types	A list of extension types for up to the first N TLS extensions observed in the TLS Hello message for a flow.
TLS version	The TLS version number observed in the TLS Hello message for a flow.
TLS key length	The length of the client key observed in the TLS ClientKeyExchange message.
TLS session ID	The session ID value observed (if any) in the TLS Hello message for a flow.
TLS random	The random value observed in the TLS Hello message for this flow.

Id. at 60.

372. As shown below, the Accused '856 Products "can enable ETA on switch or router interfaces and passively monitor encrypted flows. During the initial conversation between the POS terminal and payment gateway or the payment gateway and the payment processor, the IDP initiating the TLS handshake and several subsequent unencrypted messages are collected. Once exported to the NetFlow collector, the unencrypted metadata can be used to collect information regarding the cipher suite, version, and client's public key length as reported by the cipher suite. Additionally, all traffic destined to cloud-based services will be analyzed in the Cognitive Threat Analytics cloud for any suspicious activity." *Id.* at 16.

Solution

With Catalyst 9K access switches or ISR4K/ASR1K routers running IOS-XE 16.6.2 and Stealthwatch 6.9.2, you can enable ETA on switch or router interfaces and passively monitor encrypted flows. During the initial conversation between the POS terminal and payment gateway or the payment gateway and the payment processor, the IDP initiating the TLS handshake and several subsequent unencrypted messages are collected. Once exported to the NetFlow collector, the unencrypted metadata can be used to collect information regarding the cipher suite, version, and client's public key length as reported by the cipher suite. Additionally, all traffic destined to cloud-based services will be analyzed in the Cognitive Threat Analytics cloud for any suspicious activity.

Id. at 16.

373. The Accused '856 Products include "intraflow metadata, called *Encrypted Traffic Analytics* (ETA), [which] is derived by using new data elements or telemetry that are independent of protocol details, such as the lengths and arrival times of packets within a flow. These data elements have the property of applying equally well to both encrypted and unencrypted flows. ETA focuses on identifying malware communications in encrypted traffic through passive monitoring, the extraction of relevant data elements, and supervised machine learning with cloud based global visibility. ETA extracts three main data elements: the initial data packet, the sequence of packet length and times, and TLS-specific features." *See* Encrypted Traffic Analytics Deployment Guide, available at https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Encrypted-Traffic-Analytics-Deployment-Guide-2017DEC.pdf, attached hereto as Exhibit 33 at 1.

Appendix A: ETA Data Elements

Data Element Name	Description
Sequence of Packet Lengths and Times	An array of LENGTH values followed by an array of INTERARRIVAL TIME values describing the first N packets of a flow that carry application payload. Each LENGTH is encoded as a 16-bit integer to form a 20-byte array. Immediately following this, each INTERARRIVAL TIME is encoded as a 16-bit integer to form another 20-byte array.
Initial data packet	The content of the first packet of this flow that contains actual payload data, starting at the beginning of the IP header.
TLS records	An array of LENGTH values, followed by an array of INTERARRIVAL TIME values, followed by an array of CONTENT TYPE values, followed by an array of HANDSHAKE TYPE values. These arrays describe the first N records of a TLS flow.
TLS record lengths	A sequence of record lengths for up to the first N records of a TLS flow.
TLS record times	A sequence of TLS interarrival times for up to the first N records of a TLS flow.
TLS content types	A sequence of ContentType values for up to the first N records of a TLS flow.
TLS handshake types	A sequence of HandshakeType values for up to the first N records of a TLS flow.
TLS cipher suites	A list of up to N cipher suites offered by the client, or selected by the server in a TLS flow.
TLS extensions	An array of LENGTH values followed by an array of EXTENSION TYPE values describing the TLS extensions observed in the Hello message for a TLS flow.
TLS extension lengths	A list of extension lengths for up to the first N TLS extensions observed in the TLS Hello message for a flow.
TLS extension types	A list of extension types for up to the first N TLS extensions observed in the TLS Hello message for a flow.
TLS version	The TLS version number observed in the TLS Hello message for a flow.
TLS key length	The length of the client key observed in the TLS ClientKeyExchange message.
TLS session ID	The session ID value observed (if any) in the TLS Hello message for a flow.
TLS random	The random value observed in the TLS Hello message for this flow.

Id. at 60.

374. The Accused '856 Products practice "routing, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators."

375. As shown below, the Accused '856 Products include Malware Detection, which "can also be used to detect malware within the encrypted traffic without the need to decrypt the traffic when Cisco Stealthwatch is integrated with Cognitive Threat Analytics. When combining Flexible NetFlow and DNS information along with the ETA metadata found in the IDP, other ETA data elements such as Sequence of Packet Length and Times (SPLT) provide a

unique and valuable means for identifying malware through the detection of suspicious traffic." *See* Encrypted Traffic Analytics Deployment Guide, available at https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Encrypted-Traffic-Analytics-Deployment-Guide-2017DEC.pdf, attached hereto as Exhibit 33at 4.

Malware Detection

When implementing ETA, in addition to cryptographic assessment, the metadata collected can also be used to detect malware within the encrypted traffic without the need to decrypt the traffic when Cisco Stealthwatch is integrated with Cognitive Threat Analytics. When combining Flexible NetFlow and DNS information along with the ETA metadata found in the IDP, other ETA data elements such as Sequence of Packet Length and Times (SPLT) provide a unique and valuable means for identifying malware through the detection of suspicious traffic.

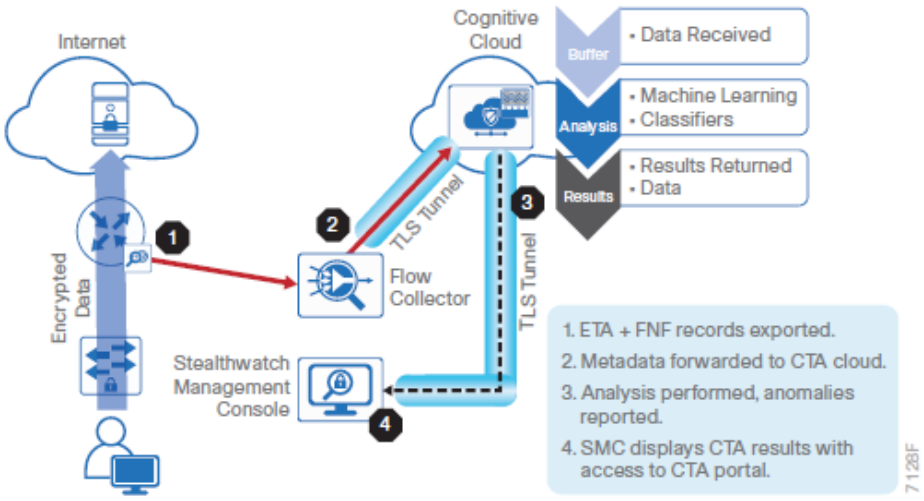
SPLT telemetry is composed of a set of two parameters describing each of the first 10 packets of a flow—the length of the application payload in that packet and the inter-arrival time from the previous packet. Only packets that carry some application payload are considered; the rest (such as SYN or SYN/ACK) are ignored. The SPLT provides visibility beyond the first packet of the encrypted flows. The analysis of the metadata contained in the IDP and SPLT greatly enhance the accuracy of malware detection in the Cognitive Threat Analytics cloud.

Although all endpoint traffic is monitored and records exported to the Stealthwatch Flow Collectors, by default, only traffic crossing the enterprise network perimeter (i.e., Internet-bound) and outside of the enterprise address space as well as all DNS queries regardless of domain, are sent by the Stealthwatch flow collector to the CTA cloud for further analysis. All communications between the flow collector and the CTA cloud as well as from the CTA cloud to the SMC is sent in an encrypted TLS tunnel as seen below.

Id. at 4.

376. As shown below, the Accused '856 Products send "FNF and ETA fields are immediately sent to the CTA cloud for analysis. Initially, there will be a brief "training" period in which analysis results may not be displayed at the SMC. This is completely normal. Once this initial period of a day or two is complete, CTA analyzes the new encrypted traffic data elements within the ETA records by applying machine learning and statistical modeling with existing classifiers. The global risk map and Encrypted Traffic Analytics data elements reinforce each other in the Cognitive Threat Analytics engine. Rather than decrypting the traffic, Stealthwatch with Cognitive Threat Analytics uses machine-learning algorithms to pinpoint malicious patterns such as data exfiltration in encrypted traffic to help identify threats and improve incident response times." *Id.* at 5.

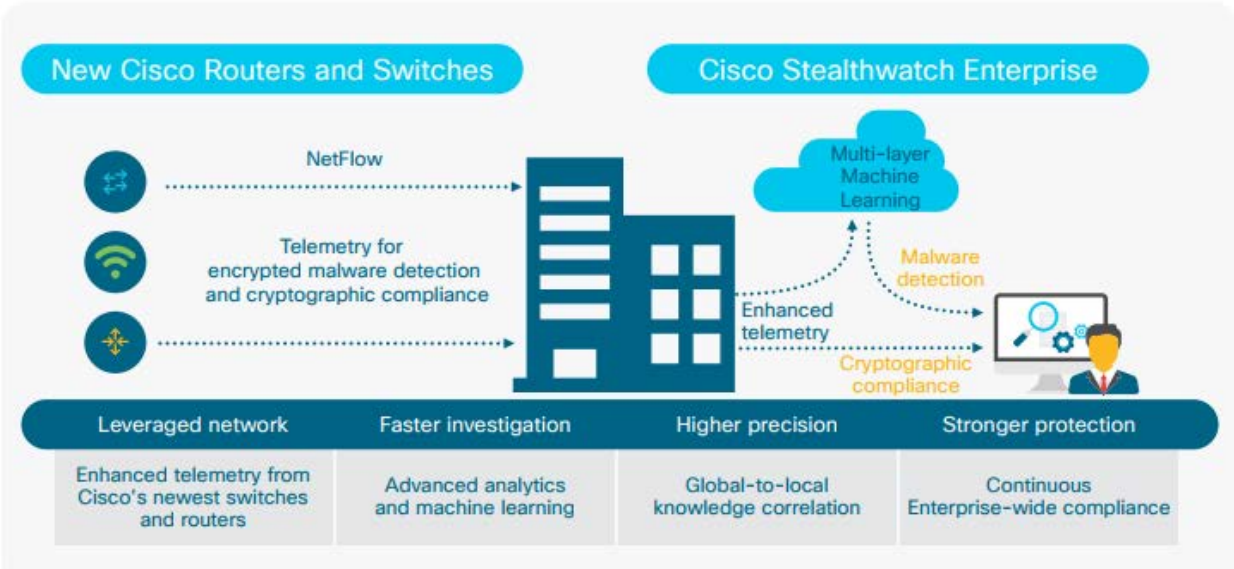
Figure 1 *ETA malware detection in Cognitive Threat Analytics cloud*



Id. at 5.

377. As shown below, the Accused '856 Products route packets for further analysis based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

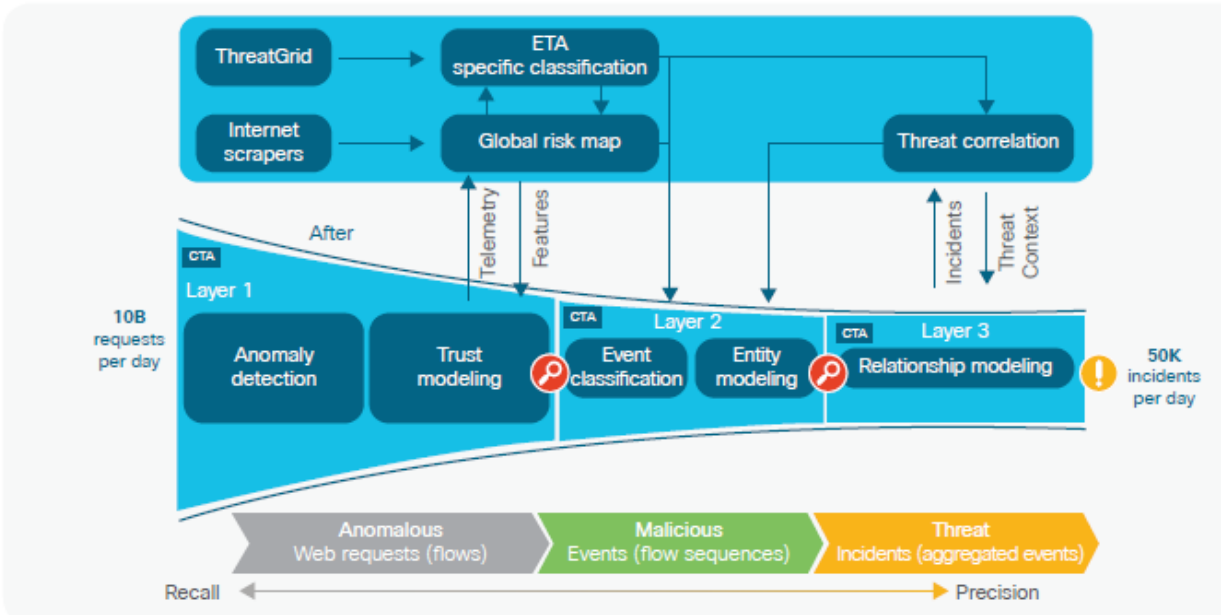
Figure 2. Encrypted Traffic Analytics – technical solution overview



See Cisco Encrypted Traffic Analytics White Paper, available at https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf, attached hereto as Exhibit 25 at 3.

378. As shown below, the Accused '856 Products include Netflow. "In the NetFlow architecture, data is transmitted from exporter to collector in sets of records. Each record in a data set has the same format, which is specified by its template. The data record consists of a series of NetFlow information elements or "fields," and a specific ID value is assigned to each field. The ID values for information elements may be globally defined and archived by the Internet Assigned Numbers Authority (IANA), or they may be enterprise specific and defined by individual organizations." *Id.* at 5.

Figure 3. Stealtwatch Enterprise Multi-layer Machine Learning



Id. at 5.

As shown below, the Accused '856 Products route the filtered packets to a proxy system:

Deployment Details

How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

```
class-map [highest class name]
```

Commands at a CLI or script prompt:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
police rate 10000 pps burst 10000
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

This section describes those procedures necessary to enable ETA and FNF on the Catalyst 9300 and 9400 switches in the campus as well as the ISR and ASR routers for branch WAN. This section consists of four processes in which you perform Stealthwatch and ETA integration, enable ETA and FNF on Catalyst switches, enable ETA and FNF on Cisco routers, and use the Stealthwatch and the CTA portal user interfaces for crypto audit and malware detection.

PROCESS

Integrating Cognitive Threat Analytics with Stealthwatch

1. Configure Stealthwatch Management Console for CTA integration
2. Configure the Flow Collector
3. Verify integration between Stealthwatch and CTA cloud
4. Define the Inside Hosts address range in Stealthwatch

These procedures assume that either direct communication or communication via a proxy are permitted from the Stealthwatch Management Center and Flow Collectors to the Cognitive Threat Analytics cloud. These communications are all via port 443 and their addresses are:

cognitive.cisco.com—108.171.128.81

etr.cloudsec.sco.cisco.com—108.171.128.86

See Encrypted Traffic Analytics Deployment Guide, available at https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Encrypted-Traffic-Analytics-Deployment-Guide-2017DEC.pdf, attached hereto as Exhibit 33 at 32.

379. As a result of Cisco'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.

380. Cisco's infringement of the '856 Patent has injured and continues to injure

Centripetal in an amount to be proven at trial.

381. Cisco has willfully infringed each of the Asserted Patents. Centripetal is informed and believes that Cisco had knowledge of the Asserted Patents through various channels and despite its knowledge of Centripetal's patent rights, engaged in egregious behavior warranting enhanced damages.

382. On or around 2014, Centripetal partnered with ThreatGRID, a company which included threat intelligence technology which Centripetal integrated with their patented products that used some of the Asserted Patents. Cisco later acquired ThreatGRID in 2016. Centripetal is informed and believes that Cisco gained increased exposure to Centripetal's patented technology as a result of the acquisition of ThreatGRID. *See* https://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/threatgrid.html, attached hereto as Exhibit 31.

383. Centripetal is further informed and believes that, on or around January 2016, Cisco requested an introduction to Centripetal through a third party, Granite Hill Capital Partners. Later, Centripetal received a point of contact introduction to Cisco from Granite Hill Capital Partners.

384. In 2016, Cisco invited Centripetal to participate in Cisco Live, which is Cisco's partner conference – in which Centripetal was asked to demonstrate its technology in Cisco's "Security Partner Village" booth. On or around June 2016, Centripetal attended the Cisco Live conference and demonstrated its patented technology, including the RuleGATE Threat Intelligence Gateway product which encompasses at least some of the Asserted Patents. Cisco currently lists Centripetal on its website located at www.cisco.com, as part of a "partner ecosystem" whose "[t]hreat intelligence platforms" use Threat Grid. *See*

https://www.cisco.com/c/en/us/products/security/threat-grid/integrations.html#~stickynav=2, attached hereto as Exhibit 32 at 3.

385. Cisco thus knew or, in the alternative, was willfully blind to Centripetal's technology and its Asserted Patents. Cisco's infringement of the '856 Patent is egregious because despite this knowledge, Centripetal is informed and believes that Cisco deliberately copied Centripetal's patented technology, which it implemented into its products and services, such as Centripetal's CleanINTERNET service and Threat Intelligence Gateway, including the RuleGATE 2000. The blatant copying of Centripetal's patented technology and disregard for Centripetal's patent rights with an objectively high likelihood of infringement is egregious behavior warranting a finding of willful infringement and enhanced damages.

386. Centripetal is informed and believes that Cisco has undertaken no efforts to design these products or services around the '856 Patent to avoid infringement despite Cisco's knowledge and understanding that its products and services infringe the '856 Patent. As such, Cisco has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '856 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.

TWENTY-SECOND CAUSE OF ACTION
(Indirect Infringement of the '856 Patent pursuant to 35 U.S.C. § 271(b))

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

388. In addition to directly infringing the '856 Patent, Cisco indirectly infringes the '856 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to perform one or more of the steps

of the method claims, either literally or under the doctrine of equivalents, of the '856 Patent, where all the steps of the method claims are performed by either Cisco, its customers, purchasers, users or developers, or some combination thereof. Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the '856 Patent, including Claims 1-23.

389. Cisco knowingly and actively aided and abetted the direct infringement of the '856 Patent by instructing and encouraging its customers, purchasers, users and developers to use the '856 Accused Products. Such instructions and encouragement include, but are not limited to, advising third parties to use the '856 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '856 Patent, specifically through the use of the Accused Catalyst Products, the Accused Router Products, and the Accused Stealthwatch Products, alone or in conjunction with one another, and by advertising and promoting the use of the '856 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '856 Accused Products in an infringing manner.

390. Cisco updates and maintains an HTTP site with Cisco's quick start guides, administration guides, user guides, operating instructions, blogs, white papers, data sheets and training certification programs which cover in depth aspects of operating Cisco's offerings. *See* https://www.cisco.com/c/en/us/support/switches/catalyst-9300-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 34; *see also* https://www.cisco.com/c/en/us/support/switches/catalyst-9400-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 35;

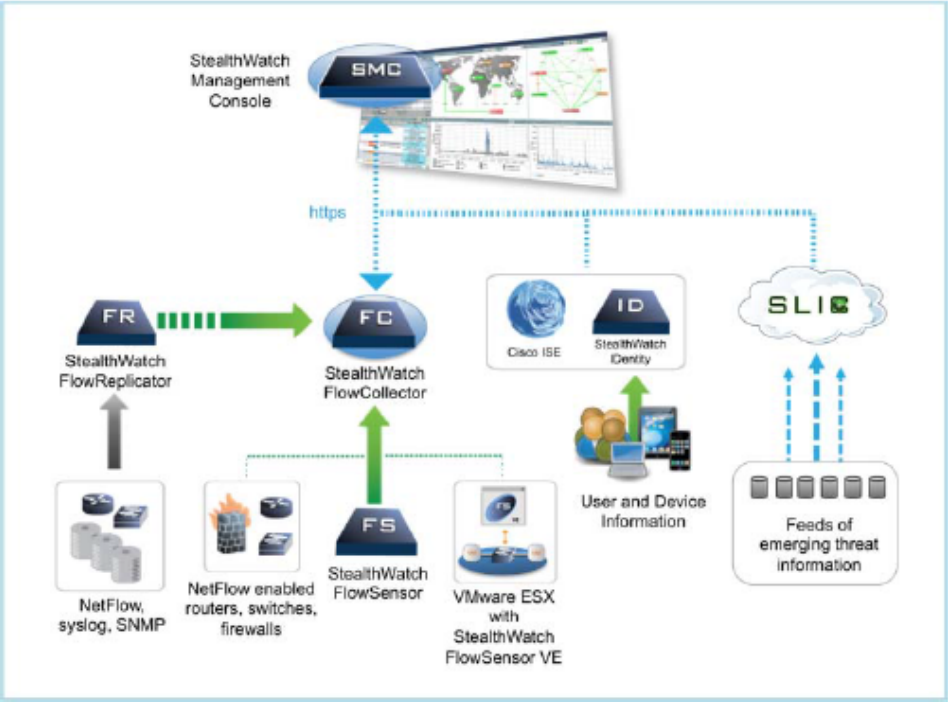
https://www.cisco.com/c/en/us/support/switches/catalyst-9500-series-switches/tsd-products-support-series-home.html, attached hereto as Exhibit 36; https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.pdf, attached hereto as Exhibit 16; https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/datasheet-c78-739053.pdf, attached hereto as Exhibit 17; https://www.cisco.com/c/en/us/support/routers/index.html, attached hereto as Exhibit 37; https://www.cisco.com/c/dam/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/at-a-glance-c45-612993.pdf, attached hereto as Exhibit 18; https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/datasheet-c78-732542.pdf, attached hereto as Exhibit 19; https://blogs.cisco.com/enterprise/cisco-traffic-analysis-encrypted-threat-analytics, attached hereto as Exhibit 38; https://communities.cisco.com/docs/DOC-76964, attached hereto as Exhibit 39; https://www.cisco.com/c/en/us/support/security/stealthwatch/tsd-products-support-series-home.html, attached hereto as Exhibit 40; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-guides-list.html, attached hereto as Exhibit 41; https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/hardware/installation/SW_6_9_1_Hardware_Installation_DV_1_2.pdf, attached hereto as Exhibit 42; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-and-configuration-guides-list.html, attached hereto as Exhibit 43; https://www.cisco.com/c/en/us/support/security/stealthwatch/products-programming-reference-guides-list.html, attached hereto as Exhibit 44; https://www.cisco.com/c/en/us/training-

events/training-certifications/certifications/associate/ccna-routing-switching.html, attached hereto as Exhibit 45.

391. These documents provide instructions, directions and/or require others, including its customers, purchasers, users, and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '856 Patent, where all the steps of the method claims are performed by either Cisco, its customers, purchasers, users or developers, or some combination thereof. For example, Cisco includes the Stealthwatch System Hardware Installation Guide, which provides instructions and recommendations on how to install and deploy the Accused '856 Products in an infringing manner as shown below.

Placement Considerations

As shown in the figure below, Stealthwatch system products can be strategically deployed to provide optimal coverage of key network segments throughout the network, whether in the internal network, at the perimeter, or in the DMZ.



Placing the SMC

As the management device, the Stealthwatch Management Console (SMC) should be installed at a location on your network that is accessible to all the devices sending data to it.

If you have a failover pair of SMCs, it is recommended that you install the primary SMC and the secondary SMC in separate physical locations. This strategy will enhance a disaster recovery effort should it become necessary.

Placing the Stealthwatch Flow Collector

As collection and monitoring devices, the Stealthwatch Flow Collector for NetFlow appliance and the Stealthwatch Flow Collector for sFlow appliance should be installed at a location on your network that is accessible to the NetFlow or sFlow devices sending the data to a Flow Collector, as well as any devices you plan to use to access the management interface.

Note: When you place a Flow Collector outside a firewall, Lancope recommends that you turn off the setting "Accept traffic from any exporter."

Placing the Stealthwatch Flow Sensor

As a passive monitoring device, the Stealthwatch Flow Sensor can sit at multiple points on your network to observe and record IP activity, thereby protecting network integrity and detecting security breaches. The Flow Sensor features integrated Web-based management systems that facilitate either centralized or remote management and administration.

The Flow Sensor appliance is most effective when placed at critical segments of your corporate network as follows:

- Inside your firewall to monitor traffic and determine if a firewall breach has occurred
- Outside your firewall, monitoring traffic flow to analyze who is threatening your firewall
- At sensitive segments of your network, offering protection from disgruntled employees or hackers with root access
- At remote office locations that constitute vulnerable network extensions
- On your business network for protocol use management (for example, on your transaction services subnet to determine if a hacker is running Telnet or FTP and compromising your customers' financial data)

Placing Other Stealthwatch Products

The only requirement for the placement of other Stealthwatch products, such as the Stealthwatch UDP Director (also known as FlowReplicator), or a VM server containing a Stealthwatch Flow Sensor Virtual Edition (VE), is that they have an unobstructed communication path to the rest of your Stealthwatch products as applicable.

Exhibit 42 at 11-12.

392. As such, Cisco knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Cisco, one or more method claims of the '856 Patent.

PRAYER FOR RELIEF

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

(A) An entry of judgment holding that Cisco has infringed and is infringing the '193 Patent, the '176 Patent, the '077 Patent, the '722 Patent, the '806 Patent, the '713 Patent, the '552 Patent, the '213 Patent, the '205 Patent, the '148 Patent, and the '856 Patent; has induced infringement and is inducing infringement of the '193 Patent, the '176 Patent, the '077 Patent, the '722 Patent, the '806 Patent, the '713 Patent, the '552 Patent, the '213 Patent, the '205 Patent, the '148 Patent, and the '856 Patent;

(B) A preliminary and permanent injunction against Cisco and its officers, employees, agents, servants, attorneys, instrumentalities, and/or those in privity with them, from infringing the '193 Patent, the '176 Patent, the '077 Patent, the '722 Patent, the '806 Patent, the '713 Patent, the '552 Patent, the '213 Patent, the '205 Patent, the '148 Patent, and the '856 Patent, or inducing the infringement of the '193 Patent, the '176 Patent, the '077 Patent, the '722 Patent, the '806 Patent, the '713 Patent, the '552 Patent, the '213 Patent, the '205 Patent, the '148 Patent, and the '856 Patent and for all further and proper injunctive relief pursuant to 35 U.S.C. § 283;

(C) An award to Centripetal of such damages as it shall prove at trial against Cisco that is adequate to fully compensate Centripetal for Cisco's infringement of the '193 Patent, the '176 Patent, the '077 Patent, the '722 Patent, the '806 Patent, the '713 Patent, the '552 Patent, the '213 Patent, the '205 Patent, the '148 Patent, and the '856 Patent, said damages to be no

less than a reasonable royalty;

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

(E) A determination that the damages against Cisco 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 '193 Patent, the '176 Patent, the '077 Patent, the '722 Patent, the '806 Patent, the '713 Patent, the '552 Patent, the '213 Patent, the '205 Patent, the '148 Patent, and the '856 Patent; and

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

Respectfully submitted,

Dated: March 29, 2018

By: */s/ Kevin M. O'Donnell*_____

Kevin M. O'Donnell (VSB #30086)
Jeffery T. Martin, Jr. (VSB #71860)
HENRY & O'DONNELL, P.C.
300 N. Washington Street – Suite 204
Alexandria, VA 22314
Telephone: (703) 548-2100
Facsimile: (703) 548-2105
kmo@henrylaw.com
jtm@henrylaw.com

Paul J. Andre
Lisa Kobialka
James Hannah
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

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: March 29, 2018

By: */s/ Kevin M. O'Donnell*_____

Kevin M. O'Donnell (VSB #30086)
Jeffery T. Martin, Jr. (VSB #71860)
HENRY & O'DONNELL, P.C.
300 N. Washington Street – Suite 204
Alexandria, VA 22314
Telephone: (703) 548-2100
Facsimile: (703) 548-2105
kmo@henrylaw.com
jtm@henrylaw.com

Paul J. Andre
Lisa Kobialka
James Hannah
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

Attorneys for Plaintiff
CENTRIPETAL NETWORKS, INC.

CERTIFICATE OF SERVICE

I hereby certify that on the 29th day of March 2018, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system, which will then send a notification of such filing (NEF) to the following:

Christopher Joseph Tyson
Email: cjtyson@duanemorris.com

Daniel T. McCloskey
Email: DTMcCloskey@duanemorris.com

Jennifer H. Forte
Email: jhforte@duanemorris.com

John Robert Gibson
Email: jrgibson@duanemorris.com

Joseph A. Powers
Email: japowers@duanemorris.com

Louis Norwood Jameson
Email: wjameson@duanemorris.com

/s/ Kevin M. O'Donnell
Kevin M. O'Donnell (VSB #30086)