

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

QPRIVACY USA LLC,

Plaintiff,

v.

CISCO SYSTEMS, INC.,

Defendant.

Civil Action No. _____

JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff QPrivacy USA LLC (“QPrivacy”) brings this action against Defendant Cisco Systems, Inc. (“Cisco” or “Defendant”) for infringement of QPrivacy’s United States Patent Nos. 11,106,824 (“the ’824 Patent”) and 11,816,249 (“the ’249 Patent”) (collectively, the “Asserted Patents”), and hereby alleges as follows:

NATURE OF THE ACTION

1. This is an action for patent infringement. These claims arise under the patents laws of the United States, 35 U.S.C. §§ 1, *et seq.*, as a result of Defendant’s infringement of the Asserted Patents.

2. QPrivacy owns the entire right, title, and interest in and to each of the Asserted Patents, and possesses all rights to sue for infringement of the Asserted Patents and recover past damages and/or royalties prior to the expiration of the Asserted Patents.

3. Without authorization from QPrivacy, Defendant makes, uses, sells, offers for sale, and/or imports into the United States certain server and networking devices, including Cisco ethernet switches, routers, edge networking products, wireless controllers, and software that implement Encrypted Traffic Analytics (ETA) technology (collectively, the “Accused Products”).

PARTIES

4. QPrivacy is a limited liability company organized and existing under the laws of the State of Texas, with its principal place of business at 1127 Judson Rd., Suite 211, Longview, Texas 75606.

5. QPrivacy's technologies focus on providing enhanced technology which not only provides greater security from network attacks but also maintains data privacy and integrity.

6. QPrivacy uses its protective solutions to secure, control and manage client data in public networks, enable organizations to meet content-based regulations (privacy) and secure generative AI behavior on their Websites and native Mobile Applications (iOS and Android).

7. QPrivacy holds patents in the EU, USA and Israel. See <https://www.qprivacy.com/patents/>.

8. QPrivacy's parent company and predecessor in interest in the patents Privacy Rating Ltd. has launched multiple products including QPaudit, QPrules, and QPtrust, with customers across different markets and lines of business.

9. On information and belief, Defendant Cisco is a Delaware corporation with its principal place of business at 170 West Tasman Drive, San Jose, California 95134.

10. On information and belief, Cisco is registered to do business in Texas, maintains places of business in Texas, and conducts business in Texas. Cisco has at least two places of business in this district, including a multi-building campus with over 1,400 employees at 2250 East President George Bush Turnpike, Richardson, Texas 75082, and a 162,000 square foot data center at 2260 Chelsea Blvd., Allen, Texas 75013. In 2019, the Collin County Appraisal District appraised these facilities at a combined value over \$300,000,000.

11. Cisco has a permanent and continuous presence in Texas and a regular and established place of business in the Eastern District of Texas. Cisco can be served with process through its registered agent for service of process at Corporation Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701-3128.

12. Defendant Cisco designs, makes, manufactures, sells, offers to sell, imports, distributes, advertises and/or uses the Accused Products in the United States and in this District.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action for patent infringement pursuant to 28 U.S.C. §§ 1331 and 1338(a).

14. This Court has personal jurisdiction over the Defendant in this action pursuant to due process and/or the Texas Long Arm Statute. Defendant has committed acts within this District giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Defendant would not offend traditional notions of fair play and substantial justice. Defendant has purposely availed themselves of the laws and protections of the United States and the State of Texas by knowingly making, using, selling, offering for sale, distributing and/or advertising the Accused Products in Texas and this District. Defendant maintains continuous and systematic contacts within this District by selling and offering for sale products and services to customers in this District and by offering for sale products and services that are used in this District. Defendant, directly or through subsidiaries or intermediaries, has regularly and systematically conducted and conducts substantial business in this District, including but not limited to: (i) making, using, offering for sale and/or selling infringing products or services in this District; (ii) engaging in at least part of the infringing acts alleged herein; (iii) purposefully and voluntarily placing one or more infringing products or services into the stream of commerce

with the expectation that those products or services will be purchased and/or used by consumers in this District; and/or (iv) regularly doing or soliciting business, engaging in other persistent courses of conduct or deriving substantial revenue from goods and services provided to individuals in Texas and in this District. Defendant has targeted the State of Texas and this District by conducting regular business therein, and has placed and continues to place infringing products into the stream of commerce through an established distribution channel with the expectation and/or knowledge that they will be purchased by consumers in the State of Texas and this District.

15. QPrivacy's claims for patent infringement arise directly from and/or relate to the above-referenced activity.

16. Venue is proper in this District under 28 U.S.C. §§ 1391(b)-(d) and 1400(b) for the reasons set forth above.

17. Venue is also proper because, on information and belief, Cisco has a regular and established place of business in this District, including facilities in Richardson, Texas and Allen, Texas. Cisco is registered with the Secretary of State to do business in the State of Texas. Cisco also has authorized sellers and sales representatives that offer for sale and sell infringing products to consumers throughout Texas and in this District, including at least Cynergy Technology based in Tyler, Texas and Longview, Texas. On information and belief, Cisco currently operates out of or makes use of leased, work-share, co-op or other arrangements for space, offices or facilities in this District, including through its partners and/or agents.

18. For example, on information and belief, Cisco implements a comprehensive work-from-home policy under which Cisco has adopted or ratified one or more additional places of business in this District, including but not limited to the homes of employees, such that the collection of these locations constitutes an aggregate network of regular and established places in

this District, in and from which business is operated. On information and belief, Cisco specifically advertises for and solicits employees to reside and work remotely in this District, including to support its customers in the District, and provides and/or stores literature, equipment and/or inventory at those locations for the purpose of enabling these employees to conduct their jobs and use such literature, equipment and/or inventory specifically in this District. On information and belief, Cisco employs service technicians and sales representatives in this District who provide support and sales services to existing Cisco customers and prospective customers residing in this District. The work of these Cisco service technicians and sales representatives is therefore inextricably tied to this District.

19. Further, Cisco has admitted or not contested personal jurisdiction in this District. *See Orckit Corp. v. Cisco Systems, Inc.*, No. 2:22-cv-276-JRG-RSP, Dkt. 26 (E.D. Tex. Oct. 28, 2022).

FACTUAL ALLEGATIONS

20. This lawsuit relates to significant advancements in the management of private data during communication between a remote server and a user device, as further described in the Asserted Patents.

A. The Asserted Patents

21. The '824 Patent is entitled "System and Method for Dynamic Management of Private Data" and issued on August 31, 2021. The named inventors on the '824 Patent are Yoseph Koren and Yehonatan Wasserman. QPrivacy owns by assignment the entire right, title, and interest in and to the '824 Patent. A true and correct copy of the '824 Patent is attached hereto as Exhibit 1.

22. The '249 Patent is entitled "System and Method for Dynamic Management of Private Data and issued on November 14, 2023. The named inventors on the '249 Patent are Yoseph Koren and Yehonatan Wasserman. QPrivacy owns by assignment the entire right, title, and interest in and to the '249 Patent. A true and correct copy of the '249 Patent is attached hereto as Exhibit 2.

B. The Accused Products

23. Defendant has, without QPrivacy's authority, made, used, offered to sell, sold, and/or imported into the United States, and/or instructed others regarding the making, use, sale, offer for sale, or importation of certain server and network devices, including Cisco ethernet switches, routers, edge networking products, wireless controllers, and software that implement Encrypted Traffic Analytics (ETA) technology, that directly infringe (literally or under the doctrine of equivalents), induce the infringement of, and/or are made or produced under, or by means of, a process covered by, one or more claims of each of the Asserted Patents. This includes, but is not limited to, Cisco's Secure Network Analytics suite of products and software.

24. Cisco offers numerous infringing devices and products including, but not limited to, devices identified with the following exemplary device/product numbers: Cisco Catalyst 9400 Series Switches, Cisco Catalyst 9300 Series Switches, Cisco Meraki Cloud Managed Switches, Cisco ISR 1000 Series Routers, Cisco Catalyst IE9300 Rugged Series Switches, Cisco Catalyst 8000 Edge Platforms Family, Cisco Catalyst IE3400 Heavy Duty Series IE Switches, Cisco Cloud Service Router 1000v, Cisco Catalyst IE3400 Rugged Series Switches, Cisco Integrated Services Virtual Router, Cisco Catalyst IE3300 Rugged Series Switches, Cisco Catalyst 8500 Series Edge Platforms, Cisco Catalyst 9800-40 Wireless Controller, Cisco DNA Software, Cisco Catalyst 9800-80 Wireless Controller, Cisco DNA Software for Wireless, Cisco

Catalyst 9800-L Wireless Controller, Cisco Secure Network Analytics, Cisco Catalyst 9800-CL Wireless Controller for Cloud, Cisco 4000 Family Integrated Services Routers, and Cisco ASR 1000 Series Routers. The exemplary products listed in this Complaint are nonexhaustive and nonlimiting. Further discovery may reveal additional infringing devices and products.

25. Defendant, directly or indirectly through their affiliates, subsidiaries, agents, customers, or other representatives, makes, uses, sells and/or offers for sale the Accused Products in the United States in this District, and/or imports the Accused Products into the United States.

26. Defendant has had knowledge of the Asserted Patents at least since the filing of this Complaint.

27. The allegations set forth herein are exemplary and without prejudice to infringement contentions provided pursuant to the Court's orders and local rules. By setting forth these allegations, QPrivacy does not convey or imply any particular claim construction or the precise scope of the claims. These infringement allegations are based on currently available information and a reasonable investigation of the Accused Products. QPrivacy reserves all rights, including the right to modify this description based on information obtained during discovery.

COUNT I

DEFENDANT'S INFRINGEMENT OF U.S. PATENT NO. 11,106,824

28. QPrivacy realleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

29. The claims of the '824 Patent relate to managing private data during network communications. As noted in the '824 Patent itself, "[d]uring communication with external remote

servers different types of data are automatically (and uncontrollably) shared, sometimes without the knowledge of the user (e.g., the owner of the data).” ’824 Patent at 1:22-25. The claims of the ’824 Patent patentably improve security of data communications, even when the underlying data content itself is not read. The claimed approaches therefore present specific, non-abstract improvements to a very specific technological feature—management of private data.

30. The claims of the ’824 Patent are valid and enforceable, and each enjoys a statutory presumption of validity under 35 U.S.C. § 282.

31. Defendant’s infringing activities violate 35 U.S.C. § 271.

32. Defendant infringes at least claim 17 of the ’824 Patent.

33. For example, Claim 17 of the ’824 Patent recites:

17. A system for dynamic management of private data during communication between a remote server and at least one user's device, the system comprising: a memory; a communication data type database, comprising at least one communication data type corresponding to sharing of at least one data packet from the user's device; a privacy preference database, comprising a list of allowed types of data packets for sharing during communication with the at least one user's device; a communication module, to allow communication between the remote server and the at least one user's device; and a processor, coupled to a response database and to the privacy preference database, wherein the processor is configured to instruct the remote server to determine at least one data type for sharing of data packet that is compatible with the list of allowed patterns of data packets for sharing, and wherein the at least one data type is determined in accordance with characteristics of the communication data packet, and wherein the content of the at least one data packet is not read by the remote server for continued operation by the user's device in real time during communication between the remote server and the user's device.

34. The Accused Products implement Encrypted Traffic Analytics (ETA) technology and contain a system for dynamic management of private data during communication between a remote server and at least one user's device. ETA analyzes encrypted data traffic to and from Cisco devices without decrypting the underlying data.

Encrypted traffic analytics

Cisco, with its expertise in the network infrastructure market, conducted extensive research and has introduced an innovative and revolutionary technology, [Encrypted Traffic Analytics](#). It helps illuminate the dark corners in encrypted traffic without any decryption by using new types of data elements or telemetry that are independent of protocol details.

Encrypted Traffic Analytics extracts four main data elements:

- 1. Sequence of Packet Lengths and Times (SPLT):** SPLT conveys the length (number of bytes) of each packet's application payload for the first several packets of a flow, along with the interarrival times of those packets
- 2. Initial Data Packet (IDP):** 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 and address, and other data elements
- 3. Byte distribution:** The byte distribution represents the probability that a specific byte value appears in the payload of a packet within a flow
- 4. TLS-specific features:** The TLS handshake is composed of several messages that contain interesting, unencrypted metadata used to extract data elements, such as cipher suite, TLS version, and the client's public key length




Using these data elements or enhanced telemetry, Encrypted Traffic Analytics can help detect malicious activity in encrypted traffic by applying advanced security analytics. At the same time, the integrity of the encrypted traffic is maintained because there is no need for bulk decryption.

Achieve cryptographic compliance

While using encryption for data privacy and protection, an organization should be able to answer the questions, How much of the digital business uses strong encryption? What is the quality of that encryption? This information is very important to prevent attackers from getting into the encrypted stream in the first place. Today, the only way to ensure that encrypted traffic is policy compliant is to perform periodic audits to look for any TLS violations. However, this is not a great strategy due to the number of devices and the amount of traffic flowing through the business. Encrypted Traffic Analytics provides continuous monitoring without the cost and time overhead of decryption-based monitoring. Using the collected enhanced telemetry, Secure Network Analytics provides the ability to view and search on parameters such as encryption key exchange, encryption algorithm, key length, TLS/SSL version, etc. to help ensure cryptographic compliance.

Source: <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/at-a-glance-c45-740079.pdf>

Features and benefits

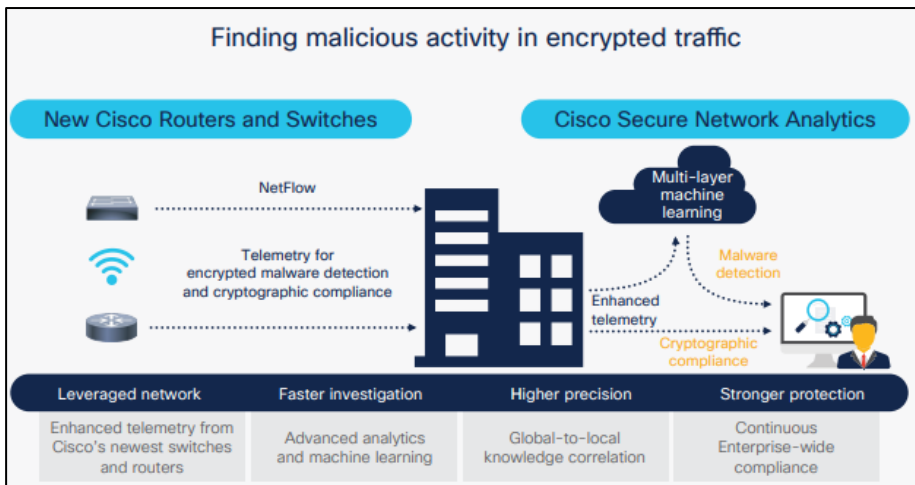
 <p>Get comprehensive visibility and analytics (PDF)</p> <p>Detect attacks across the dynamic network with high-fidelity alerts enriched with context such as user, device, location, timestamp, and application. Analyze encrypted traffic for threats and compliance, without decryption.</p>	 <p>Speed up incident response</p> <p>Quickly detect unknown malware, insider threats like data exfiltration, policy violations, and other sophisticated attacks using advanced analytics. Store telemetry data for long periods for forensic analysis.</p>	 <p>Simplify network segmentation</p> <p>Define smarter segmentation policies without disrupting the business. Create custom alerts to detect any unauthorized access and ensure compliance. Use Secure Network Analytics with Identity Services Engine (ISE) to enforce policies and contain threats.</p>
---	---	---

Source: <https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html>

35. The Accused Products monitor and store telemetry data in order to analyze and compare network traffic and then determine a response based on that comparison.

Detect malware hidden in encrypted traffic

The enhanced network telemetry from the latest Cisco routers and switches is collected by Cisco Secure Network Analytics, a comprehensive network visibility and security analytics product. It uses advanced entity modeling and multilayer machine learning, constantly identifying who is on the network and what they are doing, and can detect anomalous behavior in real time to identify threats. It also uses a global threat map to identify and correlate known global threats to the local environment. This considerably improves the fidelity of malware detection in encrypted traffic, and at the same time provides end-to-end confidentiality and maintains channel integrity because there is no decryption—an industry first.



Source: <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/at-a-glance-c45-740079.pdf>

Features and benefits

Get comprehensive visibility and analytics (PDF)

Detect attacks across the dynamic network with high-fidelity alerts enriched with context such as user, device, location, timestamp, and application. Analyze encrypted traffic for threats and compliance, without decryption.

Speed up incident response

Quickly detect unknown malware, insider threats like data exfiltration, policy violations, and other sophisticated attacks using advanced analytics. Store telemetry data for long periods for forensic analysis.

Simplify network segmentation

Define smarter segmentation policies without disrupting the business. Create custom alerts to detect any unauthorized access and ensure compliance. Use Secure Network Analytics with Identity Services Engine (ISE) to enforce policies and contain threats.

Source: <https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html>

Flow Sensor produces two new data elements: the sequence of packet lengths and times and the initial data packet. The initial data packet is a treasure trove of metadata, because, remember, all encrypted sessions start out unencrypted initially. Cisco's unique Application-Specific Integrated Circuit (ASIC) architecture provides the ability to extract these data elements without slowing down the data network.

This enhanced telemetry is passed on to Secure Network Analytics, which applies the multiple analytics techniques described in the previous section to detect malware in encrypted traffic with high fidelity.

Advanced Persistent Threats (APTs)

APTs are highly targeted attacks against an organization with the primary purpose of stealing valuable information without being detected, so they can continue to persist over a long period of time. Using advanced behavioral modeling, Secure Network Analytics can gain a deep understanding of the normal behavior within the organization combined with the knowledge of known bad behavior using the Global Risk Map. Thus, it's able to detect activities associated with APTs such as reconnaissance, scanning, command-and-control communications, suspicious lateral network behavior, etc.

Insider threats

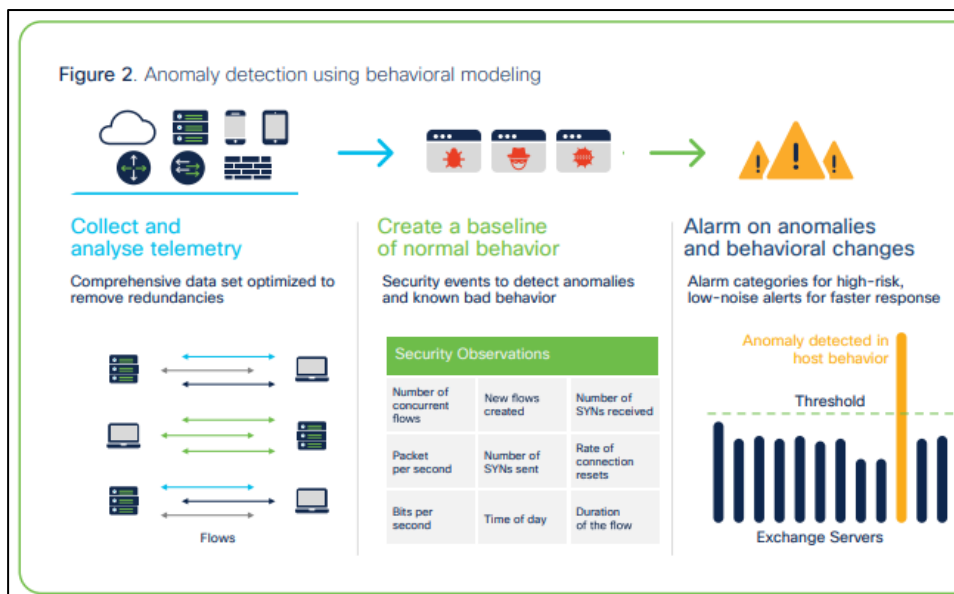
Among the most valuable assets that an organization has are its intellectual property, confidential information, and information stored in the company networks. Data breaches cost organizations millions of dollars. The average cost per lost or stolen record is \$158, which amounts to about \$4 million per year on data breaches. Insider threats, such as compromised user credentials or disgruntled employees, hoard data in order to exfiltrate it to the outside world for financial gain or just to cause harm.

Using behavioral modeling to detect anomalous behavior, a "data hoarding" or "exfiltration" alarm is generated. The host that triggers the alarm can be investigated with one click. Secure Network Analytics uses the network to provide additional contextual information about the host such as username, MAC address, location, etc. And if needed, Secure Network Analytics can **quarantine** the suspected host off the network. This is enabled by the integration with Cisco Secure Network Access.

Source: <https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch/white-paper-c11-740605.pdf>

1. Behavioral modeling

Secure Network Analytics closely monitors the activity of every device on the network and is able to create a baseline of normal behavior. In addition, it also has a deep understanding of known bad behavior. It applies close to 100 different security events or heuristics that look at various types of traffic behavior, such as scanning, beaconing host, brute force login, suspect data hoarding, suspect data loss, etc. These security events feed into high-level logical alarm categories. Some security events can also trigger alarms on their own. So the system is able to correlate multiple, isolated anomalous incidents and piece them all together to determine what kind of attack might be in play, and also tie it to a specific device and user (Figure 2). The incident can be further investigated by time as well as by the associated telemetry. This is context at its best. Physicians examining a patient don't look at a symptom in isolation to figure out what's wrong. They look at the whole picture to provide a diagnosis. Similarly, Secure Network Analytics records every anomalous activity in the network and looks at it holistically to generate contextual alarms that can help security teams prioritize risks.



2. Multilayered machine learning

Secure Network Analytics also applies **machine learning**, both supervised and unsupervised, to discover advanced threats and malicious communications. It integrates with a cloud-based multistage machine learning analytics pipeline which correlates threat behaviors seen in the enterprise with those seen globally.

The system analyzes user and device behavior to discover malware infections, command-and-control communications, data exfiltration, and potentially unwanted applications operating in an organization's infrastructure. There are multiple layers of processing, where a combination of techniques from artificial intelligence, machine learning and mathematical statistics helps the network to self-learn its normal activity so it can identify malicious activity.

This network security analytics pipeline, which collects telemetry from every part of the extended network, including encrypted traffic, is unique to Secure Network Analytics. It gradually builds a notion of "what is anomalous," then classifies actual individual pieces of "threat activity," and finally arrives at a final conviction of whether or not a device or user is in fact compromised. It is through a very careful analysis and correlation that we are able to bring in small pieces of evidence that all together will allow us to finally convict a compromised entity.

This capability is important because a typical enterprise may receive tons of alerts daily, and it's not possible for resource-strapped security teams to investigate all those alerts. The machine learning engine processes massive amounts of data in near real time to discover critical incidents with high confidence and is also able to suggest clear courses of actions to remediate quickly.

Source: <https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch/white-paper-c11-740605.pdf>

36. The Accused Products perform the encrypted traffic analysis and determination of response in real time.

Benefits of the solution

- **Enhanced visibility:** Gain insight into threats in encrypted traffic using network analytics and machine learning. Obtain contextual threat intelligence with real-time analysis correlated with user and device information
- **Cryptographic assessment:** Help ensure enterprise compliance with cryptographic protocols and visibility into and knowledge of not only what is being encrypted in the network, but also the strength of the encryption
- **Faster time to response:** Quickly contain infected devices and users by detecting threats within encrypted traffic in real time without relying on slow, decryption-based methods
- **Time and cost savings:** Use the network as the foundation for the security posture, capitalizing on security investments in the network

Source: <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/at-a-glance-c45-740079.pdf>

37. The Accused Products contain memory and processors in order to perform the collection, analysis, and response determination.

Product Highlights

- The Cisco Unified Access Data Plane (UADP) 3.0sec ASIC on C9400X-SUP-2XL, C9400X-SUP-2 and Cisco Unified Access Data Plane (UADP) 2.0 ASIC on C9400-SUP-1/1XL/1XL-Y is ready for next-generation technologies with its programmable pipeline, microengine capabilities, and template-based configurable allocation of Layer 2, Layer 3, forwarding, Access Control List (ACL), and Quality of Service (QoS) entries
- Intel 2.4-GHz x86 with up to 960 GB of SATA SSD local storage for container-based application hosting
- Up to 4 non-blocking 100/40 Gigabit Ethernet uplinks and up to 4 non-blocking 25/10 Gigabit Ethernet uplinks on Supervisor-2/2XL

Table 5. Cisco Catalyst 9400 Supervisor Engine Performance and Scalability Features

Features	Performance and scalability			
Supervisor Engine	C9400-SUP-1	C9400-SUP-1XL/C9400-SUP-1XL-Y	C9400X-SUP-2	C9400X-SUP-2XL
Centralized wired capacity	Up to 1.44 Tbps	Up to 1.44 Tbps	Up to 9.6 Tbps	Up to 9.6 Tbps
Per-slot switching Capacity	80 Gbps	240 Gbps – C9404R 120 Gbps – C9407R 80 Gbps – C9410R	240 Gbps – C9404R 240 Gbps – C9407R 240 Gbps – C9410R	480 Gbps – C9404R 480 Gbps – C9407R 480 Gbps – C9410R
Total number of MAC addresses	Up to 64,000 ¹	Up to 64,000 ^{1,2}	Up to 64,000 ^{1,2}	Up to 64,000 ^{1,2}
Total number of IPv4 routes (ARP plus learned routes)	Up to 112,000 ³	Up to 144,000 ^{1,4}	Up to 256,000 ⁵	Up to 256,000 ⁵
FNF entries (v4/v6)	Up to 384,000/192,000	Up to 384,000/192,000	Up to 384,000/192,000 ⁶	Up to 384,000/192,000 ⁶
DRAM	16 GB	16 GB	16 GB	16 GB
Flash	10 GB	10 GB	10 GB	10 GB
VLAN IDs	4096	4096	4096	4096
PVST Instances	300 ⁷	300 ⁷	300	300
STP Virtual Ports (Port VLANs) for PVST	13,000	13,000	13,000	13,000
STP Virtual Ports (Port VLANs) for MST	13,000	13,000	13,000	13,000
SSD capacity	960 GB	960 GB	960 GB	960 GB
Total Switched Virtual	1,000	1,000	1,000	1,000

Table 1. Cisco Catalyst 9400 Series chassis features

Feature	Cisco Catalyst C9404R Chassis	Cisco Catalyst C9407R Chassis	Cisco Catalyst C9410R Chassis
Total number of slots	4	7	10
Line-card slots	2	5	8
Supervisor engine slots	2 ¹	2 ²	2 ³
Dedicated supervisor engine slot numbers	2 and 3 ⁴	3 and 4 ⁴	5 and 6 ⁴
Supervisor engine redundancy	Yes	Yes	Yes
Supervisor engines supported	C9400X-SUP-2XL, C9400X-SUP-2, C9400-SUP-1XL, C9400-SUP-1XL-Y, C9400-SUP-1	C9400X-SUP-2XL, C9400X-SUP-2, C9400-SUP-1XL, C9400-SUP-1XL-Y, C9400-SUP-1	C9400X-SUP-2XL, C9400X-SUP-2, C9400-SUP-1XL, C9400-SUP-1XL-Y, C9400-SUP-1

Supervisor configuration

The Catalyst 9400 Series offers an industry-leading supervisor engine built for secure networks, IoT applications, next generation mobility and cloud adoption. Supervisor Engine-2 options (Sup-2, Sup-2XL) and Supervisor Engine-1 options (Sup-1, Sup-1XL, Sup-1XL-Y) are built with the latest Unified Access Dataplane ASIC future-proofed for next generation technologies with its programmable pipeline, microengine capabilities and template-based configurable allocation of Layer 2, Layer 3, forwarding, Access Control Lists (ACLs) and QoS entries.

Table 2. Cisco Catalyst 9400 Series Supervisor Engine maximum bandwidth per slot

Feature	Cisco Catalyst 9400 Series Supervisor Engine C9400-SUP-1	Cisco Catalyst 9400 Series Supervisor Engine C9400-SUP-1XL	Cisco Catalyst 9400 Series Supervisor Engine C9400-SUP-1XL-Y	Cisco Catalyst 9400 Series Supervisor Engine C9400X-SUP-2	Cisco Catalyst 9400 Series Supervisor Engine C9400X-SUP-2XL
Cisco Catalyst C9404R chassis	80 Gbps/slot	240 Gbps/slot	240 Gbps/slot	240 Gbps/slot	480 Gbps/slot
Cisco Catalyst C9407R chassis	80 Gbps/slot	120 Gbps/slot	120 Gbps/slot	240 Gbps/slot	480 Gbps/slot
Cisco Catalyst C9410R chassis	80 Gbps/slot	80 Gbps/slot	80 Gbps/slot	240 Gbps/slot	480 Gbps/slot

Source: <https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/nb-06-cat9400-ser-data-sheet-cte-en.pdf>

38. The Accused Products satisfy all claim limitations of one or more claims of the '824 Patent. Defendant has infringed and continues to directly infringe one or more claims of the '824 Patent by making, using, selling, and/or offering for sale in the United States and/or importing into the United States the Accused Products. To the extent that any element is not literally present, each such element is present under the doctrine of equivalents because it performs substantially the same function in substantially the same way to achieve substantially the same result, and any differences between the Accused Products and claim element are insubstantial.

39. Defendant also knowingly and intentionally induces infringement of at least Claim 17 of the '824 Patent in violation of 35 U.S.C. § 271(b). Through at least the filing and service of this Complaint, Defendant has had knowledge of the '824 Patent and the infringing nature of the Accused Products. Despite this knowledge of the '824 Patent and its infringement, Defendant continues to actively encourage and instruct their customers and end users (for example, through user manuals and online instruction materials on its website and various service and customer support) to use the Accused Products in ways that directly infringe the '824 Patent. Defendant does so knowing and intending that its customers and end users will commit these infringing acts.

Defendant also continues to make, use, offer for sale, sell, and/or import the Accused Products, despite their knowledge of the '824 Patent, thereby specifically intending for and inducing their customers to infringe the '824 Patent through the customers' normal and customary use of the Accused Products.

40. Defendant has also infringed, and continues to infringe, at least Claim 17 of the '824 Patent by selling, offering for sale, or importing into the United States, the Accused Products, knowing that the Accused Products constitute a material part of the inventions claimed in the '824 Patent, are especially made or adapted to infringe the '824 Patent, and are not staple articles or commodities of commerce suitable for non-infringing use. Defendant has been, and currently is, contributorily infringing the '824 Patent in violation of 35 U.S.C. §§ 271(c) and (f).

41. By making, using, offering for sale, selling and/or importing into the United States the Accused Products, Defendant has injured Plaintiff and is liable for infringement of the '824 Patent pursuant to 35 U.S.C. § 271.

42. As a result of Defendant's infringement of the '824 Patent, Plaintiff is entitled to monetary damages in an amount adequate to compensate for Defendant's infringement, but in no event less than a reasonable royalty for the use made of the invention by Defendant, together with interest and costs as fixed by the Court.

43. Defendant also has knowledge of the '824 Patent at least due to the filing of this Complaint, and based on that knowledge, Defendant willfully infringes the '824 Patent.

44. Defendant's infringing activities have injured and will continue to injure Plaintiff, unless and until this Court enters an injunction prohibiting further infringement of the '824 Patent, and, specifically, enjoining further manufacture, use, sale, importation, and/or offers for sale that come within the scope of the patent claims.

COUNT II

DEFENDANT’S INFRINGEMENT OF U.S. PATENT NO. 11,816,249

45. QPrivacy realleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

46. The claims of the ’249 Patent relate to managing private data during network communications. As noted in the ’249 Patent itself, “[d]uring communication with external remote servers different types of data are automatically (and uncontrollably) shared, sometimes without the knowledge of the user (e.g., the owner of the data).” ’249 Patent at 1:25-28. The claims of the ’249 Patent patentably improve security of data communications, even when the underlying data itself is encrypted. The claimed approaches therefore present specific, non-abstract improvements to a very specific technological feature—management of private data.

47. The claims of the ’249 Patent are valid and enforceable, and each enjoys a statutory presumption of validity under 35 U.S.C. § 282.

48. Defendant’s infringing activities violate 35 U.S.C. § 271.

49. Defendant infringes at least claim 1 of the ’249 Patent.

50. For example, Claim 1 of the ’249 Patent recites:

1. A method of dynamic management of encrypted data during communication between a remote server and a user's device, the method comprising:
receiving, by the remote server, a communication comprising encrypted data packets;
determining, by the remote server, a content of at least one data packet of the communication in accordance with characteristics of the at least one data packet, and wherein the content of the at least one data packet is not decrypted by the remote server, and the determination of the content is performed by the remote server in real time during a communication session between the remote server and the user's device;
storing, by the remote server, a preference list;
determining, by the remote server, based on a comparison of the determined content, whether to modify the at least one data packet, and if so, modifying the at least one data packet; and

sharing, by the remote server, the modified communication.

51. The Accused Products implement Encrypted Traffic Analytics (ETA) technology and implement a method of dynamic management of encrypted data during communication between a remote server and a user's device. ETA analyzes encrypted data traffic to and from Cisco devices without decrypting the underlying data.

Encrypted traffic analytics

Cisco, with its expertise in the network infrastructure market, conducted extensive research and has introduced an innovative and revolutionary technology, [Encrypted Traffic Analytics](#). It helps illuminate the dark corners in encrypted traffic without any decryption by using new types of data elements or telemetry that are independent of protocol details.

Encrypted Traffic Analytics extracts four main data elements:

- 1. Sequence of Packet Lengths and Times (SPLT):** SPLT conveys the length (number of bytes) of each packet's application payload for the first several packets of a flow, along with the interarrival times of those packets
- 2. Initial Data Packet (IDP):** 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 and address, and other data elements
- 3. Byte distribution:** The byte distribution represents the probability that a specific byte value appears in the payload of a packet within a flow
- 4. TLS-specific features:** The TLS handshake is composed of several messages that contain interesting, unencrypted metadata used to extract data elements, such as cipher suite, TLS version, and the client's public key length




Using these data elements or enhanced telemetry, Encrypted Traffic Analytics can help detect malicious activity in encrypted traffic by applying advanced security analytics. At the same time, the integrity of the encrypted traffic is maintained because there is no need for bulk decryption.

Achieve cryptographic compliance

While using encryption for data privacy and protection, an organization should be able to answer the questions, How much of the digital business uses strong encryption? What is the quality of that encryption? This information is very important to prevent attackers from getting into the encrypted stream in the first place. Today, the only way to ensure that encrypted traffic is policy compliant is to perform periodic audits to look for any TLS violations. However, this is not a great strategy due to the number of devices and the amount of traffic flowing through the business. Encrypted Traffic Analytics provides continuous monitoring without the cost and time overhead of decryption-based monitoring. Using the collected enhanced telemetry, Secure Network Analytics provides the ability to view and search on parameters such as encryption key exchange, encryption algorithm, key length, TLS/SSL version, etc. to help ensure cryptographic compliance.

Source: <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/at-a-glance-c45-740079.pdf>

Features and benefits

		
<p>Get comprehensive visibility and analytics (PDF)</p> <p>Detect attacks across the dynamic network with high-fidelity alerts enriched with context such as user, device, location, timestamp, and application. Analyze encrypted traffic for threats and compliance, without decryption.</p>	<p>Speed up incident response</p> <p>Quickly detect unknown malware, insider threats like data exfiltration, policy violations, and other sophisticated attacks using advanced analytics. Store telemetry data for long periods for forensic analysis.</p>	<p>Simplify network segmentation</p> <p>Define smarter segmentation policies without disrupting the business. Create custom alerts to detect any unauthorized access and ensure compliance. Use Secure Network Analytics with Identity Services Engine (ISE) to enforce policies and contain threats.</p>

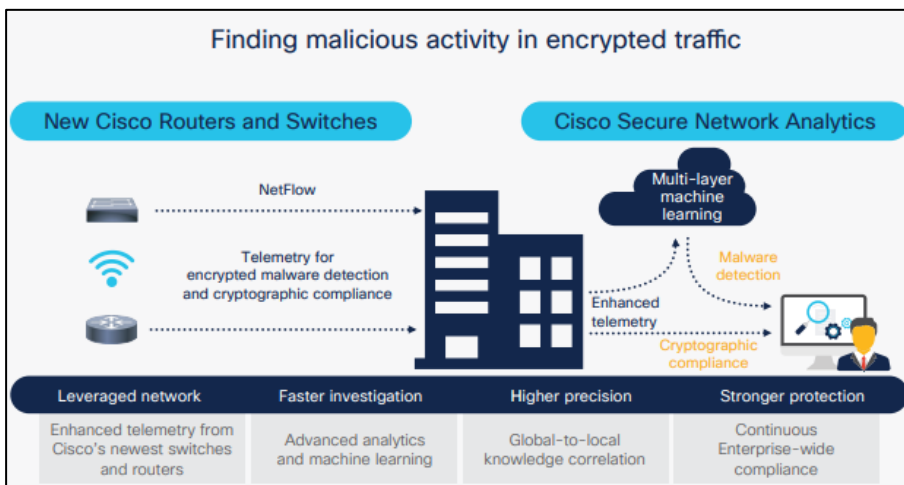
Source: <https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html>

52. The Accused Products monitor and store telemetry data in order to analyze and compare network traffic and then determine a response based on that comparison.

53. The Accused Products are gatekeeper remote servers in order to perform the collection, analysis, and response determination.




Detect malware hidden in encrypted traffic

The enhanced network telemetry from the latest Cisco routers and switches is collected by Cisco Secure Network Analytics, a comprehensive network visibility and security analytics product. It uses advanced entity modeling and multilayer machine learning, constantly identifying who is on the network and what they are doing, and can detect anomalous behavior in real time to identify threats. It also uses a global threat map to identify and correlate known global threats to the local environment. This considerably improves the fidelity of malware detection in encrypted traffic, and at the same time provides end-to-end confidentiality and maintains channel integrity because there is no decryption—an industry first.



Source: <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/at-a-glance-c45-740079.pdf>

Features and benefits

		
<p>Get comprehensive visibility and analytics (PDF)</p> <p>Detect attacks across the dynamic network with high-fidelity alerts enriched with context such as user, device, location, timestamp, and application. Analyze encrypted traffic for threats and compliance, without decryption.</p>	<p>Speed up incident response</p> <p>Quickly detect unknown malware, insider threats like data exfiltration, policy violations, and other sophisticated attacks using advanced analytics. Store telemetry data for long periods for forensic analysis.</p>	<p>Simplify network segmentation</p> <p>Define smarter segmentation policies without disrupting the business. Create custom alerts to detect any unauthorized access and ensure compliance. Use Secure Network Analytics with Identity Services Engine (ISE) to enforce policies and contain threats.</p>

Source: <https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html>

Flow Sensor produces two new data elements: the sequence of packet lengths and times and the initial data packet. The initial data packet is a treasure trove of metadata, because, remember, all encrypted sessions start out unencrypted initially. Cisco's unique Application-Specific Integrated Circuit (ASIC) architecture provides the ability to extract these data elements without slowing down the data network.

This enhanced telemetry is passed on to Secure Network Analytics, which applies the multiple analytics techniques described in the previous section to detect malware in encrypted traffic with high fidelity.

Advanced Persistent Threats (APTs)

APTs are highly targeted attacks against an organization with the primary purpose of stealing valuable information without being detected, so they can continue to persist over a long period of time. Using advanced behavioral modeling, Secure Network Analytics can gain a deep understanding of the normal behavior within the organization combined with the knowledge of known bad behavior using the Global Risk Map. Thus, it's able to detect activities associated with APTs such as reconnaissance, scanning, command-and-control communications, suspicious lateral network behavior, etc.

Insider threats

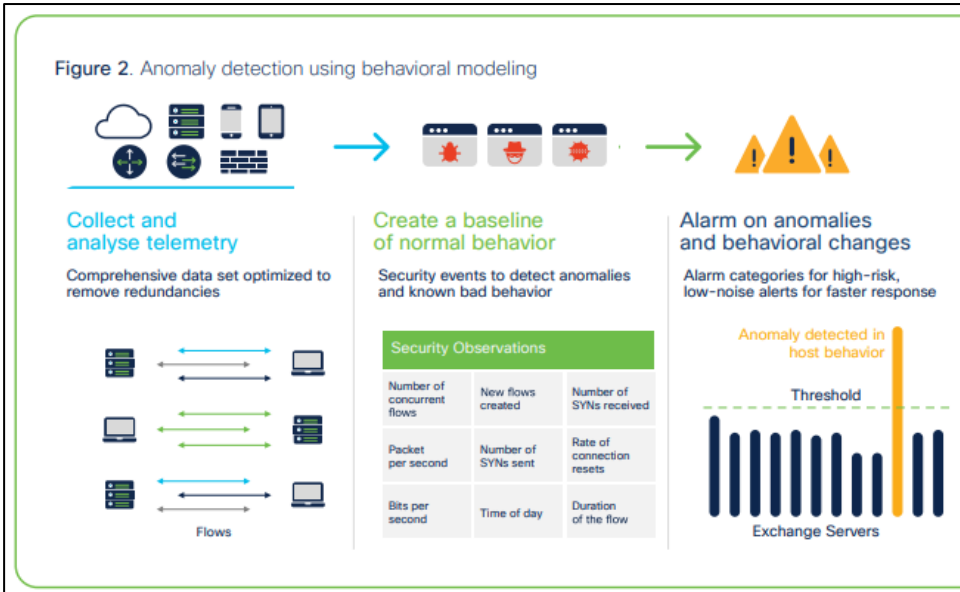
Among the most valuable assets that an organization has are its intellectual property, confidential information, and information stored in the company networks. Data breaches cost organizations millions of dollars. The average cost per lost or stolen record is \$158, which amounts to about \$4 million per year on data breaches. Insider threats, such as compromised user credentials or disgruntled employees, hoard data in order to exfiltrate it to the outside world for financial gain or just to cause harm.

Using behavioral modeling to detect anomalous behavior, a "data hoarding" or "exfiltration" alarm is generated. The host that triggers the alarm can be investigated with one click. Secure Network Analytics uses the network to provide additional contextual information about the host such as username, MAC address, location, etc. And if needed, Secure Network Analytics can **quarantine** the suspected host off the network. This is enabled by the integration with Cisco Secure Network Access.

Source: <https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch/white-paper-c11-740605.pdf>

1. Behavioral modeling

Secure Network Analytics closely monitors the activity of every device on the network and is able to create a baseline of normal behavior. In addition, it also has a deep understanding of known bad behavior. It applies close to 100 different security events or heuristics that look at various types of traffic behavior, such as scanning, beaconing host, brute force login, suspect data hoarding, suspect data loss, etc. These security events feed into high-level logical alarm categories. Some security events can also trigger alarms on their own. So the system is able to correlate multiple, isolated anomalous incidents and piece them all together to determine what kind of attack might be in play, and also tie it to a specific device and user (Figure 2). The incident can be further investigated by time as well as by the associated telemetry. This is context at its best. Physicians examining a patient don't look at a symptom in isolation to figure out what's wrong. They look at the whole picture to provide a diagnosis. Similarly, Secure Network Analytics records every anomalous activity in the network and looks at it holistically to generate contextual alarms that can help security teams prioritize risks.



2. Multilayered machine learning

Secure Network Analytics also applies **machine learning**, both supervised and unsupervised, to discover advanced threats and malicious communications. It integrates with a cloud-based multistage machine learning analytics pipeline which correlates threat behaviors seen in the enterprise with those seen globally.

The system analyzes user and device behavior to discover malware infections, command-and-control communications, data exfiltration, and potentially unwanted applications operating in an organization's infrastructure. There are multiple layers of processing, where a combination of techniques from artificial intelligence, machine learning and mathematical statistics helps the network to self-learn its normal activity so it can identify malicious activity.

This network security analytics pipeline, which collects telemetry from every part of the extended network, including encrypted traffic, is unique to Secure Network Analytics. It gradually builds a notion of "what is anomalous," then classifies actual individual pieces of "threat activity," and finally arrives at a final conviction of whether or not a device or user is in fact compromised. It is through a very careful analysis and correlation that we are able to bring in small pieces of evidence that all together will allow us to finally convict a compromised entity.

This capability is important because a typical enterprise may receive tons of alerts daily, and it's not possible for resource-strapped security teams to investigate all those alerts. The machine learning engine processes massive amounts of data in near real time to discover critical incidents with high confidence and is also able to suggest clear courses of actions to remediate quickly.

Source: <https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch/white-paper-c11-740605.pdf>

54. The Accused Products perform the encrypted traffic analysis and determination of response in real time.

Benefits of the solution

- **Enhanced visibility:** Gain insight into threats in encrypted traffic using network analytics and machine learning. Obtain contextual threat intelligence with real-time analysis correlated with user and device information
- **Cryptographic assessment:** Help ensure enterprise compliance with cryptographic protocols and visibility into and knowledge of not only what is being encrypted in the network, but also the strength of the encryption
- **Faster time to response:** Quickly contain infected devices and users by detecting threats within encrypted traffic in real time without relying on slow, decryption-based methods
- **Time and cost savings:** Use the network as the foundation for the security posture, capitalizing on security investments in the network

Source: <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/at-a-glance-c45-740079.pdf>

55. The Accused Products satisfy all claim limitations of one or more claims of the '249 Patent. Defendant has infringed and continues to directly infringe one or more claims of the '249 Patent by making, using, selling, and/or offering for sale in the United States and/or importing into the United States the Accused Products. To the extent that any element is not literally present, each such element is present under the doctrine of equivalents because it performs substantially

the same function in substantially the same way to achieve substantially the same result, and any differences between the Accused Products and claim element are insubstantial.

56. Defendant also knowingly and intentionally induces infringement of at least Claim 1 of the '249 Patent in violation of 35 U.S.C. § 271(b). Through at least the filing and service of this Complaint, Defendant has had knowledge of the '249 Patent and the infringing nature of the Accused Products. Despite this knowledge of the '249 Patent and its infringement, Defendant continues to actively encourage and instruct their customers and end users (for example, through user manuals and online instruction materials on its website and various service and customer support) to use the Accused Products in ways that directly infringe the '249 Patent. Defendant does so knowing and intending that its customers and end users will commit these infringing acts. Defendant also continues to make, use, offer for sale, sell, and/or import the Accused Products, despite their knowledge of the '249 Patent, thereby specifically intending for and inducing their customers to infringe the '249 Patent through the customers' normal and customary use of the Accused Products.

57. Defendant has also infringed, and continues to infringe, at least Claim 1 of the '249 Patent by selling, offering for sale, or importing into the United States, the Accused Products, knowing that the Accused Products constitute a material part of the inventions claimed in the '249 Patent, are especially made or adapted to infringe the '249 Patent, and are not staple articles or commodities of commerce suitable for non-infringing use. Defendant has been, and currently is, contributorily infringing the '249 Patent in violation of 35 U.S.C. §§ 271(c) and (f).

58. By making, using, offering for sale, selling and/or importing into the United States the Accused Products, Defendant has injured Plaintiff and is liable for infringement of the '249 Patent pursuant to 35 U.S.C. § 271.

59. As a result of Defendant's infringement of the '249 Patent, Plaintiff is entitled to monetary damages in an amount adequate to compensate for Defendant's infringement, but in no event less than a reasonable royalty for the use made of the invention by Defendant, together with interest and costs as fixed by the Court.

60. Defendant also has knowledge of the '249 Patent at least due to the filing of this Complaint, and based on that knowledge, Defendant willfully infringes the '249 Patent.

61. Defendant's infringing activities have injured and will continue to injure Plaintiff, unless and until this Court enters an injunction prohibiting further infringement of the '249 Patent, and, specifically, enjoining further manufacture, use, sale, importation, and/or offers for sale that come within the scope of the patent claims.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter:

(a) A judgment in favor of Plaintiff that Defendant has infringed the '824 Patent and the '249 Patent;

(b) A judgment and order requiring Defendant to pay Plaintiff its damages, costs, expenses, and pre-judgment and post-judgment interest for Defendant's infringement of the '824 Patent and the '249 Patent;

(c) A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees against Defendant;

(d) An award of enhanced damages to Plaintiff as a result of Defendant's willful infringement;

(e) An injunction prohibiting further infringement of the '824 Patent and the '249 Patent, and, specifically, enjoining further manufacture, use, sale, importation, and/or offers for sale that come within the scope of the patent claims; and

(f) Any and all other relief as the Court may deem appropriate and just under the circumstances.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, QPrivacy hereby demands a trial by jury on all issues so triable by right.

Dated: October 21, 2024

Respectfully submitted,

/s/ Robert M. Harkins

Elizabeth L. DeRieux
State Bar No. 05770585
Capshaw DeRieux, LLP
114 E. Commerce Ave.
Gladewater, TX 75647
Telephone: 903-845-5770
ccapshaw@capshawlaw.com
ederieux@capshawlaw.com

G. Blake Thompson
State Bar No. 24042033
Blake@TheMannFirm.com
J. Mark Mann
State Bar No. 12926150
Mark@TheMannFirm.com
MANN | TINDEL | THOMPSON
112 E. Line Street, Suite 304
Tyler, Texas 75702
(903) 657-8540
(903) 657-6003 (fax)

Robert M. Harkins
CA Bar No. 179525
Cherian LLP
2001 Addison St., Suite 275
Berkeley, CA 94704
bobh@cherianllp.com
Telephone: (510) 944-0190

Thomas M. Dunham
DC Bar No. 448407
Adam A. Allgood
TX Bar No. 24059403
Cherian LLP
1901 L St. NW, Suite 700
Washington, DC 20036
tomd@cherianllp.com
adama@cherianllp.com
Telephone: (202) 838-1560

Stephanie R. Wood
TX Bar No. 24057928

stephaniew@cherianllp.com

Cherian LLP

8350 N. Central Expressway, Suite 1900

Dallas, TX 75206

Telephone: (945) 205-0301

ATTORNEYS FOR PLAINTIFF

QPRIVACY USA LLC