

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF TEXAS  
TEXARKANA DIVISION

SABLE NETWORKS, INC. AND  
SABLE IP, LLC,

*Plaintiffs,*

v.

SPLUNK INC., SPLUNK SERVICES LLC,  
AND CRITICAL START INC.,

*Defendants.*

Civil Action No. 5:21-cv-00040-RWS

**JURY TRIAL DEMANDED**

**AMENDED COMPLAINT FOR PATENT INFRINGEMENT**

Sable Networks, Inc. and Sable IP, LLC (collectively, “Sable” or “Plaintiffs”) bring this action and make the following allegations of patent infringement relating to U.S. Patent Nos.: 7,630,358 (the “’358 patent”); 8,243,593 (the “’593 patent”); and 8,817,790 (the “’790 patent”) (collectively, the “patents-in-suit”). Defendants Splunk Inc. and Splunk Services, LLC (collectively, “Splunk”) infringes the ‘358, ‘593, and ‘790 patents in violation of the patent laws of the United States of America, 35 U.S.C. § 1 *et seq.* Defendants Splunk and Critical Start Inc. (“Critical Start”) (collectively, “Defendants”) infringe the ‘593 patent in violation of the patent laws of the United States of America, 35 U.S.C. § 1 *et seq.*

**INTRODUCTION**

1. The patents-in-suit arise from technologies developed by Dr. Lawrence G. Roberts - one of the founding fathers of the internet.<sup>1</sup> The patents relate to technologies for efficiently managing the flow of data packets over routers and switch devices. Dr. Roberts and engineers at

---

<sup>1</sup> Chris Woodford, THE INTERNET: A HISTORICAL ENCYCLOPEDIA VOLUME 2 at 204 (2005) (“Widely regarded as one of the founding fathers of the Internet, Lawrence Roberts was the primary architect of ARPANET, the predecessor of the Internet.”).

Caspian Networks, Inc. and later Sable Networks, Inc. developed these technologies to address the increasing amount of data sent over computer networks.

2. Dr. Roberts is best known for his work as the Chief Scientist of the Advanced Research Projects Agency (ARPA) where he designed and oversaw the implementation of ARPANET, the precursor to the internet. Dr. Roberts' work on ARPANET played a key role in the development of digital network transmission technologies.<sup>2</sup> Initially, ARPANET was used primarily to send electronic mail and Dr. Roberts developed the first program for reading and sending electronic messages.



Keenan Mayo and Peter Newcomb, *How The Web Was Won*, VANITY FAIR at 96-97 (January 7, 2009); *One of the Engineers Who Invented the Internet Wants to Build A Radical new Router*, IEEE SPECTRUM MAGAZINE (July 2009); Katie Hafner, *Billions Served Daily, and Counting*, N.Y. TIMES at G1 (December 6, 2001) (“Lawrence Roberts, who was then a manager at the Advanced Research Projects Agency’s Information Processing Techniques Office, solved that problem after his boss began complaining about the volume of e-mail piling up in his in box. In 1972, Dr. Roberts produced the first e-mail manager, called RD, which included a filing system, as well as a Delete function.”).

3. Dr. Roberts’ work on ARPANET played a key role in the development of packet switching networks. Packet switching is a digital network transmission process in which data is broken into parts which are sent independently and reassembled at a destination. Electronic

<sup>2</sup> Katie Hafner, *Lawrence Roberts, Who Helped Design Internet’s Precursor*, N.Y. TIMES at A2 (December 31, 2018) (“Dr. Roberts was considered the decisive force behind packet switching, the technology that breaks data into discrete bundles that are then sent along various paths around a network and reassembled at their destination.”).

messages sent over the ARPANET were broken up into packets then routed over a network to a destination. “In designing the ARPANET, Roberts expanded on the work he'd done at MIT, using those tiny data packets to send information from place to place.”<sup>3</sup> Packet switching has become the primary technology for data communications over computer networks.



George Johnson, *From Two Small Nodes, a Mighty Web Has Grown*, N.Y. TIMES at F1 (October 12, 1999).

4. After leaving ARPANET, Dr. Roberts grew increasingly concerned that existing technologies for routing data packets were incapable of addressing the increasing amounts of data traversing the internet.<sup>4</sup> Dr. Roberts identified that as the “Net grows, the more loss and transmission of data occurs. Eventually, gridlock will set in.”<sup>5</sup>

***The Internet is broken. I should know: I designed it.*** In 1967, I wrote the first plan for the ancestor of today's Internet, the Advanced Research Projects Agency Network, or ARPANET, and then led the team that designed and built it. The main idea was to share the available network infrastructure by sending data as small, independent packets, which, though they might arrive at different times, would still generally make it to their destinations. The small computers that directed the data

<sup>3</sup> Code Metz, *Larry Roberts Calls Himself the Founder of The Internet. Who Are You To Argue*, WIRED MAGAZINE (September 24, 2012); John C. McDonald, FUNDAMENTALS OF DIGITAL SWITCHING at 211 (1990) (“The ARPANET was, in part, an experimental verification of the packet switching concept. Robert’s objective was a new capability for resource sharing.”).

<sup>4</sup> eWeek Editors, *Feeling A Little Congested*, EWEEK MAGAZINE (September 24, 2001) (“Lawrence Roberts, one of the primary developers of Internet precursor ARPANet and CTO of Caspian Networks, recently released research indicating that Net traffic has quadrupled during the past year alone.”).

<sup>5</sup> Michael Cooney, *Can ATM Save The Internet*, NETWORK WORLD at 16 (May 20, 1996); Lawrence Roberts, A RADICAL NEW ROUTER, IEEE Spectrum Vol. 46 34-39 (August 2009).

traffic-I called them Interface Message Processors, or IMPs-evolved into today's routers, and for a long time they've kept up with the Net's phenomenal growth. Until now.

Lawrence Roberts, *A Radical New Router*, IEEE SPECTRUM Vol. 46(7) at 34 (August 2009) (emphasis added).

5. In 1998, Dr. Roberts founded Caspian Networks.<sup>6</sup> At Caspian Networks, Dr. Roberts developed a new kind of internet router to efficiently route packets over a network. This new router was aimed at addressing concerns about network “gridlock.” In a 2001 interview with Wired Magazine, Dr. Roberts discussed the router he was developing at Caspian Networks – the Apeiro. “Roberts says the Apeiro will also create new revenue streams for the carriers by solving the ‘voice and video problem.’ IP voice and video, unlike email and static Web pages, breaks down dramatically if there's a delay - as little as a few milliseconds - in getting packets from host to recipient.”<sup>7</sup>



Jim Duffy, *Router Newcomers take on Cisco, Juniper*, NETWORK WORLD at 14 (April 14, 2013); Stephen Lawson, *Caspian Testing Stellar Core Offering*, NETWORK WORLD at 33 (December 17, 2001); Tim Greene, *Caspian Plans Superfast Routing For The 'Net Core*, NETWORK WORLD at 10 (January 29, 2001); Andrew P. Madden, *Company Spotlight: Caspian Networks*, MIT TECHNOLOGY REVIEW at 33 (August 2005); and Loring Wirbel, *Caspian Moves Apeiro Router To Full Availability*, EE TIMES (April 14, 2003).

<sup>6</sup> Caspian Networks, Inc. was founded in 1998 as Packetcom, LLC and changed its name to Caspian Networks, Inc. in 1999.

<sup>7</sup> John McHugh, *The n-Dimensional Superswitch*, WIRED MAGAZINE (May 1, 2001).

6. The Apeiro debuted in 2003. The Apeiro, a flow-based router, can identify the nature of a packet – be it audio, text, or video, and prioritize it accordingly. The Apeiro included numerous technological advances including quality of service (QoS) routing and flow-based routing.

7. At its height, Caspian Networks Inc. raised more than \$300 million dollars and grew to more than 320 employees in the pursuit of developing and commercializing Dr. Roberts' groundbreaking networking technologies, including building flow-based routers that advanced quality of service and load balancing performance. However, despite early success with its technology and business, Caspian hit hard times when the telecommunications bubble burst.

8. Sable Networks, Inc. was formed by Dr. Sang Hwa Lee to further develop and commercialize the flow-based networking technologies developed by Dr. Roberts and Caspian Networks.<sup>8</sup> Sable Networks, Inc. has continued its product development efforts and has gained commercial success with customers in Japan, South Korea, and China. Customers of Sable Networks, Inc. have included: SK Telecom, NTT Bizlink, Hanaro Telecom, Dacom Corporation, USEN Corporation, Korea Telecom, China Unicom, China Telecom, and China Tietong.

---




<sup>8</sup> Dr. Lee, through his company Mobile Convergence, Ltd. purchased the assets of Caspian Networks Inc. and subsequently created Sable Networks, Inc.





*SK Telecom and Sable Networks Sign Convergence Network Deal*, COMMS UPDATE – TELECOM NEWS SERVICE (February 4, 2009) (“South Korean operator SK Telecom has announced that it has signed a deal with US-based network and solutions provider Sable Networks.”); *China Telecom Deploys Sable*, LIGHT READING NEWS FEED (November 19, 2007) (“Sable Networks Inc., a leading provider of service controllers, today announced that China Telecom Ltd, the largest landline telecom company in China, has deployed the Sable Networks Service Controller in their network.”).

9. Armed with the assets of Caspian Networks Inc. as well as members of Caspian Networks’ technical team, Sable Networks, Inc. continued the product development efforts stemming from Dr. Roberts’ flow-based router technologies. Sable Networks, Inc. developed custom application-specific integrated circuits (“ASIC”) designed for flow traffic management. Sable Network, Inc.’s ASICs include the Sable Networks SPI, which enables 20 Gigabit flow processing. In addition, Sable Networks, Inc. developed and released S-Series Service Controllers (e.g., S80 and S240 Service Controller models) that contain Sable Networks’ flow-based programmable ASICs, POS and Ethernet interfaces, and carrier-hardened routing and scalability from 10 to 800 Gigabits.

<b>S-Series Products</b>			
	<b>S240</b>	<b>S80</b>	<b>S20</b>
			
Throughput	240G Multi-Shelf System (Scales up to 720Gbps)	80G Single-Shelf System	20G Stand-Alone System
Interfaces	GIGE, 10GbE, POS	GigE, 10GbE, POS	GigE
Operation Mode	Transparent Mode / Routing Mode (BGPIOSPF...)		
Flow QoS	MR (Maximum Rate) / GR (Guaranteed Rate) / AR (Available Rate) / CR (Composite Rate)		
Flow Setup	1.5 M Flows / sec / Line Card		
Concurrent Flow	4 M Flows / Line Card		
Subscriber Management	8,000 Services Classification Rules / Line Card		

SABLE NETWORKS S-SERIES SERVICE CONTROLLERS (showing the S240-240G Multi-Shelf System, S80-80G Single-Shelf System, and S20-20G Stand-Alone System).

10. Sable pursues the reasonable royalties owed for Splunk's use of the inventions claimed in Sable's patent portfolio, which arise from Caspian Networks and Sable Networks' groundbreaking technology.

#### **SABLE'S PATENT PORTFOLIO**

11. Sable's patent portfolio includes over 34 patent assets, including 14 granted U.S. patents. Dr. Lawrence Roberts' pioneering work on QoS traffic prioritization, flow-based switching and routing, and the work of Dr. Roberts' colleagues at Caspian Networks Inc. and Sable Networks, Inc. are claimed in the various patents owned by Sable.

12. Highlighting the importance of the patents-in-suit is the fact that the Sable's patent portfolio has been cited by over 1,000 U.S. and international patents and patent applications assigned to a wide variety of the largest companies operating in the computer networking field. Sable's patents have been cited by companies such as:

- Cisco Systems, Inc.<sup>9</sup>

<sup>9</sup> See, e.g., U.S. Patent Nos. 7,411,965; 7,436,830; 7,539,499; 7,580,351; 7,702,765; 7,817,546; 7,936,695; 8,077,721; 8,493,867; 8,868,775; and 9,013,985.

- Juniper Networks, Inc.<sup>10</sup>
- Broadcom Limited<sup>11</sup>
- EMC Corporation<sup>12</sup>
- F5 Networks, Inc.<sup>13</sup>
- Verizon Communications Inc.<sup>14</sup>
- Microsoft Corporation<sup>15</sup>
- Intel Corporation<sup>16</sup>
- Extreme Networks, Inc.<sup>17</sup>
- Huawei Technologies Co., Ltd.<sup>18</sup>

### THE PARTIES

#### SABLE NETWORKS, INC.

13. Sable Networks, Inc. (“Sable Networks”) is a corporation organized and existing under the laws of the State of California.

14. Sable Networks was formed to continue the research, development, and commercialization work of Caspian Networks Inc., which was founded by Dr. Lawrence Roberts to provide flow-based switching and routing technologies to improve the efficiency and quality of computer networks.

15. Sable Networks is the owner by assignment of all of the patents-in-suit.

---

<sup>10</sup> See, e.g., U.S. Patent Nos. 7,463,639; 7,702,810; 7,826,375; 8,593,970; 8,717,889; 8,811,163; 8,811,183; 8,964,556; 9,032,089; 9,065,773; and 9,832,099.

<sup>11</sup> See, e.g., U.S. Patent No. 7,187,687; 7,206,283; 7,266,117; 7,596,139; 7,649,885; 8,014,315; 8,037,399; 8,170,044; 8,194,666; 8,271,859; 8,448,162; 8,493,988; 8,514,716; and 7,657,703.

<sup>12</sup> See, e.g., U.S. Patent Nos. 6,976,134; 7,185,062; 7,404,000; 7,421,509; 7,864,758; and 8,085,794.

<sup>13</sup> See, e.g., U.S. Patent Nos. 7,206,282; 7,580,353; 8,418,233; 8,565,088; 9,225,479; 9,106,606; 9,130,846; 9,210,177; 9,614,772; 9,967,331; and 9,832,069.

<sup>14</sup> See, e.g., U.S. Patent Nos. 7,349,393; 7,821,929; 8,218,569; 8,289,973; 9,282,113; and 8,913,623.

<sup>15</sup> See, e.g., U.S. Patent Nos. 7,567,504; 7,590,736; 7,669,235; 7,778,422; 7,941,309; 7,636,917; 9,571,550; and 9,800,592.

<sup>16</sup> See, e.g., U.S. Patent Nos. 7,177,956; 7,283,464; 9,485,178; 9,047,417; 8,718,096; 8,036,246; 8,493,852; and 8,730,984.

<sup>17</sup> See, e.g., U.S. Patent Nos. 7,903,654; 7,978,614; 8,149,839; 10,212,224; 9,112,780; and 8,395,996.

<sup>18</sup> See, e.g., U.S. Patent Nos. 7,903,553; 7,957,421; 10,015,079; 10,505,840; and Chinese Patent Nos. CN108028828 and CN106161333.



**SABLE IP, LLC**

16. Sable IP, LLC (“Sable IP”) is a Delaware limited liability company with its principal place of business at 225 S. 6th Street, Suite 3900, Minneapolis, Minnesota 55402. Pursuant to an exclusive license agreement with Sable Networks, Sable IP is the exclusive licensee of the patents-in-suit.

**SPLUNK DEFENDANTS**

17. Splunk Inc. is a Delaware corporation with its principal place of business at 270 Brannan Street, San Francisco, CA 94107. Splunk Inc. may be served through its registered agent National Registered Agents, Inc., 1999 Bryan Street, Suite 900, Dallas, TX 75201. Splunk Inc. is registered to do business in the State of Texas and has been since at least October 3, 2008.

18. Splunk Services LLC is a Delaware limited liability company with its principal place of business at 270 Brannan Street, San Francisco, CA 94107. Splunk Services LLC may be served through its registered agent National Registered Agents, Inc., 1209 Orange Street, Wilmington, DE 19801. Splunk Services LLC is a wholly-owned subsidiary of Splunk Inc.

19. Splunk Inc. conducts business operations within the Eastern District of Texas where it sells, develops, and/or markets its products, including facilities at 5360 Legacy Place, Ste. 250, Plano, Texas 75024.

**CRITICAL START INC.**

20. Critical Start, Inc. (“Critical Start”) is a Delaware corporation with its principal place of business at 6100 Tennyson Parkway, Suite 200, Plano, Texas 75024. Critical Start, Inc. may be served through its registered agent Northwest Registered Agent Service, Inc., 8 The Green, Suite B, Dover, Delaware 19901.

21. Critical Start conducts business operations within the Eastern District of Texas, including in its corporate headquarters in Plano, Texas, where Critical Start, Inc. sells, develops, and/or markets the product accused of infringement in this action.

**JURISDICTION AND VENUE**

22. This action arises under the patent laws of the United States, Title 35 of the United States Code. Accordingly, this Court has exclusive subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

23. This Court has personal jurisdiction over Defendants in this action because Defendants have committed acts within the Eastern District of Texas giving rise to this action and have established minimum contacts with this forum such that the exercise of jurisdiction over Defendants would not offend traditional notions of fair play and substantial justice. Defendants, directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), have committed and continue to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe one or more of the patents-in-suit. Moreover, Defendants have registered to do business in the State of Texas, have offices and facilities in the State of Texas, and actively direct their activities to customers located in the State of Texas.

24. Venue is proper in this district under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). Defendant Splunk is registered to do business in the State of Texas, has offices in the State of Texas, has transacted business in the Eastern District of Texas and has committed acts of direct and indirect infringement in the Eastern District of Texas. Defendant Critical Start is registered to do business in the State of Texas, has its principal office and headquarters in the Eastern District of Texas, and has committed acts of direct and indirect infringement in the Eastern District of Texas.

25. Defendants have regular and established places of business in this District and have committed acts of infringement in this District. Splunk has a permanent office location at 5360 Legacy Dr, Plano, Texas 75024, which is located within this District. Splunk employs full-time personnel such as sales personnel and engineers in this District, including in Plano, Texas. Splunk has also committed acts of infringement in this District by commercializing, marketing, selling, distributing, testing, and servicing certain accused products. Critical Start is headquartered out of its principal offices, located at 6100 Tennyson Pkwy, Suite 200, Plano, Texas 75024, which is in this District. Splunk has also committed acts of infringement in this District by marketing, selling, distributing, testing, and servicing certain accused products.

26. This Court has personal jurisdiction over Defendants. Defendants have conducted and does conduct business within the State of Texas. Defendants, directly or through subsidiaries or intermediaries (including distributors, retailers, and others), ship, distribute, make, use, offer for sale, sell, import, and/or advertise (including by providing interactive web pages) their products and/or services in the United States and the Eastern District of Texas and/or contribute to and actively induce customers to ship, distribute, make, use, offer for sale, sell, import, and/or advertise (including the provision of an interactive web page) infringing products and/or services in the United States and the Eastern District of Texas. Defendants, directly and through subsidiaries or intermediaries (including distributors, retailers, and others), have purposefully and voluntarily placed one or more infringing products and/or services, as described below, into the stream of commerce with the expectation that those products will be purchased and used by customers and/or consumers in the Eastern District of Texas. These infringing products and/or services have been and continue to be made, used, sold, offered for sale, purchased, and/or imported by customers and/or consumers in the Eastern District of Texas. Defendants have committed acts of patent

infringement within the Eastern District of Texas. Defendants interact with customers in Texas, including through visits to customer sites in Texas. Through these interactions and visits, Defendants directly infringe one or more of the patents-in-suit. Defendants also interact with customers who sell the accused products into Texas, knowing that these customers will sell the accused products into Texas, either directly or through intermediaries.

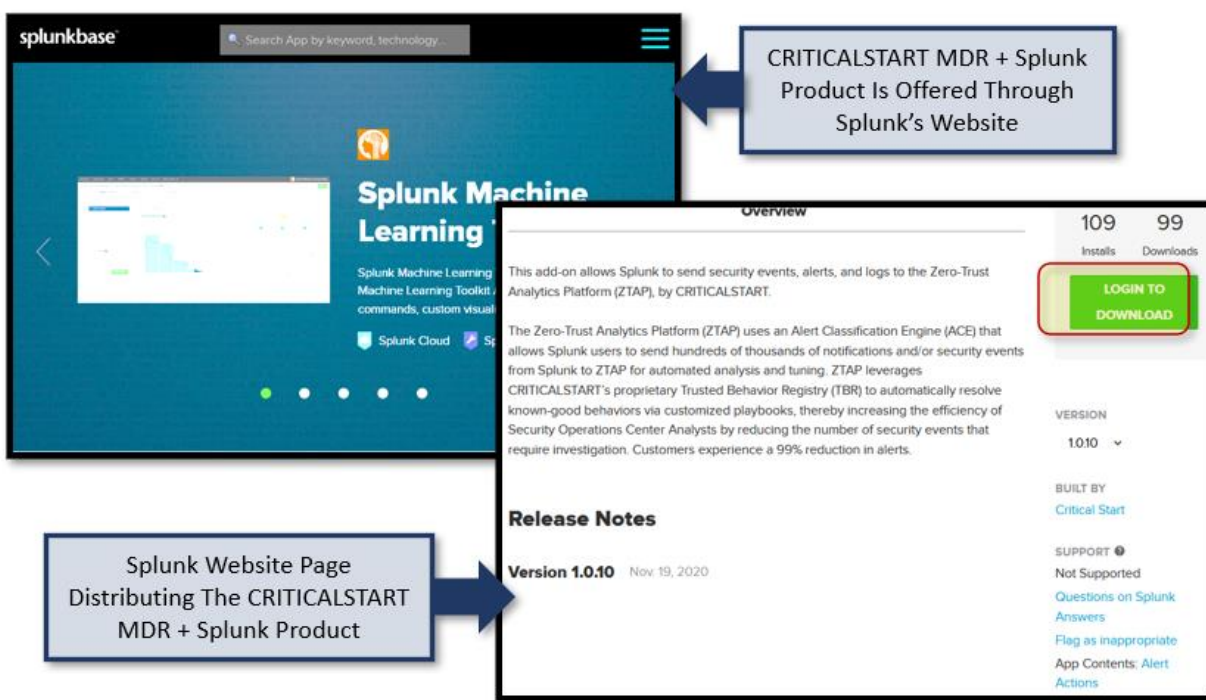
27. Defendants have minimum contacts with this District such that the maintenance of this action within this District would not offend traditional notions of fair play and substantial justice. Thus, the Court therefore has both general and specific personal jurisdiction over Defendants.

**THE SPLUNK-CRITICAL START JOINT PRODUCT OFFERING**

28. Joinder of the Defendants is proper under 35 U.S.C. § 299. Common questions of fact relating to Defendants' infringement arise in this action. These common questions include questions of fact and law concerning Splunk and Critical Start's infringement of the '593 patent through the incorporation of common packet processing components in the accused CRITICALSTART MDR + Splunk offering. Common questions of fact as to the profits and revenues derived by Splunk and Critical Start will arise. Common questions of fact will also exist with regard to Splunk and Critical Start's defenses, if any, in this litigation.

29. The allegations of patent infringement contained herein arise out of the same series of transactions or occurrences relating to the making, using, selling, offering for sale, and/or importing within the United States, the products accused of infringing the '593 patent — CRITICALSTART MDR + Splunk offering which includes: CriticalSTART Managed SIEM Services for Splunk, Splunk Enterprise Versions 7.2 and later, the Zero Trust Analytics Platform (ZTAP), and the Critical Start Security Operations Add-on.

30. This joint offering is made available by Splunk and Critical Start. For example, users of the CRITICALSTART MDR + Splunk offering are instructed by Critical Start to download the product offering from Splunk. Specifically, the Critical Start Security Operations Add-on is hosted by, distributed from, and downloadable on Splunk's website and servers.



SPLUNKBASE.COM WEBSITE - CRITICAL START SECURITY OPERATIONS ADD-ON (last visited June 2021), *available at*: <https://splunkbase.splunk.com/> (annotation added).

31. Splunk Enterprise and Splunk Cloud are specifically developed, marketed, licensed and distributed by Splunk to be used in offerings such as the CRITICALSTART MDR + Splunk Product offering.

32. Splunk is liable for induced and contributory infringement of the '593 Patent based on forming a joint enterprise with Critical Start with respect to building and/or distributing Splunk Enterprise, Splunk Cloud, and the Critical Start Security Operations Module which are specifically built to perform the infringing functionality.



Splunk Enterprise and Splunk Enterprise Security are Gartner-recognized leaders in the SIEM market. However, they also suffer from the same alert-overload problem as other SIEMs. Because of this, Splunk and ATA<sup>19</sup> formed a partnership to provide “out of the box” integration between the ATA Platform and Splunk. For Splunk customers, this partnership provides the best of both worlds: they can continue to benefit from Splunk’s deep monitoring, analysis and investigative capabilities, but improve overall system and employee efficiency by reducing the number of events required for investigation. This, in turn, requires fewer staff to investigate security events, which gives operations managers new flexibility in staff configuration and budget prioritization.

*Advanced Threat Analytics for Splunk*, CRITICAL START’S ADVANCED THREAT ANALYTICS WEBSITE (last visited June 2021), available at: <https://www.advancedthreatanalytics.com/solutions-ata-for-splunk> (emphasis added).

33. The CRITICALSTART MDR + Splunk Product is based on a partnership between Critical Start and Splunk and is described in Critical Start’s documentation as the “CRITICALSTART MDR-+Splunk” “complete offering.” The following excerpt from a 2020 article from the Critical Start website describes the CRITICALSTART MDR-+Splunk Product as the result of a “Partnership” between Critical Start and Splunk.

---

<sup>19</sup> The CRITICALSTART MDR + Splunk product was initially offered by Advanced Threat Analytics, Inc. (“ATA”) which was purchased by Critical Start in 2018.

### Capability Comparison

	CRITICALSTART MDR + Splunk	Arctic Wolf	eSentire	Secureworks
Cloud-Native SIEM offering	●	●	○	○
Custom Use Cases	●	×	×	●
MDR Platform with Trusted Behavior Registry that resolves 100% of alerts	●	×	×	×
Native iOS and Android applications for alert investigation, collaboration and response	●	×	×	×
Multi-Tenant so client can have multiple organizations with N-level hierarchy	●	●	●	×
Manage and report on all alerts from SIEM and EDR in one platform	●	○	×	●
Review process available to customers, providing transparent quality control for analyst investigations	●	×	×	×
Contractually guaranteed Service Level Agreement for Analyst Time to Detect and Respond to Alert (as compared to SLO)	●	×	×	○

● Complete Offering
○ Partial Offering
× No offering

*Critical Start Managed SIEM Services for Splunk, CRITICAL START DOCUMENTATION (2020) (annotation added).*

34. Splunk’s relationship with Critical Start goes beyond simply selling Splunk components. Because the selection and incorporation process for technology in the CRITICALSTART MDR + Splunk Product offering is a lengthy one, Critical Start works closely with Splunk to “define” and “design” products placed in the CRITICALSTART MDR + Splunk Product offering. Critical Start’s documentation states, “CRITICALSTART will provide Security Monitoring and Event Management (“SIEM”) services via Splunk including: rule writing, report generation, alert generation and incident workflow.”

35. Splunk and Critical Start share a community of pecuniary interests in the development and distribution of the CRITICALSTART MDR + Splunk Product offering. For example, upon information and belief, there are indemnification and revenue provisions, as set forth in the agreements between the two companies. Both Splunk and Critical Start derive financial benefit from the development and distribution of the CRITICALSTART MDR + Splunk Product offering.

36. Splunk-provided components contained in the CRITICALSTART MDR + Splunk Product offering have been identified by Critical Start as providing a “complete offering” when offering as part of the CRITICALSTART MDR + Splunk Product.<sup>20</sup>

37. Splunk and Critical Start have represented to the public that they have “partnered” and are jointly providing a “complete offering” through the CRITICALSTART MDR + Splunk Product offering.

38. Splunk conditions both the manner and timing of the performance of steps by Critical Start in building and distributing the CRITICALSTART MDR + Splunk Product offerings.

---

<sup>20</sup> *CriticalStart Managed SIEM Services for Splunk*, CRITICAL START DOCUMENTATION AT 2 (2020).

39. The inclusion of the Splunk components in the CRITICALSTART MDR + Splunk Product offerings has been described as offering “comprehensive insights” in the CRITICALSTART MDR + Splunk Product offerings. Further, Critical Start hosts and maintains the CRITICALSTART MDR + Splunk Product offerings at data centers and other points-of-presence. Critical management of the CRITICALSTART MDR + Splunk Product offering is conducted in Plano, Texas by Critical Start. The following is an excerpt from a third-party report on the CRITICALSTART MDR + Splunk Product offering.

The operations and corporate facilities are located in Plano, TX. Critical Start, Inc. utilizes a combination local area network (“LAN”) / wide area network (“WAN”) to share data among its employees. The corporate IT data center is located in the headquarters facility, contains no production/customer systems or data, and is accessible 24 hours a day, 7 days a week, and 365 days a year to authorized Critical Start personnel. Critical Start uses internal IT expertise and follows internal business and IT policies and procedures to support its daily IT administration and service operation.

*Independent SOC 3 Report for Security and Privacy Trust Services Criteria for Critical Start, Inc., SYSTEM AND ORGANIZATION CONTROLS 3 (SOC) 3 REPORT at 9 (October 2020).*

40. Critical Start jointly offers the CRITICALSTART MDR + Splunk Product including through deploying Splunk Indexers, Search Heads, and Forward/Deployment Servers. In 2020, Critical Start commissioned a report on its Professional Services and Managed Detection and Response (MDR) System from a third-party to verify its statements regarding the CRITICALSTART MDR + Splunk Product were accurate. The report described the deployment of Splunk products by Critical Start in the CRITICALSTART MDR + Splunk product offering.

The production elements deployed on site at a customer for Splunk include:

- The UF contains only the components that are necessary to forward data. The UF gets data from a variety of inputs and forwards the data to a Splunk deployment for indexing and searching. It can also forward data to another forwarder as an intermediate step before sending the data onward to an indexer.
- A heavy forwarder is a full Splunk Enterprise instance that can index, search, and change data as well as forward it. The heavy forwarder has some features disabled to reduce system resource usage.

*Independent SOC 3 Report for Security and Privacy Trust Services Criteria for Critical Start, Inc., SYSTEM AND ORGANIZATION CONTROLS 3 (SOC) 3 REPORT at 9 (October 2020).*

41. Splunk offers, distributes, and maintains components of the CRITICALSTART MDR + Splunk Product offerings on websites, web servers, and data centers. These websites include [www.splunkbase.com](http://www.splunkbase.com) where customers of the CRITICALSTART MDR + Splunk Product offering are required to create a Splunk Account and download the Critical Start Security Operations module from a Splunk web server.

### **THE ASSERTED PATENTS**

#### **U.S. PATENT NO. 7,630,358**

42. U.S. Patent No. 7,630,358 (“the ‘358 patent”) entitled, *Mechanism for Implementing Multiple Logical Routers Within A Single Physical Router*, was filed on July 9, 2002, and claims priority to July 9, 2001. The ‘358 patent is subject to a 35 U.S.C. § 154(b) term extension of 1,136 days. Sable Networks, Inc. is the owner by assignment of the ‘358 patent. Sable IP is the exclusive licensee of the ‘358 patent. A true and correct copy of the ‘358 patent is attached hereto as Exhibit A.

43. The ‘358 patent claims specific methods and systems for implementing multiple logical routers within a single physical router.



44. The '358 patent discloses systems and methods that combine the benefits of multi-routers and virtual routers. The logical routers are included within the same physical router; however, internal links permit improved efficiency over virtual routers because the technologies claimed in the '358 patent can take advantage of the fact that the logical routers are not standalone routers but are embodied in the same physical router.

45. The '358 patent discloses technology for implementing multiple logical routers within a single physical router.

46. The '358 patent discloses a router with a first set of one or more components capable of being configured to implement a first logical router within the router.

47. The '358 patent discloses a router with a second set of one or more components capable of being configured to implement a second logical router within the router.

48. The '358 patent discloses a router with a forwarding routing table that comprises an identifier that indicates an internal link is internal rather than an external link.

49. The '358 patent discloses a router wherein the first and second sets of components comprise functionality for establishing the internal link between the first logical router and the second logical router and advertising the internal link to other routers external to the router such that the first and second logical routers appear to the other routers as interconnected standalone routers, wherein the internal link is a logical, non-physical entity.

50. The '358 patent has been cited by 42 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have all cited the '358 patent as relevant prior art:

- Cisco Systems, Inc.
- Dell Technologies, Inc.
- Juniper Networks, Inc.
- Nicira, Inc.

- International Business Machines Corporation
- NantWorks, LLC
- Telefonaktiebolaget LM Ericsson
- Verizon Communications, Inc.

**U.S. PATENT NO. 8,243,593**

51. U.S. Patent No. 8,243,593 entitled, *Mechanism for Identifying and Penalizing Misbehaving Flows in a Network*, was filed on December 22, 2004. The '593 patent is subject to a 35 U.S.C. § 154(b) term extension of 1,098 days. Sable Networks, Inc. is the owner by assignment of the '593 patent. Sable IP is the exclusive licensee of the '593 patent. A true and correct copy of the '593 patent is attached hereto as Exhibit B.

52. The '593 patent discloses novel methods and systems for processing a flow of a series of information packets.

53. The inventions disclosed in the '593 patent teach technologies that permit the identification and control of less desirable network traffic.

54. Because the characteristics of data packets in undesirable network traffic can be disguised, the '593 patent improves the operation of computer networks by disclosing technologies that monitor the characteristics of flows of data packets rather than ancillary factors such as port numbers or signatures.

55. The '593 patent discloses tracking the behavioral statistics of a flow of data packets that can be used to determine whether the flow is undesirable.

56. The '593 patent further discloses taking actions to penalize the flow of undesirable network traffic.

57. The '593 patent discloses a method for processing a flow of a series of information packets that maintains a set of behavioral statistics for the flow, wherein the set of behavioral

statistics is updated based on each information packet belonging to the flow, as each information packet is processed.

58. The '593 patent discloses a method for processing a flow of a series of information packets that determines, based at least partially upon the set of behavioral statistics, whether the flow is exhibiting undesirable behavior.

59. The '593 patent discloses that the determination as to whether the flow is exhibiting undesirable behavior is made regardless of the presence or absence of congestion.

60. The '593 patent discloses a method for processing a flow of data packets that enforces a penalty on the flow in response to a determination that the flow is exhibiting undesirable behavior.

61. The '593 patent has been cited by 17 patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '593 patent as relevant prior art.

- Cisco Systems, Inc.
- AT&T, Inc.
- International Business Machines Corporation
- Telecom Italia S.p.A.
- McAfee, LLC

**U.S. PATENT NO. 8,817,790**

62. U.S. Patent No. 8,817,790 (the “‘790 patent”) entitled, *Identifying Flows Based on Behavior Characteristics and Applying User-Defined Actions*, was filed on September 23, 2011, and claims priority to July 31, 2006. Sable Networks, Inc. is the owner by assignment of the ‘790 patent. Sable IP is the exclusive licensee of the ‘790 patent. A true and correct copy of the ‘790 patent is attached hereto as Exhibit C.

63. The '790 patent claims specific methods and devices for handling a flow of information packets.

64. The '790 patent discloses methods and systems for efficiently identifying undesirable traffic over data networks.

65. The '790 patent teaches technologies that identify traffic not by inspecting the payload of each data packet, but rather by analyzing and classifying the behavior of the data flows to identify undesirable traffic.

66. The '790 patent discloses applying a user-specified action associated with a policy applicable to data flows that are designated undesirable.

67. The '790 patent discloses a method of handling a flow that processes a flow comprised of two or more information packets having header information in common.

68. The '790 patent discloses a method of handling a flow that stores header-independent statistics about the flow in a flow block associated with the flow.

69. The '790 patent discloses a method of handling a flow that updates the header-independent statistics in the flow block as each information packet belonging to the flow is processed.

70. The '790 patent discloses a method of handling a flow that categorizes the flow as one or more traffic types by determining whether the header-independent statistics match one or more profiles corresponding to a traffic type.

71. The '790 patent discloses a method of handling a flow that performs an operation that is determined according to the one or more traffic types on one or more information packets belonging to the flow if the one or more traffic types match one or more particular traffic types designated by a user.

72. The ‘790 patent family has been cited by 24 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘790 patent family as relevant prior art:

- Cisco Systems, Inc.
- Solana Networks, Inc.
- British Telecommunications Public Limited Company
- Level 3 Communications, LLC
- Calix, Inc.
- Nokia Corporation
- Verizon Communications, Inc.
- Sprint Spectrum L.P.
- Hon Hai Precision Industry Co., Ltd.

**COUNT I**  
**INFRINGEMENT OF U.S. PATENT NO. 7,630,358**

73. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

74. Splunk designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for implementing multiple logical routers within a single physical router.

75. Splunk designs, makes, sells, offers to sell, imports, and/or uses Splunk Enterprise Versions 6.5 and later, which incorporate universal forwarders, heavy forwarders, load balancing, data routing, pipeline sets, and/or index parallelization functionality (the “Splunk ‘358 Product(s)”).

76. One or more Splunk subsidiaries and/or affiliates use the Splunk ‘358 Products in regular business operations.

77. One or more of the Splunk ‘358 Products include technology for implementing multiple logical routers within a single physical router.

78. One or more of the Splunk ‘358 Products include a router with a first set of one or more components capable of being figured to implement a first logical router within the router.



79. One or more of the Splunk '358 Products include a router with a second set of one or more components capable of being configured to implement a second logical router within the router.

80. One or more of the Splunk '358 Products include a router with a forwarding routing table that comprises an identifier that indicates an internal link is internal rather than an external link.

81. One or more of the Splunk '358 Products include a router wherein the first and second sets of components comprise functionality for establishing the internal link between the first logical router and the second logical router and advertising the internal link to other routers external to the router such that the first and second logical routers appear to the other routers as interconnected standalone routers, wherein the internal link is a logical, non-physical entity.

82. The Splunk '358 Products are available to businesses and individuals throughout the United States.

83. The Splunk '358 Products are provided to businesses and individuals located in the Eastern District of Texas.

84. Splunk has directly infringed and continues to directly infringe the '358 patent by, among other things, making, using, offering for sale, and/or selling routers implementing multiple logical routers within a single physical router, including but not limited to the Splunk '358 Products.

85. By making, using, testing, offering for sale, and/or selling routers implementing multiple logical routers within a single physical router, including but not limited to the Splunk '358 Products, Splunk has injured Plaintiffs and is liable for directly infringing one or more claims of the '358 patent, including at least claim 1, pursuant to 35 U.S.C. § 271(a).

86. Splunk also indirectly infringes the ‘358 patent by actively inducing infringement under 35 USC § 271(b).

87. Splunk has had knowledge of the ‘358 patent since at least service of this Complaint or shortly thereafter, and Splunk knew of the ‘358 patent and knew of its infringement, including by way of this lawsuit.

88. Splunk intended to induce patent infringement by third-party customers and users of the Splunk ‘358 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Splunk specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘358 patent. Splunk performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘358 patent and with the knowledge that the induced acts would constitute infringement. For example, Splunk provides the Splunk ‘358 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘358 patent, including at least claim 1, and Splunk further provides documentation and training materials that cause customers and end users of the Splunk ‘358 Products to utilize the products in a manner that directly infringe one or more claims of the ‘358 patent.<sup>21</sup> By

---

<sup>21</sup> See, e.g., *Splunk Enterprise Forwarding Data 8.1.3*, SPLUNK DOCUMENTATION (2021); *Splunk Universal Forwarder Manual 8.1.3*, SPLUNK DOCUMENTATION (2021); *Troubleshooting Universal Forwarder On Linux*, SPLUNK DOCUMENTATION (2017); *Splunk Event Processing V20 Universal Forwarding Indexer*, SPLUNK DOCUMENTATION (2019); *Splunk Validated Architectures*, SPLUNK WHITE PAPER (January 2021); Amrit Bath and Abhinav Nekkanti, *How Splunk Works*, SPLUNK .CONF2017 PRESENTATION (2017); *Splunk Enterprise Admin Manual 8.1.3*, SPLUNK DOCUMENTATION (2019); Abhinav Nekkanti, Sourav Pal, and Tameem Anwar, *Harnessing Performance and Scalability with Parallelization*, SPLUNK .CONF2016 PRESENTATION (2016); *Splunk Enterprise Managing Indexers And Clusters Of Indexers 8.1.3*, SPLUNK DOCUMENTATION (2021); Harendra Rawat, *How To Troubleshoot Blocked Ingestion Pipeline Queues With Indexers and Forwarders*, SPLUNK .CONF2019 PRESENTATION (2019); Abhinav Nekkanti, Tameem Anwar, and Sourav Pal, *Harnessing 6.3 Performance And Scalability*, SPLUNK .CONF2015 PRESENTATION (2015); Simon O’Brien and Vinu Alazath, *FN1206: The Path To Operational Enlightenment – An Introduction To Wire Data*, SPLUNK .CONF2019 PRESENTATION (2019); Ben Marcus, *PLA1906C: Starting Your Splunk Journey Get Your Data In*, SPLUNK .CONF2020 PRESENTATION (2020); *Splunk Enterprise 6:2: Forwarders*

providing instruction and training to customers and end-users on how to use the Splunk ‘358 Products in a manner that directly infringes one or more claims of the ‘358 patent, including at least claim 1, Splunk specifically intended to induce infringement of the ‘358 patent. Splunk engaged in such inducement to promote the sales of the Splunk ‘358 Products, e.g., through Splunk user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘358 patent. Accordingly, Splunk has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘358 patent, knowing that such use constitutes infringement of the ‘358 patent.

89. The ‘358 patent is well-known within the industry as demonstrated by multiple citations to the ‘358 patent in published patents and patent applications assigned to technology companies and academic institutions. Splunk is utilizing the technology claimed in the ‘358 patent without paying a reasonable royalty. Splunk is infringing the ‘358 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

90. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘358 patent.

91. As a result of Splunk’s infringement of the ‘358 patent, Plaintiffs have suffered monetary damages, and seeks recovery in an amount adequate to compensate for Splunk’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Splunk together with interest and costs as fixed by the Court.

---

*Tech Brief*, SPLUNK DOCUMENTATION (2014); David J. Cavuto, *Service and Asset Discovery With Wire Data*, SPLUNK .CONF2019 PRESENTATION (2019).

**COUNT II**  
**INFRINGEMENT OF U.S. PATENT NO. 8,243,593**

92. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

93. Splunk designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for processing a flow of a series of information packets.

94. Splunk designs, makes, sells, offers to sell, imports, and/or uses Splunk Data Stream Processor 1.2.0, Splunk Data Stream Processor 1.1.0, and Splunk Data Stream Processor 1.0.1 (collectively, the “Splunk ‘593 Product(s)”).

95. One or more Splunk subsidiaries and/or affiliates use the Splunk ‘593 Products in regular business operations.

96. One or more of the Splunk ‘593 Products include technology for processing a flow of a series of information packets. Specifically, the Splunk ‘593 Products maintain a set of behavioral statistics based on each and every information packet belonging to a flow.

97. The Splunk ‘593 Products are available to businesses and individuals throughout the United States.

98. The Splunk ‘593 Products are provided to businesses and individuals located in the Eastern District of Texas.

99. Splunk has directly infringed and continues to directly infringe the ‘593 patent by, among other things, making, using, offering for sale, and/or selling products and services for processing a flow of a series of information packets.

100. The Splunk ‘593 Products maintain a set of behavioral statistics for the flow, wherein the set of behavioral statistics is updated based on each information packet belonging to

the flow, as each information packet is processed, regardless of the presence or absence of congestion.

101. By making, using, testing, offering for sale, and/or selling products and services for processing a flow of a series of information packets, including but not limited to the Splunk ‘593 Products, Splunk has injured Plaintiffs and is liable for directly infringing one or more claims of the ‘593 patent, including at least claim 9, pursuant to 35 U.S.C. § 271(a).

102. Splunk also indirectly infringes the ‘593 patent by actively inducing infringement under 35 USC § 271(b).

103. Splunk has had knowledge of the ‘593 patent since at least service of this Complaint or shortly thereafter, and Splunk knew of the ‘593 patent and knew of its infringement, including by way of this lawsuit.

104. Splunk intended to induce patent infringement by third-party customers and users of the Splunk ‘593 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Splunk specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘593 patent. Splunk performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘593 patent and with the knowledge that the induced acts would constitute infringement. For example, Splunk provides the Splunk ‘593 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘593 patent, including at least claim 9, and Splunk further provides documentation and training materials that cause customers and end users of the Splunk ‘593 Products to utilize the products in a manner that directly infringe one or more claims of the ‘593 patent.<sup>22</sup> By

---

<sup>22</sup> See, e.g., *Splunk Data Stream Processor - Use the Data Stream Processor 1.2.0*, SPLUNK DOCUMENTATION (2021); *Splunk Data Stream Processor - Function Reference 1.2.0*, SPLUNK



providing instruction and training to customers and end-users on how to use the Splunk ‘593 Products in a manner that directly infringes one or more claims of the ‘593 patent, including at least claim 9, Splunk specifically intended to induce infringement of the ‘593 patent. Splunk engaged in such inducement to promote the sales of the Splunk ‘593 Products, e.g., through Splunk user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘593 patent. Accordingly, Splunk has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘593 patent, knowing that such use constitutes infringement of the ‘593 patent.

105. The ‘593 patent is well-known within the industry as demonstrated by multiple citations to the ‘593 patent in published patents and patent applications assigned to technology companies and academic institutions. Splunk is utilizing the technology claimed in the ‘593 patent without paying a reasonable royalty. Splunk is infringing the ‘593 patent in a manner best

---

DOCUMENTATION (2021); Ram Sriharsha and Harsha Wasalathanthri, *Unbounded Learning On Streams*, SPLUNK .CONF2019 PRESENTATION (2019); Ed Sale and Bill Muller, *Splunk DSP: Rapid, Automated, Repeatable Data Ingest – DSP + Automation = Rapid Deployment*, SPLUNK .CONF2020 PRESENTATION (2020); Poornima Devaraj and Jove Zhong, *Collect Service: Introducing A New Ingest Model*, SPLUNK .CONF2019 PRESENTATION (2019); *Splunk Data Stream Processor Deep Dive + Demonstration*, SPLUNK YOUTUBE CHANNEL (October 17, 2019), available at: <https://www.youtube.com/watch?v=WNN8EOVoBXs>; *Splunk Data Stream Processor - Install and administer the Data Stream Processor 1.2.0*, SPLUNK DOCUMENTATION (2021); Dirk Nitschke and Bashar Abdul-Jawad, *Using Splunk Stream Processor As A Data Transformation, Alerting And Action Engine*, SPLUNK .CONF2019 PRESENTATION (2019); Blaine Wastell and Thor Taylor, *FN20602: Data Stream Processor: How To Get The Most Out Of Your Data!*, SPLUNK .CONF2019 PRESENTATION (2019); Jamie Grier, *Splunk Data Stream Processor*, FLINK FORWARD YOUTUBE CHANNEL (October 28, 2020), available at: <https://www.youtube.com/watch?v=0pJQWwy33pE>; Thor Taylor and Poornima Devaraj, *PLA1735A: Getting to Know Splunk’s Data Streaming Technology*, SPLUNK .CONF2020 PRESENTATION (2020); Thor Taylor and Adam Lamar, *FN1987: Using Splunk Data Stream Processor As A Streaming Engine For Apache Kafka*, SPLUNK .CONF2019 PRESENTATION (2019); and *Splunk Data Stream Processor: Connect to Data Sources and Destinations with DSP 1.2.0*, SPLUNK DOCUMENTATION (2021).

described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

106. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘593 patent.

107. As a result of Splunk’s infringement of the ‘593 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Splunk’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Splunk together with interest and costs as fixed by the Court.

**COUNT III**  
**INFRINGEMENT OF U.S. PATENT NO. 8,243,593**

108. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

109. Splunk and Critical Start design, make, use, sell, and/or offer for sale in the United States products and/or services for processing a flow of a series of information packets.

110. Splunk and Critical Start design, make, sell, offer to sell, import, and/or use the CRITICALSTART MDR + Splunk Product offering<sup>23</sup> (the “CRITICALSTART+Splunk ‘593 Product(s)”).

111. One or more Splunk subsidiaries and/or affiliates use the CRITICALSTART+Splunk ‘593 Products in regular business operations.

112. One or more Critical Start subsidiaries and/or affiliates use the CRITICALSTART+Splunk ‘593 Products in regular business operations.

---

<sup>23</sup> *Splunk & Critical Start Solution Webpage*, CRITICAL START WEBSITE (last visited June 2021), available at: <https://www.criticalstart.com/our-solutions/managed-detection-response-services/siem/splunk>; *Critical Start Security Operations*, SPLUNKBASE WEBSITE (last visited June 2021), available at: <https://splunkbase.splunk.com/app/5252/> ./

113. One or more of the CRITICALSTART+Splunk '593 Products include technology for processing a flow of a series of information packets. Specifically, the CRITICALSTART+Splunk '593 Products maintain a set of behavioral statistics based on each and every information packet belonging to a flow.

114. The CRITICALSTART+Splunk '593 Products are available to businesses and individuals throughout the United States.

115. The CRITICALSTART+Splunk '593 Products are provided to businesses and individuals located in the Eastern District of Texas.

116. Splunk and Critical Start directly infringe and continue to directly infringe the '593 patent by, among other things, making, using, offering for sale, and/or selling products and services for processing a flow of a series of information packets.

117. The CRITICALSTART+Splunk '593 Products maintain a set of behavioral statistics for the flow, wherein the set of behavioral statistics is updated based on each information packet belonging to the flow, as each information packet is processed, regardless of the presence or absence of congestion.

118. The CRITICALSTART+Splunk '593 Products compute a badness factor for the flow based at least partially upon the set of behavioral statistics, wherein the badness factor provides an indication of whether the flow is exhibiting undesirable behavior.

119. By making, using, testing, offering for sale, and/or selling products and services for processing a flow of a series of information packets, including but not limited to the CRITICALSTART+Splunk '593 Products, Splunk and Critical Start have injured Plaintiffs and are liable for directly infringing one or more claims of the '593 patent, including at least claim 10, pursuant to 35 U.S.C. § 271(a).

120. Splunk and Critical Start also indirectly infringe the ‘593 patent by actively inducing infringement under 35 USC § 271(b).

121. Splunk has had knowledge of the ‘593 patent since at least service of the original Complaint in this matter or shortly thereafter, and Splunk knew of the ‘593 patent and knew of its infringement, including by way of this lawsuit at least since March 29, 2021.

122. Critical Start has had knowledge of the ‘593 patent since at least service of this Amended Complaint in this matter or shortly thereafter, and Critical Start knew of the ‘593 patent and knew of its infringement, including by way of this lawsuit.

123. Splunk and Critical Start intended to induce patent infringement by third-party customers and users of the CRITICALSTART+Splunk ‘593 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Splunk and Critical Start specifically intended and were aware that the normal and customary use of the accused products would infringe the ‘593 patent. Splunk and Critical Start performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘593 patent and with the knowledge that the induced acts would constitute infringement. For example, Splunk and Critical Start provide the CRITICALSTART+Splunk ‘593 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘593 patent, including at least claim 10, and Splunk and Critical Start further provide documentation and training materials that cause customers and end users of the CRITICALSTART+Splunk ‘593 Products to utilize the products in a manner that directly infringe one or more claims of the ‘593 patent.<sup>24</sup> By providing instruction and training to

---

<sup>24</sup> See, e.g., *Critical Start Services Descriptions Overview*, CRITICAL START DOCUMENTATION v06.2020 (2020); *Independent SOC 3 Report for Security and Privacy Trust Services Criteria for Critical Start, Inc.*, SYSTEM AND ORGANIZATION CONTROLS 3 (SOC) 3 REPORT (October 2020); *Splunk & Critical Start Solution Webpage*, CRITICAL START WEBSITE (last visited June

customers and end-users on how to use the CRITICALSTART+Splunk ‘593 Products in a manner that directly infringes one or more claims of the ‘593 patent, including at least claim 10, Splunk and Critical Start specifically intended to induce infringement of the ‘593 patent. Splunk and Critical Start engaged in such inducement to promote the sales of the CRITICALSTART+Splunk ‘593 Products, e.g., through Splunk and Critical Start user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘593 patent. Accordingly, Splunk and Critical Start have induced and continue to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘593 patent, knowing that such use constitutes infringement of the ‘593 patent.

124. The ‘593 patent is well-known within the industry as demonstrated by multiple citations to the ‘593 patent in published patents and patent applications assigned to technology

---

2021), available at: <https://www.criticalstart.com/our-solutions/managed-detection-response-services/siem/splunk>; *Critical Start Security Operations*, SPLUNKBASE WEBSITE (last visited June 2021), available at: <https://splunkbase.splunk.com/app/5252/>; *Advanced Threat Analytics for Splunk*, CRITICAL START’S ADVANCED THREAT ANALYTICS WEBSITE (last visited June 2021), available at: <https://www.advancedthreatanalytics.com/solutions-ata-for-splunk>; *Critical Start Managed SIEM Services for Splunk*, CRITICAL START DOCUMENTATION (2020); *Splunk Data Stream Processor - Use the Data Stream Processor 1.2.0*, SPLUNK DOCUMENTATION (2021); *Splunk Data Stream Processor - Function Reference 1.2.0*, SPLUNK DOCUMENTATION (2021); Ram Sriharsha and Harsha Wasalathanthri, *Unbounded Learning On Streams*, SPLUNK .CONF2019 PRESENTATION (2019); Ed Sale and Bill Muller, *Splunk DSP: Rapid, Automated, Repeatable Data Ingest – DSP + Automation = Rapid Deployment*, SPLUNK .CONF2020 PRESENTATION (2020); Poornima Devaraj and Jove Zhong, *Collect Service: Introducing A New Ingest Model*, SPLUNK .CONF2019 PRESENTATION (2019); *Splunk Data Stream Processor Deep Dive + Demonstration*, SPLUNK YOUTUBE CHANNEL (October 17, 2019), available at: <https://www.youtube.com/watch?v=WNN8EOVoBXs>; *Splunk Data Stream Processor - Install and administer the Data Stream Processor 1.2.0*, SPLUNK DOCUMENTATION (2021); Dirk Nitschke and Bashar Abdul-Jawad, *Using Splunk Stream Processor As A Data Transformation, Alerting And Action Engine*, SPLUNK .CONF2019 PRESENTATION (2019); Blaine Wastell and Thor Taylor, *FN20602: Data Stream Processor: How To Get The Most Out Of Your Data!*, SPLUNK .CONF2019 PRESENTATION (2019); Jamie Grier, *Splunk Data Stream Processor*, FLINK FORWARD YOUTUBE CHANNEL (October 28, 2020), available at: <https://www.youtube.com/watch?v=0pJQWwy33pE>; Thor Taylor and Poornima Devaraj, *PLA1735A: Getting to Know Splunk’s Data Streaming Technology*, SPLUNK .CONF2020 PRESENTATION (2020); Thor Taylor and Adam Lamar, *FN1987: Using Splunk Data Stream Processor As A Streaming Engine For Apache Kafka*, SPLUNK .CONF2019 PRESENTATION (2019); and *Splunk Data Stream Processor: Connect to Data Sources and Destinations with DSP 1.2.0*, SPLUNK DOCUMENTATION (2021).

companies and academic institutions. Splunk and Critical Start are utilizing the technology claimed in the '593 patent without paying a reasonable royalty. Splunk and Critical Start are infringing the '593 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

125. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '593 patent.

126. As a result of Splunk and Critical Start's infringement of the '593 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Splunk and Critical Start's infringement, but in no event less than a reasonable royalty for the use made of the invention by Splunk and Critical Start together with interest and costs as fixed by the Court.

**COUNT IV**  
**INFRINGEMENT OF U.S. PATENT NO. 8,817,790**

127. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

128. Splunk designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for handling a flow of information packets.

129. Splunk designs, makes, sells, offers to sell, imports, and/or uses Splunk Cloud and Splunk Enterprise deployments configured with Splunk Stream Versions 7.1 and later (collectively, the "Splunk '790 Products(s)").

130. One or more Splunk subsidiaries and/or affiliates use the Splunk '790 Products in regular business operations.

131. One or more of the Splunk '790 Products include technology for handling a flow of information packets. Specifically, the Splunk '790 Product process information packets that have the same header information.

132. The Splunk '790 Products are available to businesses and individuals throughout the United States.

133. The Splunk '790 Products are provided to businesses and individuals located in the Eastern District of Texas.

134. Splunk has directly infringed and continues to directly infringe the '790 patent by, among other things, making, using, offering for sale, and/or selling technology for handling a flow of information packets, including but not limited to the Splunk '790 Products.

135. The Splunk '790 Products process a flow comprised of two or more information packets having header information in common. Further, the Splunk '790 Products use header-independent statistics for traffic classification. These statistics include bit rate, packet counts, and byte counts that are used to identify a particular traffic type.

136. The Splunk '790 Products store header-independent statistics about the flow in a flow block associated with the flow.

137. The Splunk '790 Products perform traffic matching using header-independent statistics such as: total number of input packets, total number of output packets, input bit rates, and output bit rates.

138. The Splunk '790 Products update the header-independent statistics in the flow block as each information packet belonging to the flow is processed. The header-independent statistics are stored in a flow block associated with the flow.



139. The Splunk '790 Products categorize the flow as one or more traffic types by determining whether the header-independent statistics match one or more profiles corresponding to a traffic type.

140. The Splunk '790 Products perform an operation that is determined according to the one or more traffic types on one or more information packets belonging to the flow if the one or more traffic types match one or more particular traffic types designated by a user.

141. By making, using, testing, offering for sale, and/or selling products and services, including but not limited to the Splunk '790 Products, Splunk has injured Plaintiffs and is liable for directly infringing one or more claims of the '790 patent, including at least claim 1, pursuant to 35 U.S.C. § 271(a).

142. Splunk also indirectly infringes the '790 patent by actively inducing infringement under 35 USC § 271(b).

143. Splunk has had knowledge of the '790 patent since at least service of this Complaint or shortly thereafter, and Splunk knew of the '790 patent and knew of its infringement, including by way of this lawsuit.

144. Splunk intended to induce patent infringement by third-party customers and users of the Splunk '790 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Splunk specifically intended and was aware that the normal and customary use of the accused products would infringe the '790 patent. Splunk performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '790 patent and with the knowledge that the induced acts would constitute infringement. For example, Splunk provides the Splunk '790 Products that have the capability of operating in a manner that infringe one or more of the

claims of the ‘790 patent, including at least claim 1, and Splunk further provides documentation and training materials that cause customers and end users of the Splunk ‘790 Products to utilize the products in a manner that directly infringe one or more claims of the ‘790 patent.<sup>25</sup> By providing instruction and training to customers and end-users on how to use the Splunk ‘790 Products in a manner that directly infringes one or more claims of the ‘790 patent, including at least claim 1, Splunk specifically intended to induce infringement of the ‘790 patent. Splunk engaged in such inducement to promote the sales of the Splunk ‘790 Products, e.g., through Splunk user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘790 patent. Accordingly, Splunk has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘790 patent, knowing that such use constitutes infringement of the ‘790 patent.

145. The ‘790 patent is well-known within the industry as demonstrated by multiple citations to the ‘790 patent in published patents and patent applications assigned to technology

---

<sup>25</sup>See, e.g., *Splunk Stream Release Notes 7.3.0*, SPLUNK DOCUMENTATION (2021); *Splunk Stream Installation and Configuration Manual 7.3.0*, SPLUNK DOCUMENTATION (2021); *Splunk Stream User Manual 7.3.0*, SPLUNK DOCUMENTATION (2021); David Cavuto, *Service And Asset Discovery With Wire Data*, SPLUNK .CONF2019 PRESENTATION (2019); *Splunk Stream - Gain Real-Time Insights Into Application Performance And Customer Experience*, SPLUNK PRODUCT BRIEF (2017); *Splunk App For Stream – Enhance Operational Intelligence With Wire Data Capture*, SPLUNK FACT SHEET (2015); Simon O’Brien and Vinu Alazath, *FN1206: The Path To Operational Enlightenment – An Introduction To Wire Data*, SPLUNK .CONF2019 PRESENTATION (2019); David Cavuto, *Ending the Finger-Pointing Between Apps And Network Admins Using Splunk Stream For Fault Isolation*, SPLUNK .CONF2017 PRESENTATION (2017); John Stoner, *Detecting Vulnerable and Compromised Certificate Use/Abuse with Splunk Enterprise Security and Stream*, SPLUNK BLOG (November 25, 2015), available at: [https://www.splunk.com/en\\_us/blog/tips-and-tricks/detecting-certificate-abuse-with-splunk-enterprise-security-and-stream.html](https://www.splunk.com/en_us/blog/tips-and-tricks/detecting-certificate-abuse-with-splunk-enterprise-security-and-stream.html); David Cavuto, *The Truthiness of Wire Data: Using Splunk Stream For Performance Monitoring*, SPLUNK .CONF2016 PRESENTATION (2016); Mike Dickey and Clayton Ching, *What’s New: Splunk App For Stream*, SPLUNK .CONF2014 PRESENTATION (2014); Ryan Kovar, *Hunting With Splunk: The Basics*, SPLUNK BLOG (July 6, 2017), available at: [https://www.splunk.com/en\\_us/blog/security/hunting-with-splunk-the-basics.html](https://www.splunk.com/en_us/blog/security/hunting-with-splunk-the-basics.html); John Stoner, *Finding Islands In The Stream (Of Data)...*, SPLUNK BLOG (July 17, 2017), available at: [https://www.splunk.com/en\\_us/blog/security/finding-islands-in-the-stream-of-data.html](https://www.splunk.com/en_us/blog/security/finding-islands-in-the-stream-of-data.html).

companies and academic institutions. Splunk is utilizing the technology claimed in the '790 patent without paying a reasonable royalty. Splunk is infringing the '790 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

146. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '790 patent.

147. As a result of Splunk's infringement of the '790 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Splunk's infringement, but in no event less than a reasonable royalty for the use made of the invention by Splunk together with interest and costs as fixed by the Court.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs Sable IP, LLC and Sable Networks, Inc. respectfully request that this Court enter:

- A. A judgment in favor of Plaintiffs that Splunk has infringed, either literally and/or under the doctrine of equivalents, the '358, '593, and '790 patents;
- B. A judgment in favor of Plaintiffs that Splunk and Critical Start have jointly infringed, either literally and/or under the doctrine of equivalents, the '593 patent;
- C. An award of damages resulting from Splunk's acts of infringement in accordance with 35 U.S.C. § 284;
- D. An award of damages resulting from Splunk and Critical Start's acts of joint infringement in accordance with 35 U.S.C. § 284;

- E. A judgment and order finding that Splunk and Critical Start's infringement was willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate within the meaning of 35 U.S.C. § 284 and awarding to Plaintiffs enhanced damages.
- F. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiffs their reasonable attorneys' fees against Splunk and Critical Start.
- G. Any and all other relief to which Plaintiffs may show themselves to be entitled.

**JURY TRIAL DEMANDED**

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiffs Sable IP, LLC and Sable Networks, Inc. request a trial by jury of any issues so triable by right.

Dated: June 24, 2021

Respectfully submitted,

/s/ Daniel P. Hipskind

Dorian S. Berger (CA SB No. 264424)  
Daniel P. Hipskind (CA SB No. 266763)  
BERGER & HIPSKIND LLP  
9538 Brighton Way, Ste. 320  
Beverly Hills, CA 90210  
Telephone: 323-886-3430  
Facsimile: 323-978-5508  
E-mail: dsb@bergerhipskind.com  
E-mail: dph@bergerhipskind.com

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

*Attorneys for Sable Networks, Inc. and  
Sable IP, LLC*