IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SPLUNK INC., a Delaware Corporation, Plaintiff, v. CRIBL, INC., a Delaware Corporation, and CLINT SHARP, an individual, Defendants.	C.A. No. _____ JURY TRIAL DEMANDED

COMPLAINT

INTRODUCTION

This is an intellectual property case involving two competing software companies: Splunk, a pioneer and leader in the data analytics software industry, and Cribl, a business built on the back of Splunk's labor and intellectual property, without license and without regard for ethics, the rights of others, or the law.

Cribl was founded fourteen years after Splunk by a former Splunk employee, Clint Sharp. Mr. Sharp founded Cribl using code he intentionally and unlawfully took from Splunk when he was a Splunk employee without a license or permission to do so. Since that time, Cribl and Mr. Sharp have recruited numerous Splunk employees to Cribl, and have systematically encouraged employees to take Splunk's confidential technical and business documents with them. In turn, Cribl has used the information it misappropriated to compete unfairly against Splunk. At the same time, Cribl has developed and marketed its software by making unlicensed copies of Splunk's copyrighted software, and by willfully infringing the patents that the United States Patent and Trademark Office awarded to Splunk for its foundational innovations. Cribl has attempted to mislead the market into believing that Cribl is an innovator, when in fact Cribl's "innovation" is derivative of Splunk's intellectual property.

Splunk encourages fair competition, and it embraces the ability of third parties to build software on top of its software platform. Splunk recognizes that innovation by third parties working with Splunk's software makes the Splunk ecosystem better for everyone—for Splunk's customers, for Splunk itself, and for other Splunk partners. But Cribl's unlawful actions are not innovation, and they have no place on the Splunk platform or in our economy. Cribl's unethical actions, its willful disregard of intellectual property rights, and its coordinated campaign of misappropriation have left Splunk no choice but to file this lawsuit to stop Cribl's unlawful actions and to seek redress for the damage that Cribl has caused.

Plaintiff Splunk Inc. ("Splunk") files this Complaint against Defendants Cribl, Inc. ("Cribl") and Clint Sharp and alleges as follows:

1. Splunk develops and operates an industry-leading data platform for analyzing large volumes of machine data. Splunk was founded in 2003, pioneered the machine data analytics industry, and still leads it in both innovation and customer affinity to this day.

2. Cribl is a software company whose products leverage Splunk's data platform. It was founded in 2017 by three former Splunk employees. These employees built critical functionality into Cribl's first software product by improperly using Splunk source code intentionally misappropriated from Splunk. As set forth below, since this initial misuse, Cribl has taken an immense volume of additional confidential material from Splunk and used that material to compete unfairly against Splunk. Cribl has also developed its products with willful disregard for Splunk's patent rights and used Splunk software in a manner that willfully infringes Splunk's copyrights.

3. Cribl's first product was released in late 2018. At that time, Cribl did not reveal to Splunk that its product was based on misuse of misappropriated Splunk code. Instead, Cribl held itself out as a partner of Splunk. In fact, Cribl joined Splunk's official Technology Alliance Partner Program under this pretense, branding itself as the partner of a company it actually sought to undermine.

4. Not content with unlawfully taking and misusing Splunk's code, Cribl also took other confidential material from Splunk, including by soliciting important technical and business documents from departing Splunk employees, and then using those documents to further develop its software and interfere with Splunk's customer relationships. On information and belief, Cribl's

CEO and co-founder, Clint Sharp, actively participated in this effort, recruiting Splunk employees to join Cribl and encouraging them to bring Splunk confidential material with them.

5. Cribl's actions led to Splunk terminating Cribl's status as a Splunk partner. But Cribl has continued to misuse Splunk's proprietary information and has operated with wanton disregard of Splunk's patents and copyrights. For example, on information and belief, Cribl has used Splunk's copyrighted software in conjunction with its software development work and marketing, despite having no license to do so. And the software that Cribl has developed infringes numerous Splunk patents, despite, on information and belief, Cribl's awareness of the patents and knowledge of its infringement or willful blindness thereof.

6. Cribl's course of conduct has left Splunk no choice but to file this lawsuit.

7. Splunk supports a robust innovation ecosystem around its products because it believes that fair competition and collaboration on Splunk's platform will benefit Splunk's customers. Accordingly, Splunk encourages third parties—and especially its partners—to develop software that extends the features and functionality of Splunk's data platform, pursuant to its partner programs and while respecting Splunk's proprietary rights. But Cribl's actions are neither innovative nor fair.

8. Cribl built its business on a foundation of misappropriated and misused Splunk code and documents, willful infringement of intellectual property, and a disregard of contractual and ethical obligations and principles of fair competition. While Cribl now markets itself as an "innovator," and describes Splunk to its employees and customers as "stale," the reality could not be further from Cribl's characterizations. Splunk's innovations are reflected in the well over 1,000 patents it has been awarded by the United States Patent and Trademark Office, while Cribl's

"innovation" is reflected in the number of patents it possesses: zero. Since Cribl is unwilling to compete fairly in the market, it must account for its actions in court.

THE PARTIES

9. Plaintiff Splunk is a Delaware corporation with its principal place of business at 270 Brannan Street, San Francisco, CA 94107.

10. Defendant Cribl is a Delaware corporation with its principal place of business at 44 Tehama Street, Suite 201, San Francisco, CA 94105.

11. Defendant Clint Sharp is the CEO and co-founder of Cribl. On information and belief, Mr. Sharp resides in Oakland, CA.

JURISDICTION AND VENUE

12. This Court has original jurisdiction to adjudicate Splunk's Patent Act, Copyright Act, and Digital Millennium Copyright Act claims pursuant to 17 U.S.C. § 101 *et seq.*, 28 U.S.C. § 1331, and 28 U.S.C. § 1338(a). This Court has supplemental jurisdiction over the other claims asserted herein pursuant to 28 U.S.C. § 1367 because they are so related to the claims in this action for which the Court has original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution.

13. This Court has personal jurisdiction over Cribl because it is a Delaware corporation. In addition, this Court has personal jurisdiction over Mr. Sharp under the "necessary or proper party" provision of 10 Del. C. § 1334 because Mr. Sharp is an officer of Cribl, a Delaware corporation that is a party to this suit. As an officer of a Delaware corporation, Mr. Sharp has availed himself of the rights and benefits of the laws in this State. On information and belief, Mr. Sharp is a proper party because he has legal interests separate from Cribl, and Mr. Sharp was acting in his official capacity as an officer of Cribl when, among other things, he infringed Splunk's

copyrights, encouraged and induced infringement by Cribl and others of Splunk's copyrights, and when he violated the Digital Millennium Copyright Act.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b), (c) and (d), as well as 28 U.S.C. § 1400(a) and (b) because Cribl does business in and resides in this District and Mr. Sharp may be found in this District, as described above.

GENERAL ALLEGATIONS

Splunk's Technology

15. Splunk was founded in 2003. Since then, it has pioneered software that captures, indexes, and analyzes large volumes of machine data in real time, allowing users to make use of that data in profound ways. Splunk's software has applications in diverse fields ranging from information security to manufacturing to business analytics.

16. Machine data is data generated by machines and software running on those machines. Modern businesses generate this data constantly in tremendous volumes—software, servers, sensors, mobile devices, factory equipment, and essentially any other digital device are all potential sources of machine data. On its own, this data is not particularly useful—it exists in an overwhelming number of formats, it is not cross-correlated, and it is so voluminous that humans themselves have no way of gaining insights from or reacting to the data in a meaningful fashion. Prior attempts to try to manage such a large volume of varied data were inelegant and inefficient, and could not handle problems unique to "big data" and large computer networks, such as real-time changes, varied inputs, and analyzing data without structure.[1] Splunk's disruptive vision in

[1] Big data has been defined as "an accumulation of data that is too large and complex for processing by traditional database management tools." "Big Data," Merriam-Webster's Collegiate Dictionary (11th ed. 2020). The "big data" problems that Splunk solves include those that are unique to complex and massive computer networks.

2003 was to bring this diverse data into a single system, index it, and provide a platform and interface for this data to be searched, analyzed, and acted upon at scale.

17. Splunk's flagship product is named Splunk Enterprise, and can be run locally by Splunk's customers, or hosted in the cloud by Splunk for its customers (via the Splunk Cloud Platform). Splunk Enterprise ingests real-time flows of machine data from disparate sources across a distributed environment and indexes that data, regardless of its source or format. Customers can then interact with their data through an interface from which they can generate graphs, reports, alerts, dashboards, and visualizations. Customers can thus use Splunk Enterprise to monitor and react to their data in real time.

18. Splunk's software has significantly impacted the way companies across the world use data. Today, Splunk has thousands of customers, including many of the world's largest and most complex organizations in both the private and public sectors. Splunk not only pioneered the industry in which it now operates, but it continues to lead that industry.

19. Indeed, in 2021, Fortune Magazine selected Splunk as one of the 2021 World's Most Admired Companies for its highly regarded corporate reputation and continued growth as a software leader. Market reports from Gartner, Omdia Universe, Research in Action, Constellation Research, and others consistently recognize Splunk as a market leader based on the technological capabilities of its software, and for achieving high levels of customer satisfaction.

20. Many of Splunk's innovations are reflected in the well over 1,000 patents issued to it by the United States Patent and Trademark Office, and in Splunk's nearly 100 U.S. Copyright Registrations. Splunk's patents cover diverse technological innovations related to many aspects of software in this industry, from parsing rules to data visualization to remote data capture to

working with dual-queue systems. Several such technologies are at issue in this case, and related patents are addressed later in this Complaint.

21. Splunk has continuously developed and enhanced its software products for nearly two decades, as reflected in the many versions of its software it has released over the years. These software versions are protected by valid and duly issued U.S. Copyright Registrations. *See, e.g.*, Exhibit A. For example, the copyright registrations below cover numerous versions of Splunk Enterprise and related technologies (hereinafter "Splunk Enterprise" is used to refer to any or all of the below-referenced versions of Splunk Enterprise, whether deployed on premises or on the Splunk Cloud Platform):

Registered Work:	**U.S. Copyright Registration:**
Exploring Splunk Search Processing Language (SPL) Primer and Cookbook.	TX 7-631-106
Indexer 1.0 /by Splunk, Inc.	TX 7-541-301
Indexer 2.0.1 /by Splunk, Inc.	TX 7-548-761
Indexer 2.1 /by Splunk, Inc.	TX 7-556-414
Indexer 2.2.	TX 7-567-237
Splunk Enterprise 1.0.	TX 7-659-994
Splunk Enterprise 2.0.1.	TX 7-659-825
Splunk Enterprise 2.1.	TX 7-659-905
Splunk Enterprise 2.2.	TX 7-710-860
Splunk Enterprise 3.0.	TX 7-660-059
Splunk Enterprise 3.1.	TX 7-660-042
Splunk Enterprise 3.2.	TX 7-660-046
Splunk Enterprise 3.3.	TX 7-660-053
Splunk Enterprise 3.4.	TX 7-660-065
Splunk Enterprise 4.0.	TX 7-659-847
Splunk Enterprise 4.1.	TX 7-660-037
Splunk Enterprise 4.2.	TX 7-659-918
Splunk Enterprise 4.3.	TX 7-659-917
Splunk Enterprise 5.0.	TX 7-659-915
Splunk Enterprise 6.0.	TX 7-801-578
Splunk Enterprise 6.1.	TX 7-918-705
Splunk Enterprise 6.2.	TX 7-994-799
Splunk Enterprise 6.3.	TX 8-216-021
Splunk Enterprise 6.4.	TX 8-284-845
Splunk Enterprise 6.5.	TX 8-350-486

Splunk Enterprise 6.6.	TX 8-410-385
Splunk Enterprise 7.0.	TX-8-545-897
Splunk Enterprise 7.1.	TX 8-747-518
Splunk Enterprise 7.2.	TX 8-747-523
Splunk Enterprise 7.3.	TX 8-749-975
Splunk Enterprise 8.0.0.	TX 8-823-041
Splunk Enterprise 8.1.0.	TX 9-154-003
Splunk Enterprise 8.2.0.	TX 9-154-008
Splunk Enterprise 9.0.0.	TX 9-154-016
Splunk Enterprise S2S Tool.	TXu 2-335-442

Splunk's Partner Program

22. Because different businesses have different types of data and use that data in different ways, Splunk built Splunk Enterprise to be a customizable software platform. In other words, Splunk Enterprise provides a flexible foundation upon which dashboards and software can be built for application- or use case-specific purposes, sometimes referred to as "solutions," "apps," or "add-ons."

23. For example, one company might be interested in monitoring the network traffic of all servers and computers on its computer network for cyber-security purposes. This company could use Splunk Enterprise to ingest network log data from all of its computers and servers, and customize Splunk Enterprise so that its data analysis, monitoring, and visualization features are catered to security issues—*e.g.*, graphing incoming and outgoing network traffic, and providing alerts for anomalous activities on the network. On the other hand, a different company may seek to use Splunk Enterprise to handle different data for different reasons—*e.g.*, a manufacturing company may use Splunk Enterprise to ingest data from factory equipment to understand mechanical performance and throughput in real time.

24. Splunk itself publishes solutions directed to various such purposes (*e.g.*, customizations of and extensions to Splunk Enterprise that cater to advanced network threat detection, digital customer experience, cloud monitoring, or manufacturing). Splunk also supports

and encourages third parties to develop on top of the Splunk platform in appropriate and lawful ways, extending the features and functionality of the Splunk platform in accordance with their own business needs or those of Splunk's customers.

25. Indeed, Splunk maintains a Technology Alliance Partner ("TAP") Program, pursuant to which partners are provided a license to various software development tools and interfaces (such as application programming interfaces, known as "APIs") and other materials and information in order to develop software that extends the features or functionality of Splunk Enterprise. TAP partners are also granted a limited license to run Splunk Enterprise software for related software development purposes.

26. To join the TAP Program, a third party must sign and execute a contract called the TAP Agreement. *See* Exhibit B.

27. The license to Splunk Enterprise provided to Splunk TAP partners under the TAP Agreement is limited. In relevant part, the license provides TAP partners with "a nonexclusive, non-transferable, worldwide, non sublicensable license during the Term to download (and make up to five (5) copies) and use the Splunk software" for only two uses: (1) to "test the Splunk Software for purposes of developing TAP Extensions"; and (2) to "demonstrate the use of TAP Extensions with the Splunk Software to actual, potential or prospective Users." *Id.*, Section 3.3. Any use of the Splunk Software that is not in accordance with the Agreement is expressly prohibited. *Id.*, Section 4(h).

28. In particular, the TAP Agreement expressly prohibits a host of other activities. For example, the TAP Agreement does not allow TAP partners to: "(a) copy any Splunk Software (except as required to run the Splunk Software and for reasonable backup purposes); (b) modify, adapt, or create derivative works of the Splunk Software; . . . (d) decompile, disassemble or reverse

engineer the Splunk Software, or determine or attempt to determine any source code, algorithms, methods or techniques embodied in the Splunk Software, except to the extent expressly permitted by applicable law notwithstanding a contractual prohibition to the contrary; . . . [or] (f) attempt to disable or circumvent any license key or other technological mechanisms or measures intended to prevent, limit or control use or copying of, or access to, any materials included in the Splunk Software." *Id.*, Section 4.

29. As addressed in greater detail below, Cribl was formerly a Splunk partner pursuant to a TAP Agreement. Prior to its termination, the TAP Agreement granted Cribl permission to use Splunk Enterprise to develop software that extends Splunk Enterprise's features or functionality.

30. Splunk invests substantial resources into maintaining its TAP program and supporting the work of its partners.

31. For example, Splunk provides software that permits its partners to feed data into, or retrieve data from, an instance of Splunk Enterprise. Using this software, a Splunk partner can develop software capable of sending data to, or retrieving data from, an instance of Splunk Enterprise. This software—known as the "HEC" protocol—reflects Splunk's commitment to its partners: HEC is provided by Splunk to allow Splunk partners to develop software that works with Splunk Enterprise and extends its features and functionality.

32. Although Splunk provides HEC for third parties to use, Splunk maintains other aspects of its software as proprietary. One example of such proprietary software is the "S2S" protocol. S2S stands for "Splunk-to-Splunk," and this is software that Splunk itself uses to send data to, or receive data from, Splunk Enterprise and other Splunk software and technologies. Splunk does not support use of S2S by third parties, does not publish S2S's source code, and does not document S2S in a manner that facilitates third-party use of this protocol.

Cribl Was Founded to Capitalize on Splunk's Technology and Success

33. Defendant Clint Sharp is a former Senior Director of Product Management at Splunk. As a senior Splunk employee, Mr. Sharp had access to a wide array of Splunk proprietary and confidential information, including Splunk's S2S protocol and code, and played a significant role in Splunk's technical organization. Before resigning from Splunk, in early 2017, unbeknownst to Splunk and without authorization, Mr. Sharp posted a derivation of Splunk's proprietary and confidential S2S source code to his personal github webpage (a publicly accessible website for sharing source code). Mr. Sharp named this derived code "go-S2S."

34. Mr. Sharp created go-S2S by copying Splunk's S2S protocol source code without authorization to do so and creating a derivation of that code. At the time, Mr. Sharp had access to this proprietary code only by virtue of his work for Splunk, but he did not have authorization to post Splunk's code on the Internet or to create new software derived from it.

35. Splunk's S2S protocol source code is covered by Splunk's valid and duly issued U.S. Copyright Registrations for Splunk Enterprise identified in Paragraph 21, above, including, for example, U.S. Copyright Registration TXu 2-335-442.

36. On information and belief, Mr. Sharp derived go-S2S from Splunk's copyrighted source code with the intention of using it for his own personal financial gain at a different company. On information and belief, Mr. Sharp derived go-S2S from at least the code protected by the above-referenced U.S. Copyright Registrations.

37. The Splunk S2S code that Mr. Sharp copied contained Splunk copyright headers indicating authorship and ownership information, reflecting Splunk's copyright in and ownership of this code, but Mr. Sharp removed this information from the derived files that he posted on his personal github page.

38. On March 24, 2017, a few months after his initial copying of Splunk's source code, Mr. Sharp resigned from Splunk to co-found Cribl with Dritan Bitincka and Ledion Bitincka—both former software architects at Splunk. On information and belief, Mr. Sharp's plan was to build a business using the code he had taken from Splunk. For example, Mr. Sharp and Cribl sought to capitalize on their access to the S2S protocol, which until Mr. Sharp's misappropriation, had been in Splunk's exclusive control.

39. Cribl was incorporated in May 2017 and released its first software product, "LogStream," now known as "Stream," in October 2018. (Hereinafter, both "LogStream" and "Stream" are referred to as "Stream.")

40. On information and belief, go-S2S, and/or other source code copied or derived from Splunk's Splunk Enterprise source code, is currently used within Stream and has been used within Stream since its release. On information and belief, Clint Sharp provided this code to Cribl for its use within Stream, and, to this day, has encouraged and induced Cribl's use of this code. On information and belief, Mr. Sharp has done so with knowledge that go-S2S was an unlicensed derivative of Splunk's copyrighted S2S code.

41. On information and belief, each new version of Cribl's Stream software includes a new copy of this unlicensed derivative of Splunk's copyrighted S2S code.

42. In or around December 2018, Mr. Sharp added an open-source MIT license to the go-S2S source code on his personal github webpage, falsely identifying himself as the author and/or owner of the copyright in the go-S2S code, and falsely providing open-source terms for use of the go-S2S code, despite its derivation from Splunk's proprietary source code. In fact, Mr. Sharp was not the author or owner of the copyright in go-S2S, nor did he have any authority to

license the go-S2S code, which was an unlawful and unlicensed derivation of Splunk's source code.

43. On information and belief, Mr. Sharp added this false license to the go-S2S code to obscure his own unlawful copying of Splunk's copyrighted source code.

44. Mr. Sharp maintained the go-S2S code online until at least December 2021, thereby distributing a derivation of Splunk's copyrighted source code to the public and providing the public with false information regarding the copyright authorship and ownership of this code.

45. Cribl's Stream software is and has been marketed primarily to Splunk customers. Indeed, Cribl relies heavily on its Splunk experience in its advertisements and boasts about its ability to "speak… S2S." *See* Exhibit C (excerpts of https://cribl.io/blog/3-ways-logstream-can-improve-your-data-agility/).

46. A primary function of Stream is to filter the data that Splunk customers send to a Splunk Enterprise instance. In essence, Cribl's Stream sits between a Splunk customer's sources of machine data and that customer's Splunk Enterprise instance. Instead of flowing directly from data sources into Splunk Enterprise, data flows into Stream. Stream can then filter this data before it is passed along to Splunk Enterprise, with a goal of reducing the total volume of data a customer adds to its Splunk Enterprise instance.

47. On information and belief, Cribl has used its illicitly obtained support for the S2S protocol as a means to convince Splunk's customers to buy software and services from Cribl. On information and belief, Cribl's ability to get a foothold in the market depended upon its ability to make available and support the S2S protocol, which it implemented using Splunk's proprietary source code without authorization.

48. For example, by building S2S support into Cribl's software using misappropriated Splunk source code, rather than using the authorized HEC functionality that Splunk makes available to its partners, Cribl facilitated its sales efforts to Splunk's customers. Splunk had invested significant resources in creating and facilitating the creation of customer environments in which Splunk's customers used the S2S protocol to transmit data to Splunk. Some of these environments contained a very large number of data source endpoints configured to transmit data to Splunk Enterprise via S2S. On information and belief, Cribl targeted and continues to target Splunk customers with S2S environments on the basis of its illicitly obtained S2S support.

49. For example, on information and belief, Cribl advertised to Splunk customers that it was able to greatly simplify the process of deploying its Stream software to Splunk customers who were already configured to transmit data to Splunk via S2S. According to Cribl, its support for S2S meant that Splunk customers seeking to use Cribl's software would not need to spend time or money reconfiguring their customer environment to support a non-S2S protocol (such as HEC). Indeed, Cribl advertises to this day that it can "receive data from whatever you [a Splunk customer] already have in place," including the "S2S protocol." Exhibit C (https://cribl.io/blog/3-ways-logstream-can-improve-your-data-agility/).

Cribl's Continued Misappropriation and Unlawful Acts

50. Splunk was initially unaware that Mr. Sharp misappropriated the S2S source code in 2017, and permitted Cribl to join Splunk's TAP Program in 2018.

51. While it was a member of the TAP Program, Cribl held itself out to Splunk as a "partner," while surreptitiously misappropriating critical information from Splunk and seeking to undermine its reputation among employees and customers.

52. Indeed, given that Cribl's software and customer base is predicated upon Splunk's software and customer base, Cribl has embarked upon a years-long campaign of misappropriation

and other unfair and unlawful conduct to continue developing and improving its own platform using technology and information that it improperly took from Splunk.

53. As of today, over 80 ex-Splunk employees have joined Cribl, and make up, on information and belief, over a quarter of Cribl's entire workforce.

54. On information and belief, Cribl—and Mr. Sharp in particular—has recruited Splunk employees to quit Splunk and join Cribl, and specifically requested that they take confidential Splunk materials with them and provide them to Cribl. Unfortunately, as set forth below, numerous ex-Splunk employees have acceded to such requests and have, in fact, provided Splunk's confidential materials to Cribl.

55. These confidential materials include valuable technical documents—such as specifications describing confidential implementation details regarding Splunk's software and newer versions of the S2S protocol. On information and belief, these misappropriated documents have been circulated among Cribl's employees who work on developing Cribl's products. On information and belief, Cribl has used the confidential technical documents that it illicitly obtained from Splunk to develop Cribl's own software and implement proprietary Splunk technology that is found in Splunk's products.

56. The confidential materials also include valuable business materials—such as product roadmaps and proprietary data concerning Splunk's customers and known prospects, including analysis and compilations of data revealing the needs of these customers and known prospects, as well as Splunk's confidential business plans and strategies to meet those needs.

57. On information and belief, Cribl has used these misappropriated materials to target Splunk's most important accounts (and known prospects), assessing which accounts could most likely be converted to Cribl customers, and using Splunk's proprietary analysis of and information

regarding those customers for competitive advantage against Splunk. Cribl's actions have damaged Splunk in the form of, at least, lost accounts, decreased revenue from existing accounts, and damaged relationships with customers.

58. Cribl's misappropriation and misuse of Splunk proprietary information has been extensive. For example, on information and belief, in May 2021, shortly before quitting Splunk to join Cribl, Marlo Haring Barnum (a former Splunk regional sales manager) e-mailed a Splunk confidential "Top 25" customer list document to her future Cribl email address. This list included proprietary information relating to active product deployments, contract terms, and prospective business opportunities. On information and belief, other confidential and proprietary Splunk documents accessed and taken to Cribl by this former Splunk employee include additional regional customer lists, account plan templates, and pricing and commission calculators. On information and belief, these materials have been accessed by Cribl and used in Cribl's business to compete with Splunk and market Cribl's software and services to Splunk's customers and to convert Splunk customers to Cribl customers.

59. As another example, on information and belief, in June 2021, Justin Hamblin (a former Splunk sales engineer) made copies of confidential Splunk technical documents approximately two weeks before quitting Splunk to join Cribl. These documents included, on information and belief, a confidential S2S protocol specification, providing a roadmap for implementation of a new version of Splunk's S2S protocol. On information and belief, the sales engineer also copied confidential product planning materials that contained competitive intelligence specifically relating to Cribl and Splunk's future product offerings. On information and belief, these materials have been accessed by Cribl and used in Cribl's business to compete

with Splunk, to develop Cribl's software, to market Cribl's software and services to Splunk's customers, and to convert Splunk customers to Cribl customers.

60. By way of further example, on information and belief, in September 2021, Cribl accessed and used in its business a large trove of confidential Splunk business analytics data that had been exfiltrated from Splunk by Hash Basu-Choudhuri (a former Splunk sales director). This business analytics data comprised proprietary information about thousands of Splunk's customers in the EMEA (Europe, Middle East, and Africa) region, a list of active product deployments for each customer, profitability calculations, satisfaction assessments, and future business plans. On information and belief, Cribl used this document to market its software and services to Splunk's customers and to convert Splunk customers to Cribl customers.

61. As yet another example, Shane Daniels (a former Splunk sales director) began interviewing with Cribl while still employed by Splunk in July 2021. On information and belief, shortly before leaving Splunk to join Cribl in September 2021, Mr. Daniels emailed confidential internal customer information to Cribl, related to a Splunk customer from which, on information and belief, Cribl sought to obtain business. On information and belief, Mr. Daniels also took confidential information related to the productivity and account responsibilities of Splunk's sales engineers and, on information and belief, Cribl used that information to poach Splunk sales engineers to become Cribl sales engineers.

62. The above are merely a handful of examples of Cribl's campaign to obtain confidential Splunk information and use it to compete unfairly against Splunk. On information and belief, this campaign was and is encouraged by—and participated in—by Cribl and Cribl's most senior executives. Indeed, on information and belief, Clint Sharp has personally participated in attempts to solicit confidential and proprietary Splunk information from Splunk employees.

Cribl's Termination from the TAP Program

63. Whereas Cribl at least pretended to be a "partner" to Splunk in the early stages of its membership in the TAP Program, Cribl's public conduct became increasingly adversarial over time.

64. For example, on information and belief Cribl's sales employees (and Mr. Sharp in particular) disparaged Splunk and its software in conversations and sales pitches to Splunk's actual and potential customers.

65. Cribl and Mr. Sharp also sought to disparage Splunk to Splunk's own employees, as part of Cribl's efforts to recruit Splunk's employees to join Cribl. Despite building its own product on top of Splunk's (using materials misappropriated from Splunk), and despite building its business by marketing to Splunk's customer base (again, using misappropriated materials), Cribl engaged in a marketing campaign that asserted Splunk was "stale" and Cribl was a company where Splunk's employees could "keep innovating." Indeed, Cribl went so far as to commission a billboard directly outside of Splunk's headquarters to advertise this false message directly to Splunk's employees.

66. On November 2, 2021, Splunk informed Cribl that Splunk had terminated Cribl's membership in the TAP Program, thereby terminating Cribl's TAP Agreement. *See* Exhibit D (Termination Letter). This termination correspondence was directly addressed to Clint Sharp (Cribl's founder and CEO), as well as to Cribl's Legal and Finance Vice Presidents. *Id.*

67. Thus, no later than November 2, 2021, Cribl had no license to run Splunk Enterprise in connection with Cribl's commercial development and marketing of commercial extensions to Splunk Enterprise's features or functionality.

68. Despite its termination from the TAP Program, however, on information and belief, Cribl has continued to make copies of Splunk Enterprise software (including by executing that

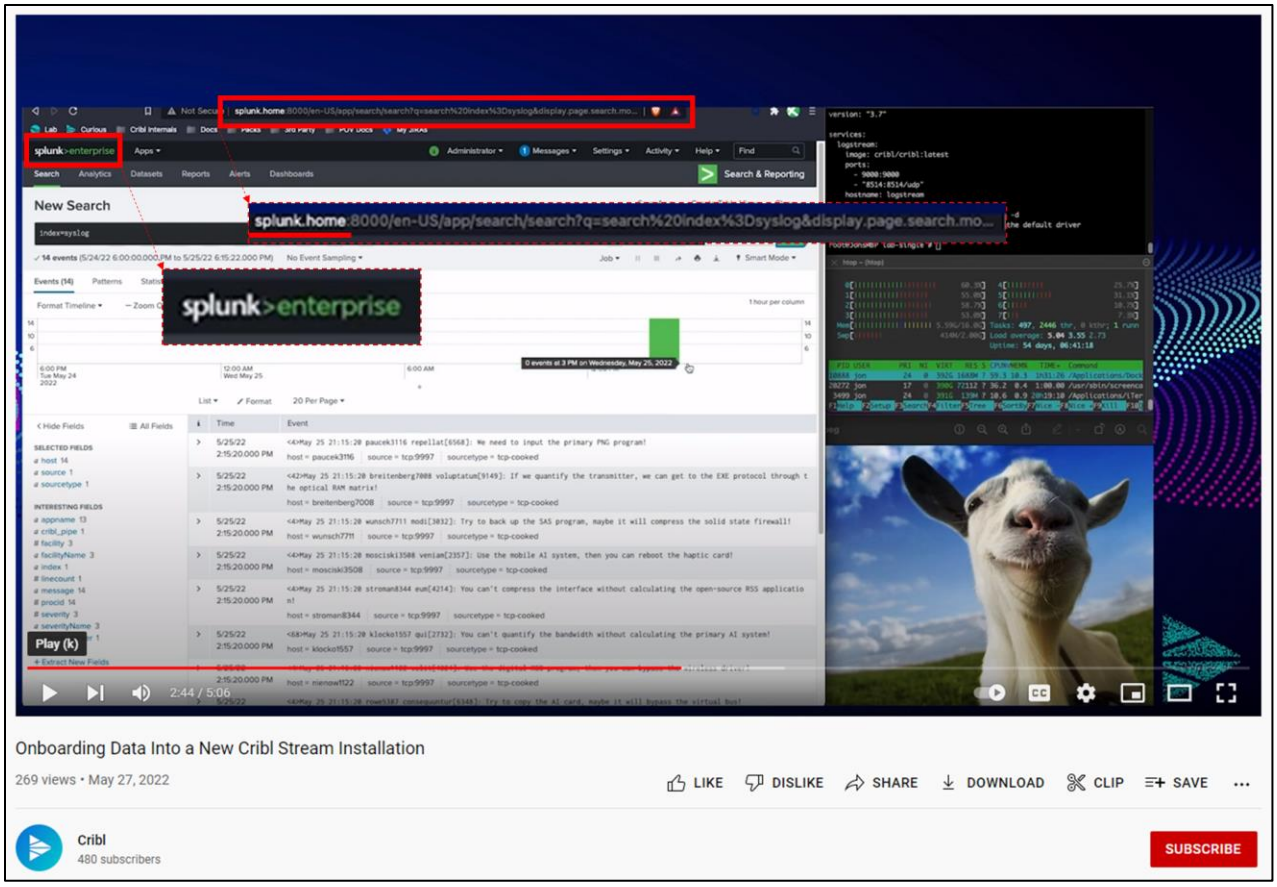
software), in connection with its marketing and development of software that depends upon and extends the features and functionality of Splunk Enterprise.

69. For example, in 2022, Cribl released an application called "Edge" that is used to manage data collection. *See* Exhibit E (excerpts of https://cribl.io/blog/announcing-cribl-edge-cribl-stream/).

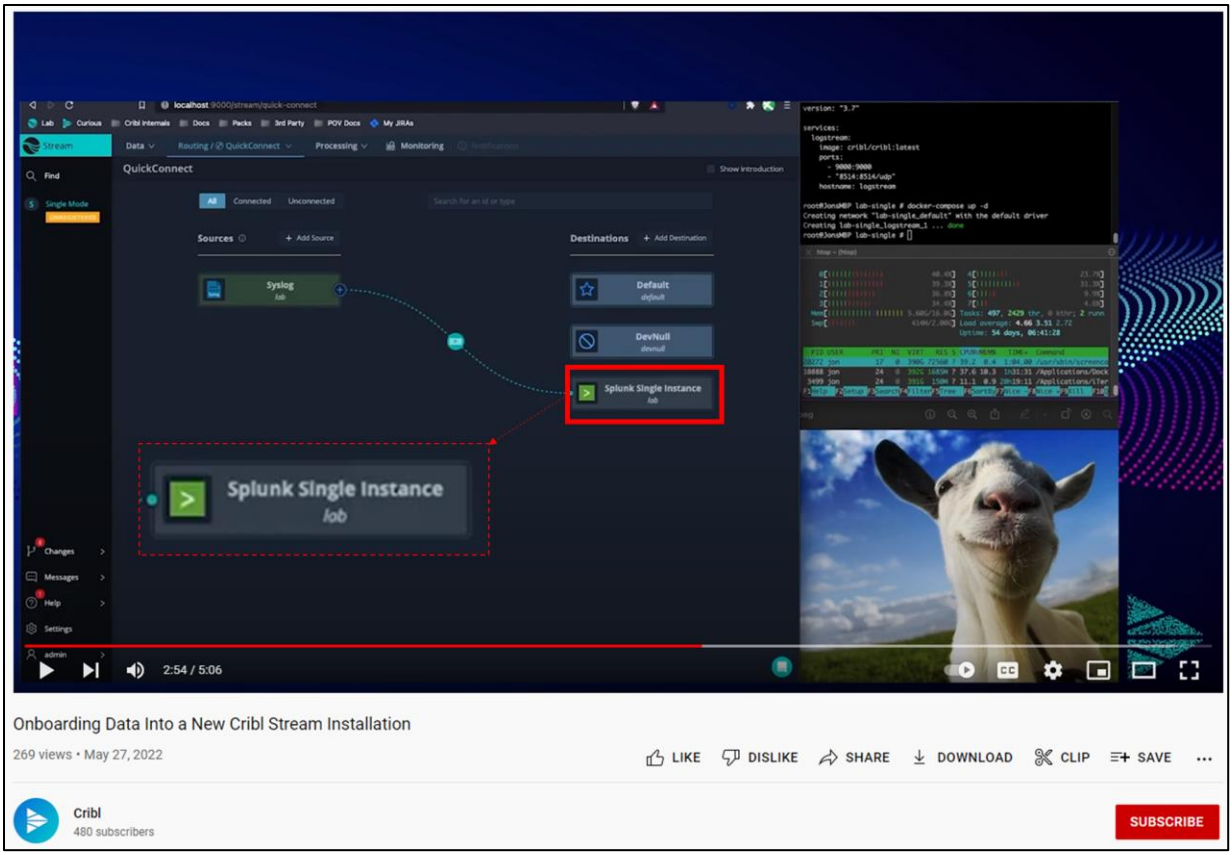
70. Many of Cribl Edge's features depend upon and make use of Splunk Enterprise. *See* Exhibit F (https://docs.cribl.io/edge/destinations-splunk/). On information and belief, in order to develop and support Edge (and in order to continue developing and supporting Stream), Cribl has executed and made copies of Splunk Enterprise software, despite having no license to do so, including as a result of its termination from Splunk's TAP Program.

71. Indeed, Cribl's own YouTube account includes videos reflecting Cribl's continued use of Splunk Enterprise software for commercial purposes, for which Cribl has no license. *See*, *e.g.*, https://www.youtube.com/watch?v=FY6UP4Fzc1s (video titled "Onboarding Data Into a New Cribl Stream Installation" and dated May 27, 2022).

72. For example, the above-cited "Onboarding Data Into a New Cribl Stream Installation" video shows a Senior Solutions Engineer at Cribl running an instance of Splunk Enterprise to advertise and demonstrate Cribl's software's features and functionality related to Splunk Enterprise:



Id. at 2:43 (annotations added in red).



Id. at 2:54 (annotations added in red).

73. Thus, despite its termination from the TAP Program and its lack of any requisite license, Cribl has continued to use and copy copyrighted Splunk Enterprise software.

74. On information and belief, Cribl's unlicensed use and copying of copyrighted Splunk Enterprise software continues to this day.

75. Additionally, on information and belief, prior to (and after) the termination of its TAP Agreement, Cribl also executed and copied Splunk Enterprise software to reverse engineer it, despite the contractual prohibition on doing so. For example, on information and belief, Cribl has attempted to reverse engineer Splunk Enterprise software for purposes of developing S2S-related functionality, including in connection with the misappropriated technical specification it

obtained that relates to newer versions of the S2S protocol than the one whose source code was unlawfully taken from Splunk by Clint Sharp.

76. Prior to the termination of the TAP Agreement, Cribl was aware that the S2S version corresponding to the code misappropriated by Clint Sharp would no longer be supported in future releases of Splunk Enterprise. Accordingly, on information and belief, Cribl attempted to build support for newer versions of S2S by using misappropriated confidential Splunk technical materials and by reverse engineering Splunk Enterprise.

Cribl's Circumvention of Technical Measures that Protect Access to Splunk Enterprise

77. In addition to its own unlicensed and unlawful use of Splunk Enterprise software, Cribl has taken various steps to thwart access controls that Splunk put in place to protect access to its customers' Splunk Enterprise instances.

78. For example, Splunk protects access to Splunk Enterprise instances by (1) refusing connections from client software that attempts to communicate via the S2S protocol and is unable to authenticate itself with a specific undocumented code phrase; and (2) restricting access to clients based on their possession of encrypted certificates that establish identity and authorization to access a Splunk Enterprise instance.

79. As to the first exemplary technical protection measure, Cribl's software authenticates itself using a code phrase copied from Splunk's confidential source code, thereby obtaining access to Splunk Enterprise by circumventing a technical protection measure.

80. As to the second exemplary technical protection measure, Splunk Enterprise supports the use of TLS (transport layer security) certificates to control access to instances of Splunk Enterprise. For customers with TLS certificates enabled, access to their Splunk Enterprise instance is restricted based upon possession of credentials encoded in a corresponding TLS certificate.

81. On information and belief, Cribl obtains credential information from Splunk TLS certificates and uses that information to access Splunk Enterprise instances without a license to do so to circumvent this technical protection measure. Cribl publishes detailed instructions to Splunk customers asking them to provide data Cribl uses for its circumvention, by extracting pertinent information from valid Splunk TLS certificates, which Cribl then uses to circumvent Splunk's certificate authentication:

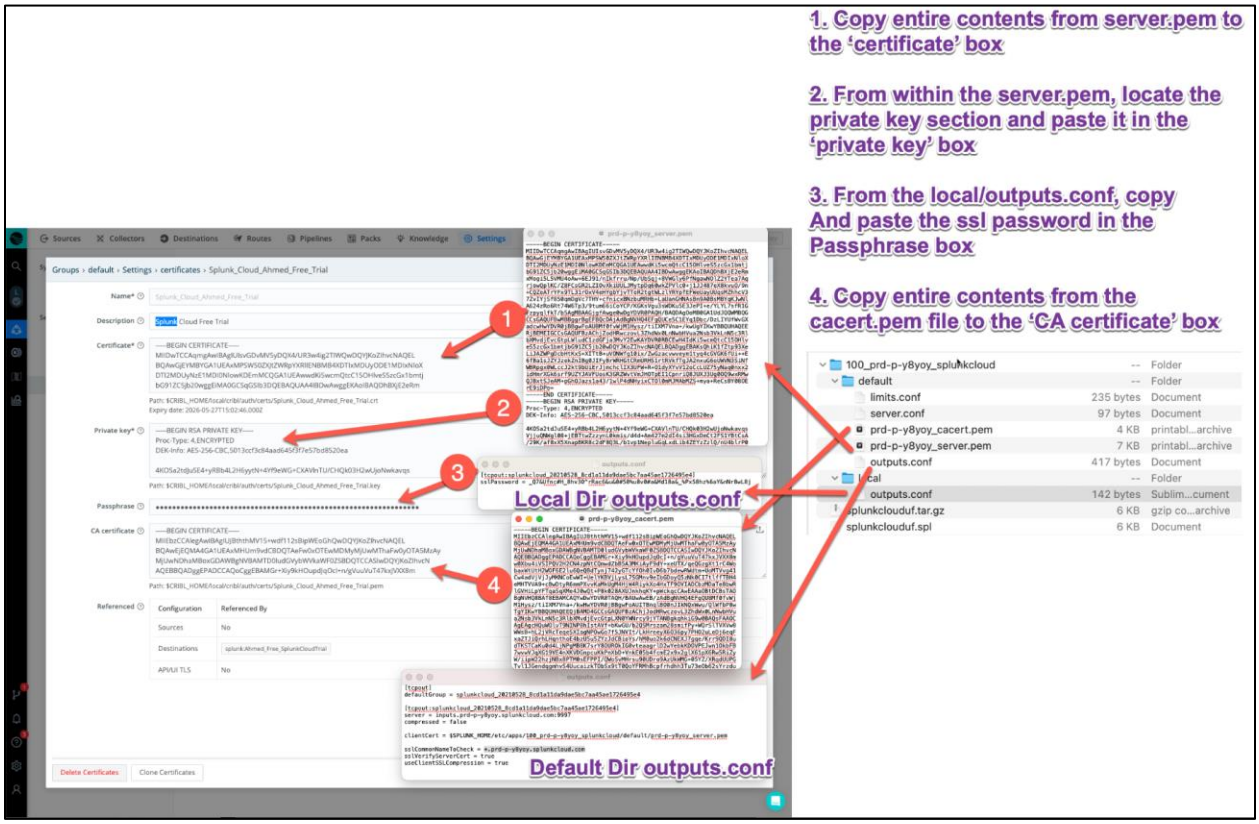


Exhibit G (https://docs.cribl.io/stream/usecase-splunk-cloud-integrations/).

82. Both Splunk's code phrase and its TLS certificates are technological measures that effectively control access to Splunk's copyrighted Splunk Enterprise software.

83. Cribl circumvents these measures to access Splunk Enterprise instances without authorization, as described above.

Splunk's Patent Portfolio

84. Splunk's ingenuity has been recognized not only by the software industry, but also by the United States Patent and Trademark Office, which has issued Splunk well over 1,000 patents for its inventions, many of which relate to Splunk Enterprise.

85. On information and belief, Cribl, its executives, and a large portion of its employees are aware of Splunk's patent portfolio, including the patents identified and addressed below.

86. For example, Mr. Sharp himself participated in Splunk's patent program, signing multiple declarations as an inventor on Splunk patent applications.

87. The same is true for the other two co-founders of Cribl, Dritan Bitincka and Ledion Bitincka (who now serves as Cribl's Chief Technical Officer), each of whom signed multiple declarations as inventors on Splunk patent applications.

88. At least 18 of Cribl's employees that Cribl hired from Splunk directly participated in Splunk's patent program as inventors.

89. And, on information and belief, all Cribl employees who formerly worked for Splunk are well aware of Splunk's extensive patent portfolio and the correspondence of the portfolio to Splunk's products and technologies, and have been since joining Cribl. During their terms of employment with Splunk, Splunk regularly discussed its portfolio with employees in meetings and internal correspondence. Indeed, Splunk publicizes its patent program regularly in internal meetings and externally at certain milestones.

90. Splunk's patent portfolio includes the patents introduced in Paragraphs 91-109, below, referred to herein as the "Patents-in-Suit."

91. U.S. Patent No. 9,762,443 ("the '443 Patent"), titled "Transformation of Network Data at Remote Capture Agents" duly and legally issued on September 12, 2017, from an application filed April 15, 2014. A true and correct copy of the '443 Patent is attached as Exhibit

H. Splunk is the owner and assignee of all right, title, and interest in and to the '443 Patent, including the right to assert all causes of action arising under said patent and to seek damages and all other remedies for the infringement thereof.

92. The '443 Patent is directed to "mechanisms for deploying and configuring network capture technology at distributed and/or remote locations." '443 Patent at 1:51-53. The patent explains that "the age of virtualization has triggered a sea change in the world of network data capture. Almost every network capture product available today is a physical hardware appliance that customers have to purchase and configure." *Id.* at 1:14-18. "However, customers are moving away from managing physical servers and data centers and toward public and private cloud computing environments that provide . . . resources as hosted services using . . . devices at remote locations. For these customers, it is either impossible, or at best extremely challenging, to deploy physical network capture devices and infrastructure in the cloud computing environments." *Id.* at 1:42-50.

93. This problem is even more acute in a networked big data environment, because as the amount of data collected by the system grows, the number of capture devices must grow along with it. And the capture devices must be deployed in farther-flung and varied locations—potentially across the globe—but must still be centrally configurable and able to process vast amounts of incoming machine and network data. Moreover, conventional network capture devices and techniques tend to be targeted to specific purposes and/or "fixed" in their implementation, such that they "preclude modification… to address different and changing business needs." *Id.* at 1:26-29. Conventional approaches can also be "cumbersome" in their data processing, which may require "Extraction, Transform, and Load ('ETL') processes… to filter, transform, and/or

aggregate data from the network traffic and enable the extraction of business value from the data." *Id.* at 1:30-41.

94. The '443 Patent addresses such problems through implementations and techniques associated with "remote capture agents" that can be deployed in distributed computing environments (such as cloud computing environments) for data capture and processing, and are configurable over a network by a configuration server in a centralized manner. The '443 Patent's remote capture agents and related techniques provide "mechanisms for streamlining the deployment and configuration of network capture technology at distributed and/or remote locations," *id.* at 2:21-23, which improve the ability to capture and process data on a distributed network, including by addressing physical challenges with conventional network capture, the inflexibility of conventional approaches, and the "cumbersome" nature of conventional processing techniques.

95. U.S. Patent No. 10,805,438 ("the '438 Patent"), entitled "Configuring the Protocol-Based Generation of Event Streams by Remote Capture Agents" duly and legally issued on October 13, 2020, from an application filed on July 1, 2019. A true and correct copy of the '438 Patent is attached as Exhibit I. Splunk is the owner and assignee of all right, title, and interest in and to the '438 Patent, including the right to assert all causes of action arising under said patent and to seek damages and all other remedies for the infringement thereof.

96. The '438 Patent also relates to remote capture agents and related configuration thereof, and concerns systems and "techniques for performing protocol-based capture of network data using remote capture agents in a distributed network environment." '438 Patent at 1:43-45. The '438 Patent notes various challenges associated with conventional network capture technology, including the difficulties associated with managing and configuring network capture

agents in a distributed network environment. These challenges include those discussed above in the context of the '443 Patent, including the difficulty in managing and configuring data capture in remote (including cloud) environments, and problems posed by conventional network capture products that are often catered for particular purposes and "are built from scratch" accordingly, and thus "may preclude modification to address different and changing business needs." *Id.* at 1:49:64. These problems are exacerbated by the volume of data and the requisite complexity of data capture in a big data environment, including the challenges associated with managing and configuring capture agents in distributed network environments with physical or virtual machines, including cloud computing environments.

97. The '438 Patent addresses such problems through implementations and techniques associated with "remote capture agents" and specific "mechanisms for streamlining the deployment and configuration of network capture technology at distributed and/or remote locations," including with relation to a configuration server and methods of using a configuration server to manage the configurations of remote capture agents. *Id.* at 2:20-23. The '438 Patent invention facilitates the configuration and control of remote capture agents by configuration servers, such that they can be dynamically adapted and deployed in a range of remote locations and efficiently provide data filtering, transformation, and aggregation functionality without drawbacks suffered by conventional approaches.

98. U.S. Patent No. 9,208,206 ("the '206 Patent"), entitled "Selecting Parsing Rules Based on Data Analysis" duly and legally issued on December 8, 2015, from an application filed July 28, 2014. A true and correct copy of the '206 Patent is attached as Exhibit J. Splunk is the owner and assignee of all right, title, and interest in and to the '206 Patent, including the right to

assert all causes of action arising under said patent and to seek damages and all other remedies for the infringement thereof.

99. The '206 Patent relates to improvements to computer systems that operate on event-based and time-based data (*e.g.*, computer systems that search, process, index, and transform machine data). The '206 patent explains that "[t]he rapid increase in the production and collection of machine-generated data has created large data sets that are difficult to search" using conventional computer searching techniques. *Id.* at 1:26-28. Put differently, the '206 patent recognized that complexities with "big data" data sets arising in large, networked environments were not suitably addressed by conventional computer search techniques, which were ill-equipped to effectively process and search this data effectively (*e.g.*, accurately or in a reasonable amount of time). This challenge owed in part to the requirement that machine data must be processed and indexed (thereby creating index data corresponding to the raw data) in order to be searchable and to be effectively usable for other data processing and visualization, and that indexing itself suffers from technical challenges. For example: "search engines may receive raw data from various data sources, including machine data. In some cases, search engines may be configured to transform raw data in various ways prior to storing it as indexed data. Sometimes the search engine configuration information used to process the received raw data may include improper and/or ineffective rules that may generate ineffective index data. If such improper index data may be added to an index store it may pollute the index reducing the quality of search results that may be produced." *Id.* at 1:32-40.

100. The '206 Patent addresses such problems, including by addressing challenges with index data and the rules that generate index data. For example, the '206 Patent claims describe specific techniques and implementations that allow for more efficient and effective generation and

modification of data parsing rules, which prevent improperly indexed data from being added to the index, thus increasing the overall quality of the index and improving the performance of indexing, searching, and processing of the machine data.

101. U.S. Patent No. 9,838,467 ("the '467 Patent"), entitled "Dynamically Instantiating Dual-Queue Systems" duly and legally issued on December 5, 2017, from an application filed on April 29, 2015. A true and correct copy of the '467 Patent is attached as Exhibit K. Splunk is the owner and assignee of all right, title, and interest in and to the '467 Patent, including the right to assert all causes of action arising under said patent and to seek damages and all other remedies for the infringement thereof.

102. The '467 Patent is directed to improvements to computing systems that "perform[] data operations with respect to data stored in one or more repositories of data," and in particular "event-based" systems that operate on machine data in network environments and deal with streams of live data that can be generated faster than they can be handled by certain computer hardware and software. *See* '467 Patent at 1:25-38, 8:47-59. In data server systems and other "system[s] that perform[] data operations . . . , it can be difficult to optimally perform data operations, particularly as the size and/or complexity of a data repository grows. System administrators may add additional system resources to improve performance, but often these resources may not achieve the desired results, and/or the added expense and overhead for the additional system resources is undesirable." *Id.* at 1:25-26; 1:36-42. This complexity can also grow as more "tenants" or "customers" are supported on the data server system.

103. The '467 Patent teaches that "dual-queue" techniques can provide a technical mechanism for addressing these problems. *See, e.g.*, '467 Patent at 8:47-59 (describing "[a]n illustrative situation" in which a queue "is receiving transactions faster than the transactions can

be sent through the in-memory data pathway," which can cause "the pushed transactions [to] be dropped as live transaction data. However, in accordance with various aspects of the present disclosure, the pushed transactions may later be sent as stale transaction data…"). And specifically, the '467 Patent claims disclose improvements to dual-queue functionality through techniques that concern dynamic instantiation and management of dual-queue nodes in an efficient manner, which is particularly useful in multi-tenant dual-queue systems. For example, the '467 Patent teaches instantiation of dual-queue nodes in connection with receipt of live data, such that nodes are not instantiated unnecessarily, and various specific techniques associated with managing and implementing instantiation, termination, migration, and memory allocation related to dual-queue nodes.

104. U.S. Patent No. 10,255,312 ("the '312 Patent"), entitled "Time Stamp Creation for Event Data," duly and legally issued on April 9, 2019, from an application filed on October 31, 2016. A true and correct copy of the '312 Patent is attached as Exhibit L. Splunk is the owner and assignee of all right, title, and interest in and to the '312 Patent, including the right to assert all causes of action arising under said patent and to seek damages and all other remedies for the infringement thereof.

105. The '312 Patent addresses technical problems associated with the manner in which conventional data processing and analysis computer systems handle "time series data organization, search, and retrieval." '312 Patent at 1:27-29. "Time series data are sequences of time stamped records occurring in one or more usually continuous streams, representing some type of activity made up of discrete events," such as "processing logs, market transactions, and sensor data from real-time monitors (supply chains, military operation networks, or security systems). The ability to index, search, and present relevant search results is important to understanding and working

with systems emitting large quantities of time series data," such as those found in big data environments. *Id.* at 1:31-39. Previous "large scale search engines (e.g., Google and Yahoo web search) are designed to address the needs of less time sensitive types of data and are built on the assumption that only one state of the data needs to be stored in the index." *Id.* at 1:40-43. They "don't meet the needs of time series data" generated by, *e.g.*, "[f]irewalls, routers, web servers, application servers and databases [which] constantly generate streams of data in the form of events occurring perhaps hundreds or thousands of times per second." *Id.* at 1:51-61.

106. The '312 Patent notes that "[c]ompared to full text search engines, which organize their indices so that retrieving documents with the highest relevance scores is most efficient, an engine for searching time series data preferably would organize the index so that access to various time ranges, including less recent time ranges, is efficient." *Id.* at 1:62-67. However, indexing time series data is "complicated because the data can be collected from multiple, different sources asynchronously and out of order." *Id.* at 2:6-9. The '312 Patent notes that this in turn leads to various challenges: "Streams of data from one source may be seconds old and data from another source may be interleaved with other sources or may be days, weeks, or months older than other sources. Moreover, data source times may not be in sync with each other, requiring adjustments in time offsets post indexing." *Id.* at 2:9-14. "Furthermore, time stamps can have an almost unlimited number of formats making identification and interpretation difficult. Time stamps within the data can be hard to locate, with no standard for location, format, or temporal granularity (e.g., day, hour, minute, second, sub-second)." *Id.* at 2:14-19.

107. In view of these challenges, the '312 Patent recognizes that conventional technology did not address the need for "[e]nabling real-time operation against large, frequently changing data sets." *Id.* at 3:9-12; *see also id.* at 3:23-27 (recognizing the need for "[t]he ability

to insert, delete and reorganize indices, on the fly as data is collected, without rebuilding the index structure" in order to "index[] time series data and provid[e] real-time search results"). "Timeframes and time-based metadata like frequency, distribution, and likelihood of occurrence are especially important when searching time series data, but difficult to achieve with" conventional methods. *Id*. at 2:35-39.

108. The '312 Patent addresses such problems and concerns techniques and implementations related to "improving machine data analysis" and handling time series data—and in particular for searching, processing, indexing, and transforming machine data—that posed problems for conventional technology. The '312 Patent claims specific techniques and implementations concerning, for example, creating a set of searchable events that involves segmenting raw time series machine data into searchable events and allowing time-based search phrases across a portion of events. The techniques and implementations address, for example, challenges related to the interrelationship of time information and machine data, including detection of time information, generation of accurate time stamps, and calculating an accurate timestamp if time information does not exist in the raw data. The '312 Patent thus addresses technical challenges in conventional systems, helping ensure that all events contain time stamps suitable for an index that can be organized and reorganized on the fly for granular and efficient access to time ranges, and supporting complex time-based search capability while allowing real-time interleaving of new data without requiring a full rebuild of the entire search index. *See*, *e.g.*, *id.* at 2:46-54, 3:23-27.

109. Splunk is the owner and assignee of all right, title, and interest in and to the Patents-in-Suit, including the right to assert all causes of action arising under said patents and to seek damages and all other remedies for the infringement thereof.

110. Moreover, as owner and assignee of the Patents-in-Suit, Splunk has marked its practicing products with the patent numbers of the Patents-in-Suit shortly after their issuance. Splunk marked its practicing products with the address of its Internet marking page, https://www.splunk.com/en_us/legal/patents.html. Splunk regularly updated and continues to regularly update its marking webpage with all of Splunk's patents, including the Patents-in-Suit. With respect to at least the '443, '206, '467, and '312 Patents, Splunk updated its marking webpage to list these patents shortly after their issuance.

111. Cribl has been aware of the Patents-in-Suit, or, at a minimum, willfully blind to their existence, since the approximately the issue date of those patents or the founding of Cribl, whichever is later.

112. All three co-founders of Cribl (Mr. Sharp, Dritan Bitincka, and Ledion Bitincka) occupied senior technical positions at Splunk at the time of their departures from Splunk. Mr. Sharp was a Senior Director of Product Management, Dritan Bitincka was a Principal Architect, and Ledion Bitincka was an Advanced Development Architect. All three co-founders of Cribl, as part of their senior technical roles at Splunk, were heavily involved with Splunk's patent program, and gained knowledge of Splunk's patent program (including as inventors), the scope of Splunk's patent portfolio, and the products related to Splunk's patent portfolio. On information and belief, each knew, for example, that Splunk's products were protected by Splunk patents, including the '206 Patent and '467 Patent, which issued before their departure, and the '443 Patent, '438 Patent, and '312 Patent, which are continuations of Splunk patents that issued before their departure. Indeed, on information and belief, Cribl's three co-founders were aware of Splunk's patent-marking page, *see* Exhibit M, https://www.splunk.com/en_us/legal/patents.html, which listed (and lists) patents that protect Splunk's products, such as Splunk Enterprise, which is a product on

which all three co-founders worked while employed at Splunk, and is a product whose features and implementation details Cribl has, on information and belief, sought to build into its own products.

113. Additionally, a substantial portion of Cribl's employees are ex-Splunk employees. Many of these Splunk employees were also heavily involved with Splunk's patent program, and gained knowledge of Splunk's patent program, the scope of Splunk's patent portfolio, and the products related to Splunk's patent portfolio while working at Splunk. On information and belief, the ex-Splunk employees hired by Cribl were aware of the Splunk patents that protected the Splunk products and technologies upon which they worked, and were aware of Splunk's patent-marking page, which listed those products and patents.

114. Additionally, on information and belief, Cribl has installed and used Splunk software, including Splunk Enterprise, since shortly after Cribl was founded (and before Cribl released any of its software to customers). Splunk's software prominently directs those who use and install its software to Splunk's patent marking webpage, which lists the Patents-in-Suit and the corresponding products and technologies to which they correspond. Given Cribl's efforts to duplicate functionality and implementation details offered by these products and technologies, to the extent Cribl was not aware that it was infringing Splunk's Patents-in-Suit, it was willfully blind to this infringement.

CAUSES OF ACTION

COUNT I: INFRINGEMENT OF THE '443 PATENT BY CRIBL

115. Splunk incorporates by reference as though fully set forth herein the allegations found in Paragraphs 1-114.

116. On information and belief, Cribl has been and is now directly infringing the '443 Patent in violation of 35 U.S.C. § 271(a) at least by making, using, selling, offering for sale, and/or

importing into the United States, at least the Stream and Edge software, through which Cribl practices one or more claims of the ’443 Patent, including at least claim 1.

117. Claim 1 recites (bracketed enumerations added):

> [1pre] A computer-implemented method performed by a remote capture agent coupled to a network, comprising:
>
> > [1a] obtaining configuration information from a configuration server over a network, wherein the configuration information is usable by the remote capture agent to generate timestamped event data from network packets and to transform the timestamped event data into transformed event data;
> >
> > [1b] monitoring network traffic comprising a plurality of network packets;
> >
> > [1c] generating, based on the configuration information, timestamped event data from at least one network packet of the plurality of network packets, wherein generating the timestamped event data includes segmenting the at least one network packet into a plurality of events and associating each event of the plurality of events with a respective timestamp;
> >
> > [1d] and transforming, based on the same configuration information, the timestamped event data into transformed event data, wherein transforming the timestamped event data includes performing an operation involving data contained in at least one event of the plurality of events.

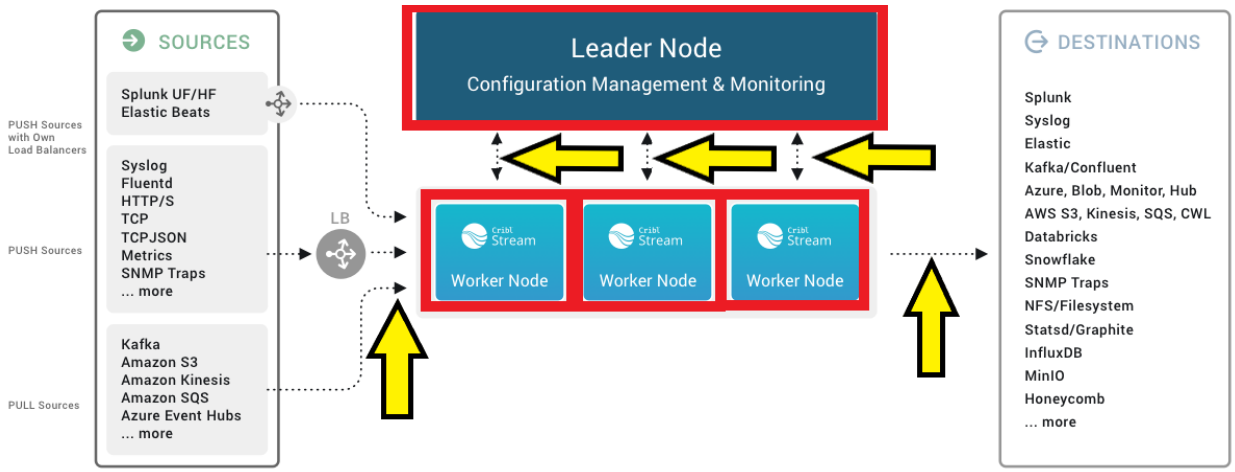
118. By way of non-limiting example, Cribl has infringed claim 1 of the ’443 Patent by committing the following infringing acts, without authorization, consent, permission, or a license from Splunk.

119. On information and belief, and to the extent the preamble is limiting, Cribl, through its Stream and Edge software, performs a computer-implemented method using a remote capture agent coupled to a network, in a manner that satisfies element [1pre] of the ’443 Patent.

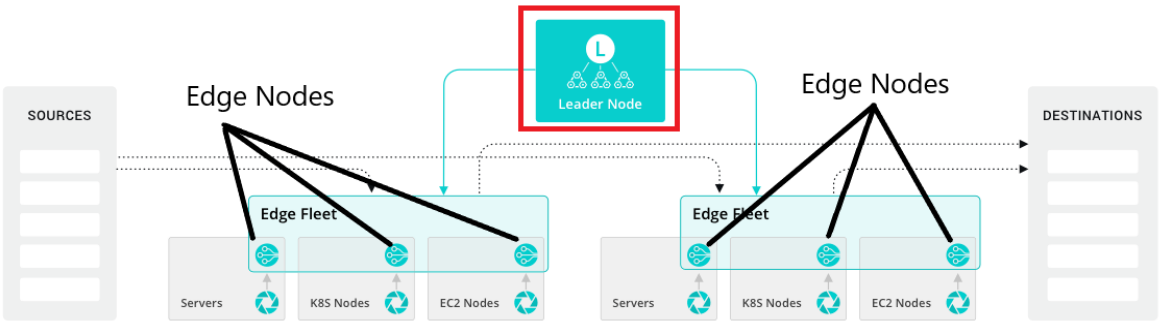
120. For example, Cribl deploys Stream and Edge on distributed systems using multiple computing devices, and configures some of the constituent computing devices to act as remote capture agents, transformation servers, and configuration servers. *See, e.g.*, Cribl Docs: Stream, "Distributed Deployment," https://docs.cribl.io/stream/deploy-distributed; Cribl Docs: Edge, "Basic Concepts," https://docs.cribl.io/edge/basic-concepts.

121. Stream and Edge are deployed in the form of three types of nodes with different responsibilities: Leader Nodes, Worker Nodes, and Edge Nodes. *See, e.g.*, Cribl Docs: Stream, "Distributed Deployment," https://docs.cribl.io/stream/deploy-distributed ("To sustain higher incoming data volumes, and/or increased processing, you can scale from a single instance up to a multi-instance, distributed deployment. The Worker instances are centrally managed by a single Leader Node, which is responsible for keeping configurations in sync, and for tracking and monitoring the instances' activity metrics."); Cribl Docs: Edge, "Basic Concepts," https://docs.cribl.io/edge/basic-concepts.

122. The nodes are connected by network connections and each node is coupled to a network, over which they communicate with each other. *See, e.g.*, Cribl Docs: Stream, "Distributed Deployment," https://docs.cribl.io/stream/deploy-distributed; Cribl Docs: Edge, "Basic Concepts," https://docs.cribl.io/edge/basic-concepts. Cribl controls all three types of nodes through a single interface visible to the user.



Cribl Docs: Stream, "Distributed Deployment," https://docs.cribl.io/stream/deploy-distributed (annotations added).



Cribl Docs: Edge, "Basic Concepts," https://docs.cribl.io/edge/basic-concepts (annotations added)

123. The Leader Node is a central configuration server and centrally authors and controls configuration of the Worker Nodes and Edge Nodes. The Worker and Edge Nodes perform the remote data capture and processing. *See, e.g.*, Cribl Docs: Stream, "Distributed Deployment," https://docs.cribl.io/stream/deploy-distributed; Cribl Docs: Edge, "Basic Concepts," https://docs.cribl.io/edge/basic-concepts.

124. On information and belief, Stream and Edge are substantially similar and are identical in material aspects with regard to the subject matter of the '443 Patent and the other Patents-in-Suit. Cribl Edge incorporates Cribl Stream's features and uses the same underlying technology. *See* Clint Sharp, "Announcing Cribl Edge & Cribl Stream," Cribl Blog,

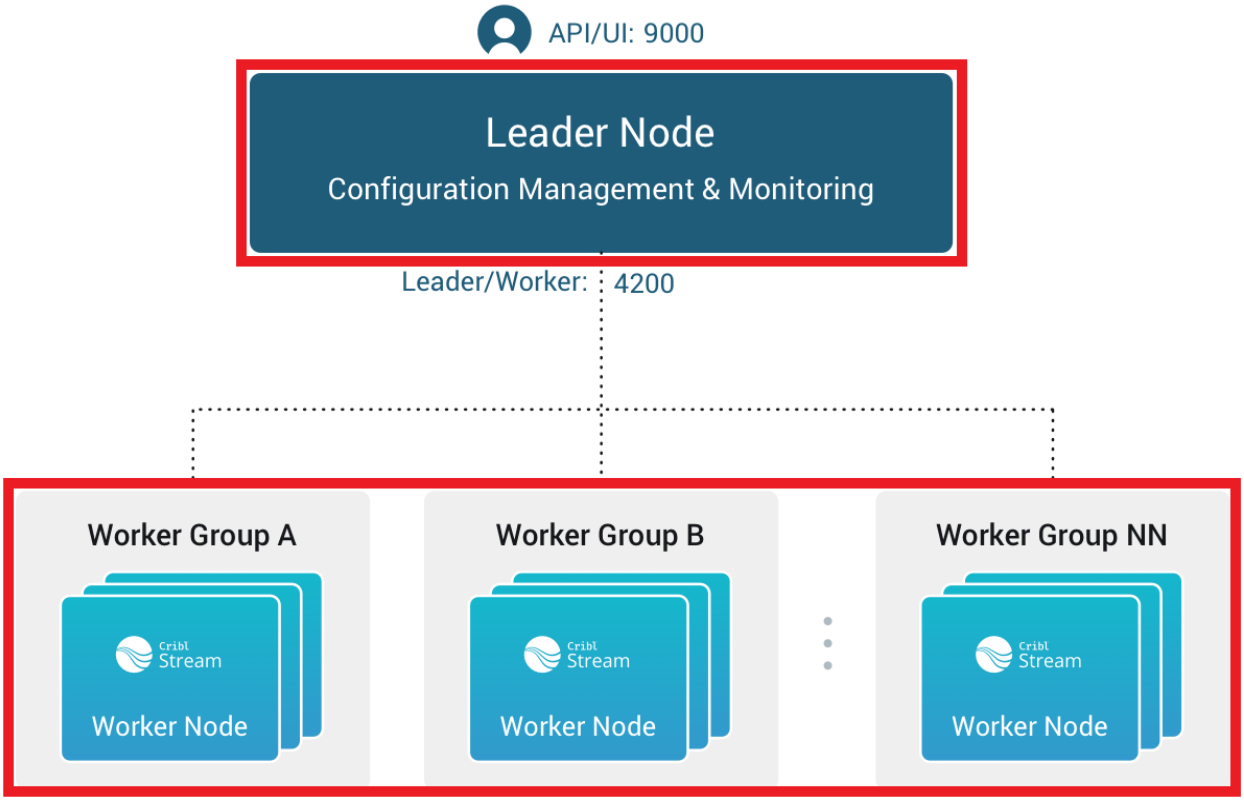
https://cribl.io/blog/announcing-cribl-edge-cribl-stream/ ("Cribl Edge scales down Cribl Stream to run on an edge node. . . . ***because Cribl Edge is the same technology behind Cribl Stream***, all our Packs and configurations can be used with Cribl Edge." (emphasis added)). Additionally, as described earlier, Stream Worker Nodes and Edge Nodes are managed identically, and the user interacts with both Worker Nodes and Edge Nodes through the same user interface.

125. On information and belief, Cribl, through its Stream and Edge software, causes the remote capture agent to obtain configuration information from a configuration server over a network, where the configuration information is usable to generate timestamped event data and transform the data, in a manner that satisfies element [1a] of the '443 Patent.

126. For example, Worker Nodes and Edge Nodes are "fully managed by . . . Leader Node[s]" and receive configuration information from Leader Nodes before the Worker Nodes and Edge Nodes can take any actions on data. Cribl Docs: Stream, "Distributed Deployment," https://docs.cribl.io/stream/deploy-distributed; *see also* Cribl Docs: Edge, "Basic Concepts," https://docs.cribl.io/edge/basic-concepts.

127. Cribl instructs Leader Nodes to send configuration information to Worker and Edge Nodes that is usable to generate timestamped event data from incoming network packets and transform the data. First, Worker and Edge Nodes receive configuration information from the Leader Node instructing the Worker and Edge Nodes to initialize and use Event Breakers to generate timestamped event data. Upon receiving the configuration information, the Worker and Edge Nodes initialize Event Breakers and generate event streams based on the instructions received in the configuration information. Cribl Event Breakers take in raw data and generate timestamped events from that raw data, and the events generated include portions of the raw data. *See, e.g.*, Cribl Docs: Stream, "Event Breakers," https://docs.cribl.io/stream/event-breakers

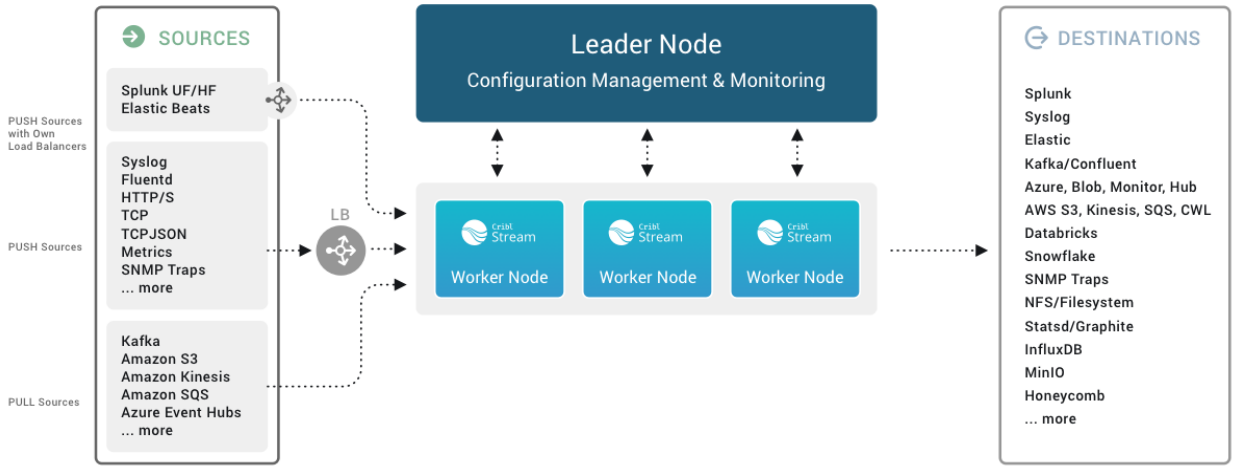
("Event Breakers help break incoming streams of data into discrete events."); Cribl Docs: Edge, "Event Breakers," https://docs.cribl.io/edge/event-breakers. Second, Worker and Edge Nodes receive configuration information instructing the Nodes to apply Functions to the data, transforming or modifying the data. As with Event Breakers, configuration information sent by the Leader Node is what prepares Worker and Edge Nodes to use Functions. Upon receiving the configuration information, the Worker and Edge Nodes apply the Functions to the data and transform the data according to the configuration information. *See, e.g.*, Cribl Docs: Stream, "Basic Concepts," https://docs.cribl.io/stream/basic-concepts ("At its core, a Function is a piece of code that executes on an event, and that encapsulates the smallest amount of processing that can happen to that event."); *see also* Cribl Docs: Edge, "Basic Concepts," https://docs.cribl.io/edge/basic-concepts.



Cribl Docs: Stream, "Distributed Deployment," https://docs.cribl.io/stream/deploy-distributed (annotations added)

128. On information and belief, Cribl, through its Stream and Edge software, monitors network traffic comprising a plurality of network packets, in a manner that satisfies element [1b] of the '443 Patent.

129. For example, Stream and Edge monitor incoming network traffic delivered over packetized network communication protocols, such as TCP. *See, e.g.*, Cribl Docs: Stream, "TCP (Raw)," https://docs.cribl.io/stream/sources-tcp-raw; Cribl Docs: Edge, "TCP (Raw)," https://docs.cribl.io/edge/sources-tcp-raw.

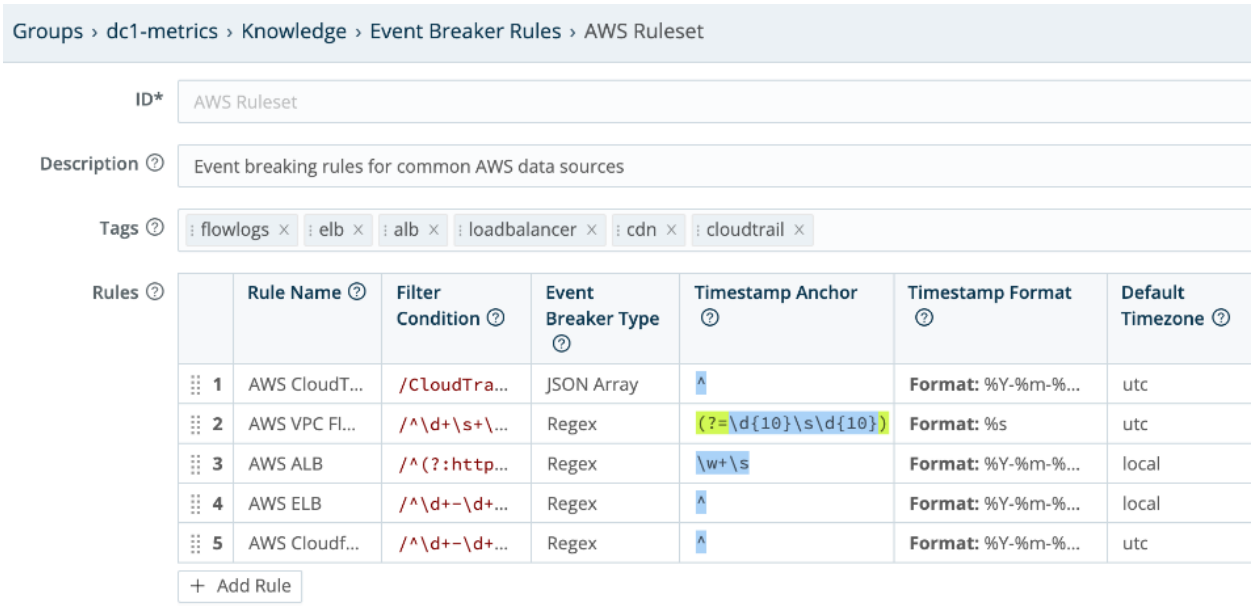


Cribl Docs: Stream, "Distributed Deployment," https://docs.cribl.io/stream/deploy-distributed

130. On information and belief, Cribl, through its Stream and Edge software, generates timestamped event data from incoming network packets, in a manner that satisfies element [1c] of the '443 Patent.

131. For example, Stream and Edge use Event Breakers to generate event data from incoming raw data. *See, e.g.*, Cribl Docs: Stream, "Event Breakers," https://docs.cribl.io/stream/event-breakers/; Cribl Docs: Edge, "Event Breakers," https://docs.cribl.io/edge/event-breakers. As explained above, Event Breakers apply filtering rules

to incoming data received as network packets, parse the incoming data into events, and then associate a timestamp with the newly created events.

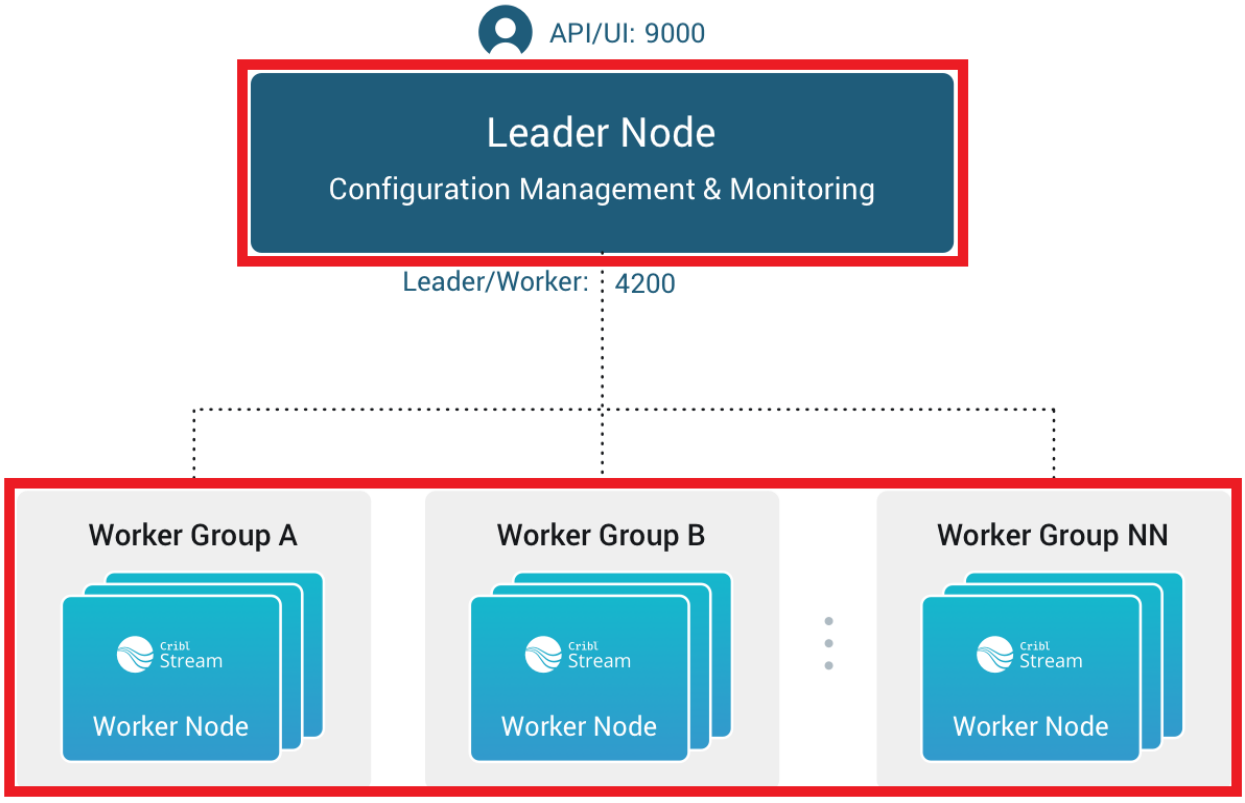


Cribl Docs: Stream, "Event Breakers," https://docs.cribl.io/stream/event-breakers.

132. On information and belief, Cribl, through its Stream and Edge software, transforms, based on the configuration information, the timestamped event data into transformed event data by performing an operation on data contained inside the timestamped event data, in a manner that satisfies element [1d] of the '443 Patent.

133. For example, as explained above, Worker Nodes and Edge Nodes receive configuration information from Leader Nodes instructing them to apply Functions to the timestamped event data generated from the incoming raw network packet data. *See, e.g.*, Cribl Docs: Stream, "Functions," https://docs.cribl.io/stream/functions ("When events enter [the system], they're processed by a series of Functions. At its core, a Function is code that executes on an event, and it encapsulates the smallest amount of processing that can happen to that event."); Cribl Docs: Edge, "Functions," https://docs.cribl.io/edge/functions. Upon receiving the configuration information from the Leader Node, the Worker and Edge Nodes apply the Functions

to the timestamped event data. Functions operate on each event that they are applied to, and "access any field within the event object," transforming the data contained within each event in multiple ways. *Id.*



Cribl Docs: Stream, "Distributed Deployment," https://docs.cribl.io/stream/deploy-distributed (annotations added)

134. Cribl's infringement is literal, under the doctrine of equivalents, or both, and its infringement is also willful. The demonstration of Cribl's infringement of claim 1 of the '443 Patent, above, is exemplary and non-limiting.

135. Cribl had actual knowledge and constructive knowledge of the '443 Patent since as early as the issue date of the '443 Patent, as described earlier in Paragraphs 85–89 and 110–114 (which Splunk incorporates by reference herein).

136. On information and belief, Cribl has been and is now indirectly infringing the '443 Patent in violation of 35 U.S.C. § 271(b) at least by instructing, encouraging, implementing, and/or

directing others how to use Stream and Edge in ways that directly infringe the '443 Patent, including claim 1, through its educational and promotional materials, support activities, as well as its service and consulting activities. Cribl has committed and continues to commit affirmative acts that cause infringement of one or more claims of the '443 Patent with knowledge of the '443 Patent and knowledge or willful blindness that the induced acts constitute infringement of one or more claims of the '443 Patent. By way of example, as set forth above, Cribl publishes on its website and on YouTube instructions that, when followed in conjunction with use of Cribl's Stream and Edge, infringe one or more claims of the '443 Patent.

137. On information and belief, Cribl contributes to the infringement of at least claim 1 of the '443 Patent by others, including its customers, distributors, and authorized resellers in violation of 35 U.S.C. § 271(c). Cribl has committed and continues to commit affirmative acts that contribute to the infringement by others, including, but not limited to, the sale, offer for sale, and/or import by Cribl of Stream and Edge in the United States, with knowledge of the '443 Patent and knowledge that Stream and Edge have no substantial non-infringing uses. Stream and Edge are especially made for or adapted for use to infringe, are not staple articles of commerce, and are not suitable for substantial non-infringing use. By way of example, Cribl sells Stream and Edge to customers who use Stream and Edge in an infringing manner, as set forth above. Stream and Edge are especially made for and/or adapted for use to infringe the '443 Patent because, on information and belief, Worker and Edge Nodes are designed to operate based on configuration information received from the Leader Node, and because Stream and Edge are designed to operate on data based on event streams generated from raw data.

138. Cribl will continue to infringe, induce infringement of, and contribute to infringement of the '443 Patent, causing irreparable harm to Splunk for which there is no adequate

remedy at law, unless enjoined by this Court. Cribl's infringement has caused and continues to cause irreparable harm to Splunk in the form of loss of business opportunities, lost sales, loss of market share, loss of goodwill, and the loss of Splunk's exclusive right to practice its inventions.

139. As a result of Cribl's willful infringement of the '443 Patent, Splunk has suffered damages and is owed no less than a reasonable royalty under 35 U.S.C. § 284 as a remedy. On information and belief, Cribl has known that its activities concerning Stream and Edge infringed one or more claims of the '443 Patent since at least September 2017.

140. On information and belief, Cribl has made no attempt to design around the claims of the '443 Patent.

141. On information and belief, Cribl does not have and has not had a reasonable basis for believing that the claims of the '443 Patent were invalid.

142. On information and belief, Cribl's Stream and Edge are available to businesses and individuals throughout the United States and in this judicial District. On information and belief, Cribl has committed acts of infringement in this District, including by inducing infringement within the State of Delaware.

COUNT II: INFRINGEMENT OF THE '438 PATENT BY CRIBL

143. Splunk incorporates by reference as though fully set forth herein the allegations found in Paragraphs 1-142.

144. On information and belief, Cribl has been and is now directly infringing the '438 Patent in violation of 35 U.S.C. § 271(a) at least by making, using, selling, offering for sale, and/or importing into the United States, at least Stream and Edge, through which Cribl practices one or more claims of the '438 Patent, including at least claim 1.

145. Claim 1 recites (bracketed enumerations added):

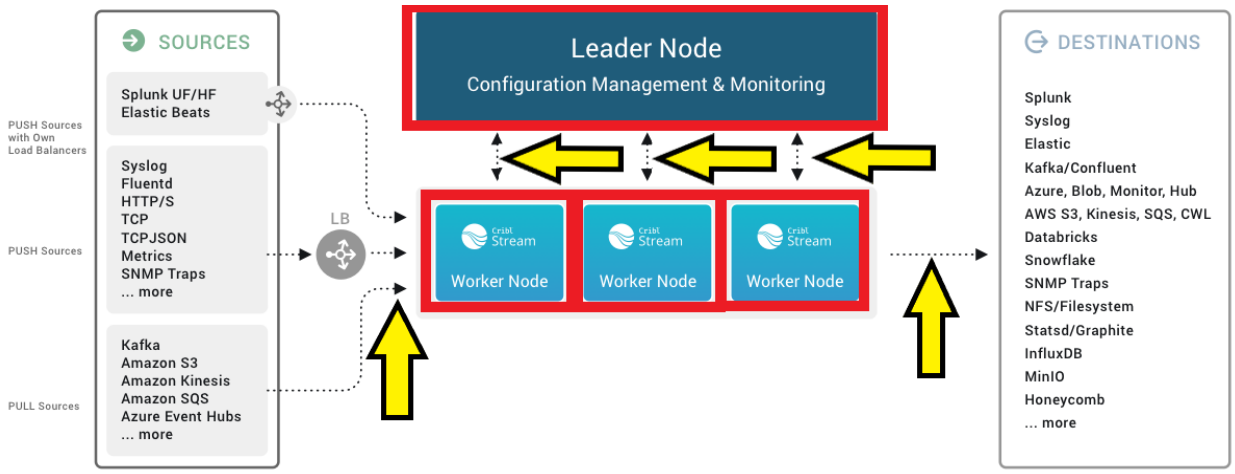
> [1pre] A computer-implemented method performed by a configuration server coupled to a remote capture agent via one or more networks, the method comprising:
>
> > [1a] receiving input requesting creation of an event stream to be generated by the remote capture agent, the input including:
> >
> > [1b] an indication of a protocol to be associated with the event stream, wherein the protocol is used by network traffic monitored by the remote capture agent, and
> >
> > [1c] a selection of an event attribute associated with the protocol, the event attribute indicating data to be extracted from network packets of the network traffic monitored by the remote capture agent;
> >
> > [1d] generating configuration data based on the input; and
> >
> > [1e] sending the configuration data to the remote capture agent, the configuration data causing the remote capture agent to generate the event stream based on the network traffic monitored by the remote capture agent and according to the configuration data.

146. By way of non-limiting example, Cribl has infringed claim 1 of the ’438 Patent by committing the following infringing acts without authorization, consent, permission or a license from Splunk.

147. On information and belief, Stream and Edge are substantially similar and are identical in all material aspects with regards to the subject matter of the ’438 Patent and the other Patents-in-Suit, as discussed in Paragraph 124 above.

148. On information and belief, and to the extent the preamble is limiting, Cribl, through its Stream and Edge software, performs a computer-implemented method using a configuration server coupled to a remote capture agent via a network, in a manner that satisfies element [1pre] of the ’438 Patent.

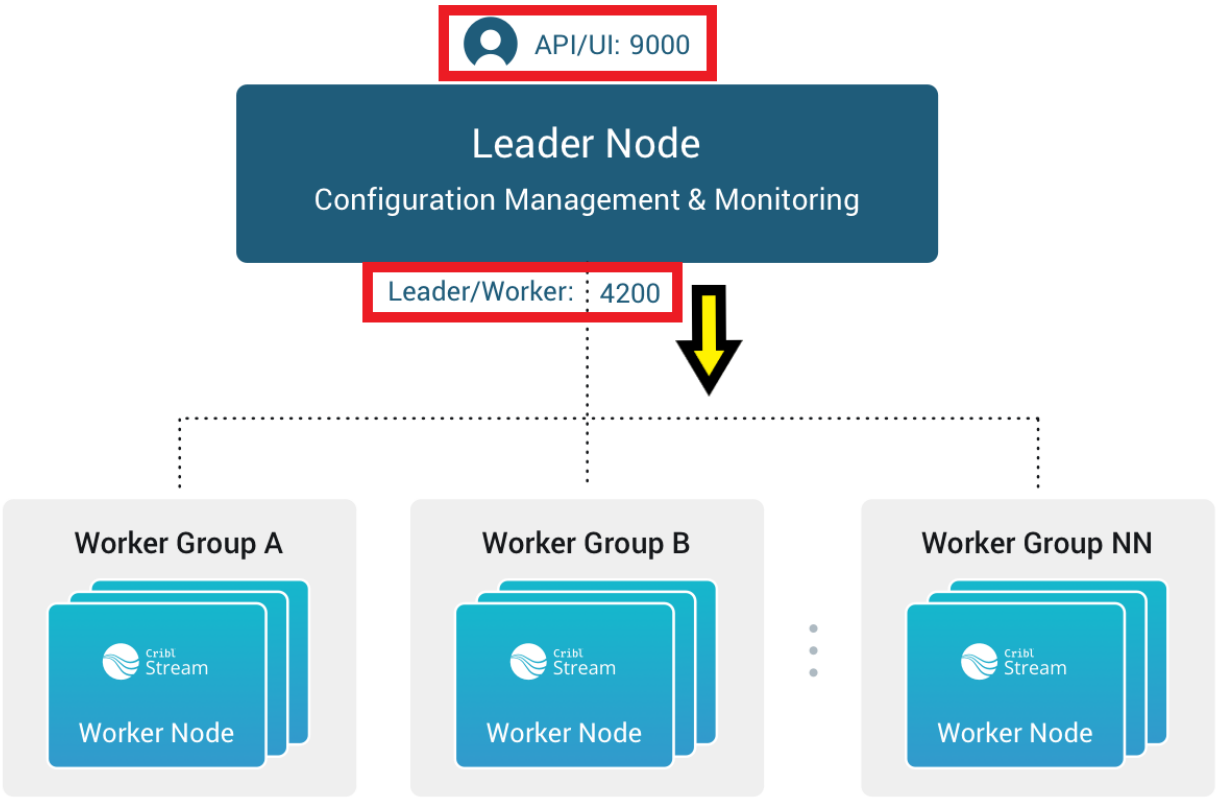
149. As explained above, Cribl deploys Stream and Edge on distributed systems and networks using multiple computing devices, and configures some of the constituent computing devices to act as remote capture agents, transformation servers, and configuration servers. *See, e.g.*, Cribl Docs: Stream, "Distributed Deployment," https://docs.cribl.io/stream/deploy-distributed; Cribl Docs: Edge, "Basic Concepts," https://docs.cribl.io/edge/basic-concepts. Stream and Edge are deployed in the form of three types of nodes with different responsibilities: Leader Nodes, Worker Nodes, and Edge Nodes. *See, e.g.*, Cribl Docs: Stream, "Distributed Deployment," https://docs.cribl.io/stream/deploy-distributed; Cribl Docs: Edge, "Basic Concepts," https://docs.cribl.io/edge/basic-concepts. The nodes are connected by network connections and each node is coupled to a network, over which they communicate with each other. *See, e.g.*, Cribl Docs: Stream, "Distributed Deployment," https://docs.cribl.io/stream/deploy-distributed; Cribl Docs: Edge, "Basic Concepts," https://docs.cribl.io/edge/basic-concepts.



Cribl Docs: Stream, "Distributed Deployment," https://docs.cribl.io/stream/deploy-distributed (annotations added).

150. On information and belief, Cribl, through its Stream and Edge software, causes the configuration server to receive input requesting creation of an event stream to be generated by the remote capture agent, in a manner that satisfies element [1a] of the '438 Patent.

151. For example, Leader Nodes are controlled and programmed using the Stream user interface and API, and receive input from the API directing each Leader Node how to control the Worker and Edge Nodes associated with the relevant Leader Node. *See, e.g.*, Cribl Docs: Stream, "Distributed Deployment," https://docs.cribl.io/stream/deploy-distributed; Cribl Docs: Edge, "Basic Concepts," https://docs.cribl.io/edge/basic-concepts.



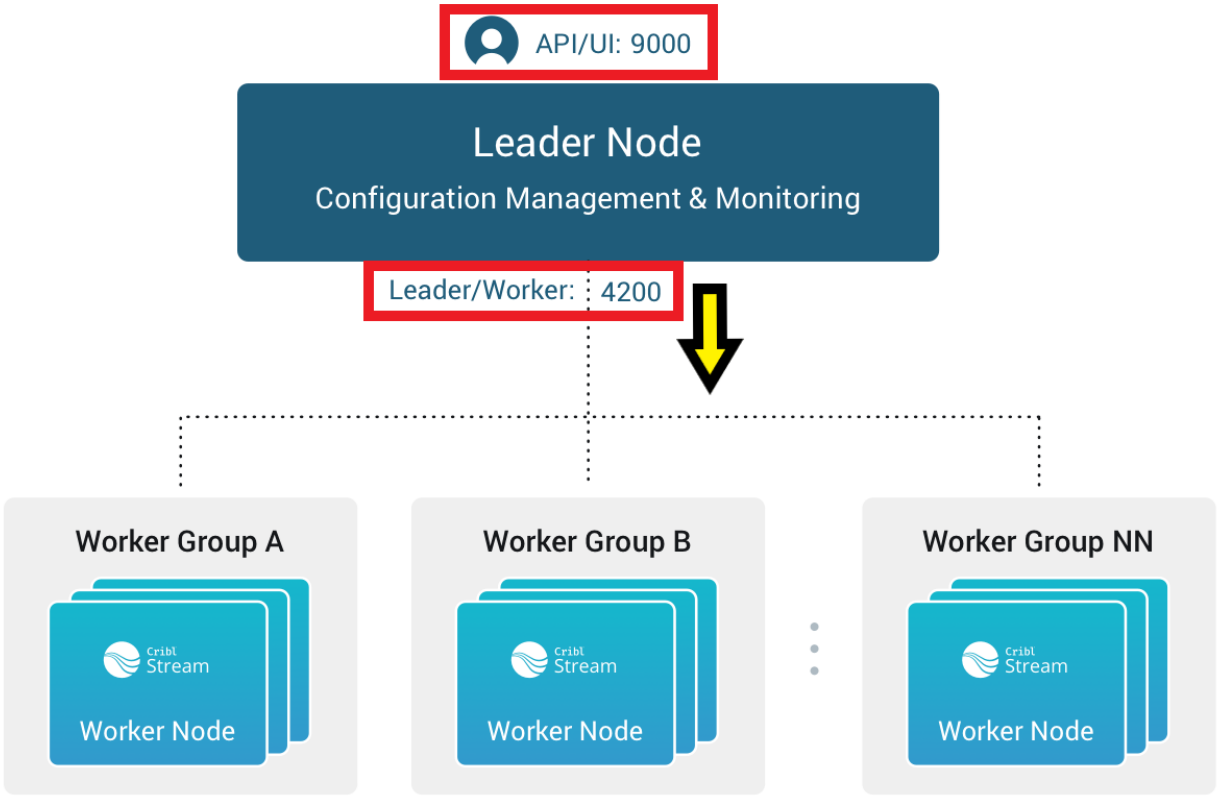
Cribl Docs: Stream, "Distributed Deployment," https://docs.cribl.io/stream/deploy-distributed (annotations added).

152. Leader Nodes are instructed to configure Worker and Edge Nodes—using Event Breakers, as described earlier—to generate an event stream from incoming network traffic. *See, e.g.*, Cribl Docs: Stream, "Event Breakers," https://docs.cribl.io/stream/event-breakers; Cribl Docs: Edge, "Event Breakers," https://docs.cribl.io/edge/event-breakers.

153. On information and belief, Cribl, through its Stream and Edge software, causes a configuration server to receive an indication of a protocol to be associated with an event stream

wherein the protocol is used by network traffic monitored by a remote capture agent, in a manner that satisfies element [1b] of the '438 Patent.

154. For example, Leader Nodes are provided with the specific protocol used by the network traffic monitored by the Worker and Edge nodes so that the Leader Node can generate the correct configuration information for the Worker and Edge Nodes. *See, e.g.*, Cribl Docs: Stream, "Distributed Deployment," https://docs.cribl.io/stream/deploy-distributed; Cribl Docs: Stream, "TCP (Raw)," https://docs.cribl.io/stream/sources-tcp-raw; *see also* Cribl Docs: Edge, "Deployment Planning," https://docs.cribl.io/edge/deploy-planning; Cribl Docs: Edge, "TCP (Raw)," https://docs.cribl.io/edge/sources-tcp-raw. As explained above, Leader Nodes centrally author configuration information for Worker and Edge Nodes, and Worker Nodes do not operate on data until Leader Nodes provide configuration information, including the protocol used by the network traffic the Worker and Edge Nodes monitor.



Cribl Docs: Stream, "Distributed Deployment," https://docs.cribl.io/stream/deploy-distributed (annotations added)

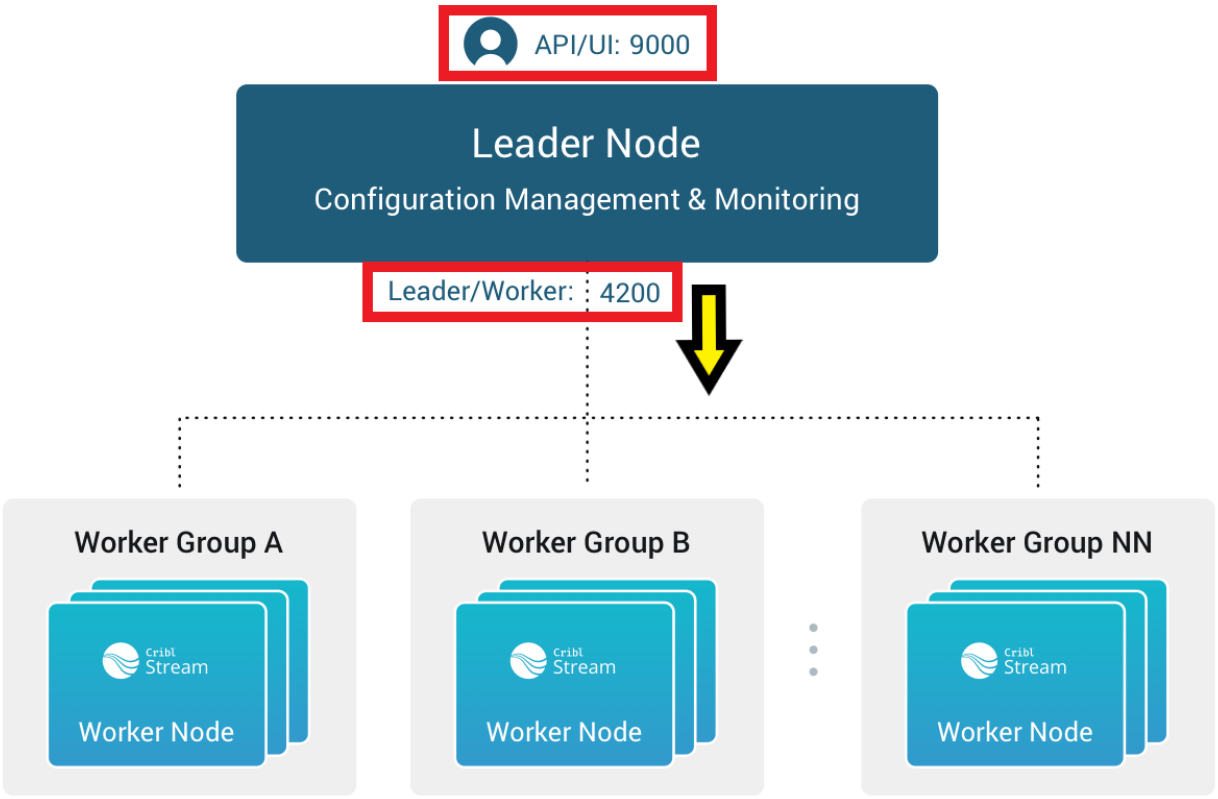
155. On information and belief, Cribl, through its Stream and Edge software, causes a configuration server to receive a selection of an event attribute associated with the protocol, the attribute indicating the data to be extracted by incoming network packets, in a manner that satisfies element [1c] of the '438 Patent.

156. For example, Leader Nodes receive a selection of event attributes when instructed to generate configuration information for accepting data from sources via network packets. *See, e.g.*, Cribl Docs: Stream, "TCP (Raw)," https://docs.cribl.io/stream/sources-tcp-raw; Cribl Docs: Edge, "TCP (Raw)," https://docs.cribl.io/edge/sources-tcp-raw. As one non-limiting example, Leader Nodes are instructed to use Event Breakers, as described earlier, when generating configuration information for sources sending network packets using the TCP protocol. *See* Cribl Docs: Stream, "TCP (Raw)," https://docs.cribl.io/stream/sources-tcp-raw; Cribl Docs: Edge, "TCP (Raw)," https://docs.cribl.io/edge/sources-tcp-raw. Thus, as explained above, Leader Nodes receive event attributes through incorporating Event Breakers.

157. On information and belief, Cribl, through its Stream and Edge software, causes the configuration server to generate configuration data based on the input received, in a manner that satisfies element [1d] of the '438 Patent.

158. For example, Leader Nodes are controlled and programmed using the Stream user interface and API, and receive input from the API directing each Leader Node how to control the Worker and Edge Nodes associated with the relevant Leader Node. *See, e.g.*, Cribl Docs: Stream, "Distributed Deployment," https://docs.cribl.io/stream/deploy-distributed; Cribl Docs: Edge, "Deployment Planning," https://docs.cribl.io/edge/deploy-planning. Leader Nodes centrally

author configuration information, and configuration information for the Worker and Edge nodes is generated at the Leader Node.



Cribl Docs: Stream, "Distributed Deployment," https://docs.cribl.io/stream/deploy-distributed (annotations added)

159. On information and belief, Cribl, through its Stream and Edge software, causes the configuration server to send the configuration data to the remote capture agent, causing the remote capture agent to generate an event stream, in a manner that satisfies element [1e] of the '438 Patent.

160. For example, as explained above, Leader Nodes are the "central location for authoring, validating, deploying, and synchronizing configurations" of Worker and Edge Nodes. Cribl Docs: Stream, "Distributed Deployment," https://docs.cribl.io/stream/deploy-distributed; *see also* Cribl Docs: Edge, "Deployment Planning," https://docs.cribl.io/edge/deploy-planning. Once the Leader Node has received instructions and has generated configuration data, it sends configuration data to the Worker and Edge Nodes. The Worker and Edge Nodes, upon receiving

the configuration information, begin generating event streams based on instructions received in the configuration data.

161. Cribl's infringement is literal, under the doctrine of equivalents, or both, and its infringement is also willful. The demonstration of Cribl's infringement of claim 1 of the '438 Patent, above, is exemplary and non-limiting.

162. Cribl had actual knowledge and constructive knowledge of the '443 Patent since as early as the issue date of the '438 Patent, as described earlier in Paragraphs 85–89 and 110–114 (which Splunk incorporates by reference here).

163. On information and belief, Cribl has been and is now indirectly infringing the '438 Patent in violation of 35 U.S.C. § 271(b) at least by instructing, encouraging, implementing, and/or directing others how to use Stream and Edge in ways that directly infringe the '438 Patent, including claim 1, through its educational and promotional materials, support activities, as well as its service and consulting activities. Cribl has committed and continues to commit affirmative acts that cause infringement of one or more claims of the '438 Patent with knowledge of the '438 Patent and knowledge or willful blindness that the induced acts constitute infringement of one or more claims of the '438 Patent. By way of example, as set forth above, Cribl publishes on its website and on YouTube instructions that, when followed in conjunction with use of Cribl's Stream and Edge, infringe one or more claims of the '438 Patent.

164. On information and belief, Cribl contributes to the infringement of at least claim 1 of the '438 Patent by others, including its customers, distributors, and authorized resellers in violation of 35 U.S.C. § 271(c). Cribl has committed and continues to commit affirmative acts that contribute to the infringement by others, including, but not limited to, the sale, offer for sale, and/or import by Cribl of Stream and Edge in the United States, with knowledge of the '438 Patent and

knowledge that Stream and Edge have no substantial non-infringing uses. Stream and Edge are especially made for or adapted for use to infringe, are not staple articles of commerce, and are not suitable for substantial non-infringing use. By way of example, Cribl sells Stream and Edge to customers who use Stream and Edge in an infringing manner, as set forth above. Stream and Edge are especially made for or adapted for use to infringe the '438 Patent because, on information and belief, Worker and Edge Nodes are designed to operate based on configuration information received from the Leader Node, and because Stream and Edge are designed to operate on data based on event streams generated from raw data.

165. Cribl will continue to infringe, induce infringement of, and contribute to infringement of the '438 Patent, causing irreparable harm to Splunk for which there is no adequate remedy at law, unless enjoined by this Court. Cribl's infringement has caused and continues to cause irreparable harm to Splunk in the form of loss of business opportunities, lost sales, loss of market share, loss of goodwill, and the loss of Splunk's exclusive right to practice its inventions.

166. As a result of Cribl's willful infringement of the '438 Patent, Splunk has suffered damages and is owed no less than a reasonable royalty under 35 U.S.C. § 284 as a remedy. On information and belief, Cribl has known that its activities concerning Stream and Edge infringed one or more claims of the '438 Patent since at least October 2020.

167. On information and belief, Cribl has made no attempt to design around the claims of the '438 Patent.

168. On information and belief, Cribl does not have and has not had a reasonable basis for believing that the claims of the '438 Patent were invalid.

169. On information and belief, Cribl's Stream and Edge are available to businesses and individuals throughout the United States and in this judicial District. On information and belief,

Cribl has committed acts of infringement in this District, including by inducing infringement within the State of Delaware.

COUNT III: INFRINGEMENT OF THE '206 PATENT BY CRIBL

170. Splunk incorporates by reference as though fully set forth herein the allegations found in Paragraphs 1-169.

171. On information and belief, Cribl has been and is now directly infringing the '206 Patent in violation of 35 U.S.C. § 271(a) at least by making, using, selling, offering for sale, and/or importing into the United States, at least Stream and Edge, through which Cribl practices one or more claims of the '206 Patent, including at least claim 1.

172. Claim 1 recites (bracketed enumerations added):

[1pre] A method, comprising:

> [1a] selecting a portion of raw data from at least one data source;
>
> [1b] analyzing at least the selected portion of raw data to find a match of a signature or pattern of a known data type, the match corresponding to a parsing rule in a plurality of stored parsing rules;
>
> [1c] parsing the selected portion of raw data into a set of searchable, time-stamped events using the parsing rule corresponding to the match, each searchable, time-stamped event in the set of searchable, time-stamped events including raw data from the selected portion of raw data;
>
> [1d] causing display of a preview of at least a portion of the set of searchable, time-stamped events in a graphical user interface;
>
> [1e] and in response to user input received via the graphical user interface, processing raw data from the at least one data source using the parsing rule corresponding to the match, to create searchable, time-stamped events, the processed raw data including at least some data not in the selected portion of raw data;

> [1f] wherein the method is performed by one or more computing devices.

173. By way of non-limiting example, Cribl has infringed claim 1 of the ’206 Patent by committing the following infringing acts, without authorization, consent, permission or a license from Splunk.

174. On information and belief, Stream and Edge are substantially similar and are identical in all material aspects with regards to the subject matter of the ’206 Patent and the other Patents-in-Suit, as discussed in Paragraph 124 above.

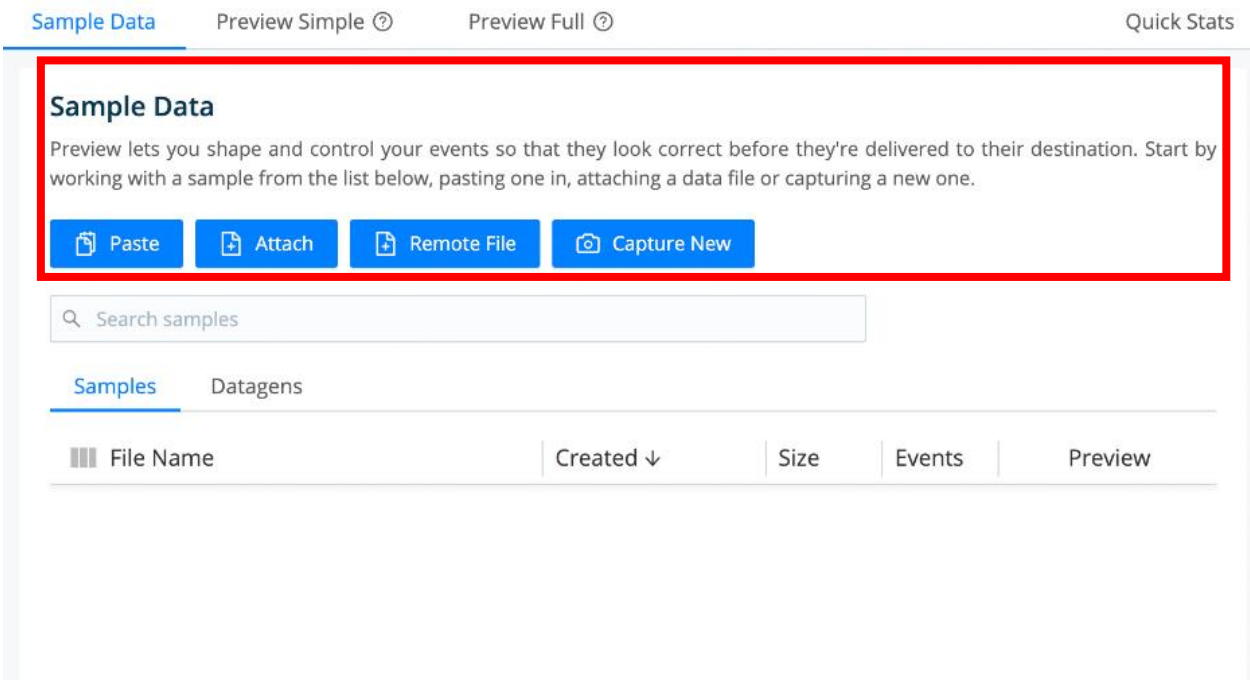
175. On information and belief, and to the extent the preamble is limiting, Cribl, through its Stream and Edge software, performs a computerized method for providing a user with a graphical user interface that displays a preview of at least a portion of raw data that has been analyzed and parsed into a set of time-stamped events and then processing the rest of the data according to user input, in a manner that satisfies element [1pre] of the ’206 Patent.

176. For example, Stream and Edge include functionality entitled Data Preview, which enables users to sample a subset of incoming data, turn the sample into a set of events, view the sampled events, and process other data in response to user input. *See, e.g.*, Cribl Docs: Stream, “Data Preview,” https://docs.cribl.io/stream/data-preview; Cribl Docs: Edge, “Data Preview,” https://docs.cribl.io/edge/data-preview. Data Preview processes the sample using Functions, the collection of which Cribl calls a Pipeline. *See, e.g.*, Cribl Docs: Stream, “Data Preview,” https://docs.cribl.io/stream/data-preview; Cribl Docs: Edge, “Data Preview,” https://docs.cribl.io/edge/data-preview. The “Data Preview features enable you to visually inspect events as they flow into and out of a Pipeline. Preview helps you shape and control events before they're delivered . . . , and helps you troubleshoot Pipeline Functions. Preview works by taking a set of sample events and passing them through the Pipeline, while displaying the inbound and

outbound results in a separate pane. Any time a Function is modified, added, or removed, the Pipeline changes, and so does its displayed output." *See, e.g.*, Cribl Docs: Stream, "Data Preview," https://docs.cribl.io/stream/data-preview; Cribl Docs: Edge, "Data Preview," https://docs.cribl.io/edge/data-preview.

177. On information and belief, Cribl, through its Stream and Edge software, selects a portion of raw data from at least one data source, in a manner that satisfies element [1a] of the '206 Patent.

178. For example, Data Preview provides multiple ways to select portions of raw data. *See, e.g.*, https://www.youtube.com/watch?_v=hsfyafZ55Oo at 9:15; Cribl Docs: Stream, "Data Preview," https://docs.cribl.io/stream/data-preview (". . . you can add samples through any of the supported options: Paste, Attach, Remote File, or Capture New. The Paste, Attach, and Remote File options work with content that needs to be broken into events . . . ."). The selected raw data that enters Data Preview is a sample taken from a raw data stream. *See, e.g.*, Cribl Docs: Stream, "Data Preview," https://docs.cribl.io/stream/data-preview; Cribl Docs: Edge, "Data Preview," https://docs.cribl.io/edge/data-preview.



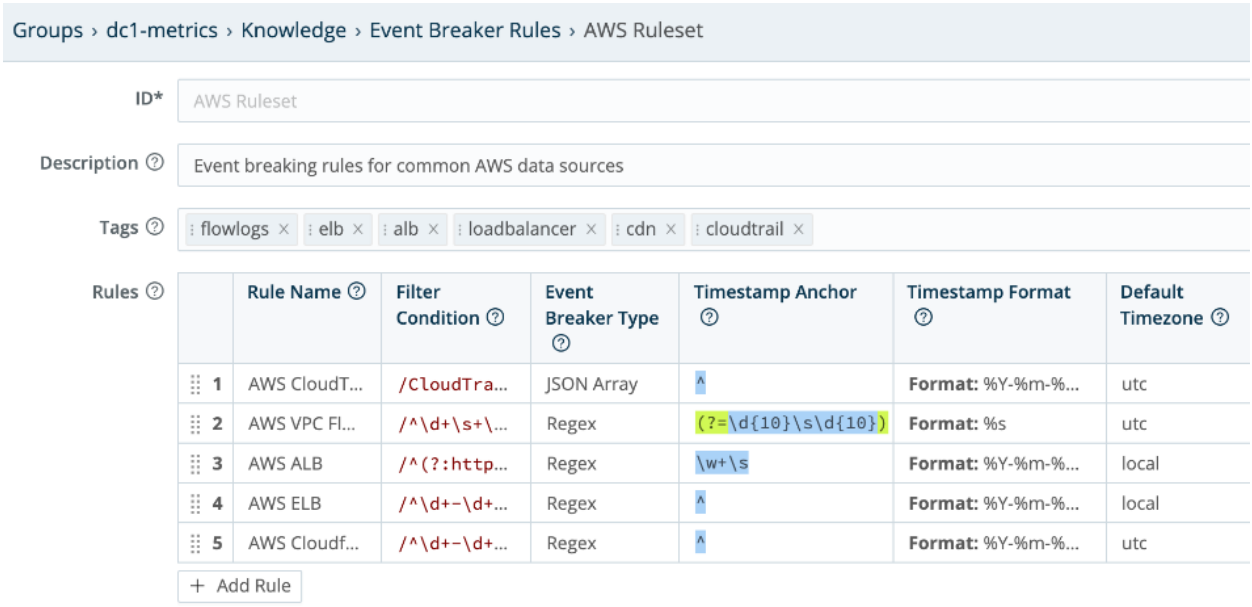
Cribl Docs: Stream, "Data Preview," https://docs.cribl.io/stream/data-preview (annotations added).

179. On information and belief, Cribl, through its Stream and Edge software, analyzes the selected portion of raw data to find a match to a stored parsing rule, in a manner that satisfies element [1b] of the '206 Patent.

180. For example, Data Preview incorporates Event Breakers into its sample data addition process. *See, e.g.*, Cribl Docs: Stream, "Data Preview," https://docs.cribl.io/stream/data-preview; Cribl Docs: Edge, "Data Preview," https://docs.cribl.io/edge/data-preview.

181. Event Breakers apply a stored filtering rule to incoming data and use the filtering rule to find any match in the set of incoming data. *See* Cribl Docs: Stream, "Event Breakers," https://docs.cribl.io/stream/event-breakers/ ("As a stream of data moves into the engine, a rule's filter expression is applied. If the expression evaluates to true, the rule configurations are engaged for the entire duration of that stream."); *see also* Cribl Docs: Edge, "Data Preview," https://docs.cribl.io/edge/data-preview. The filtering is definable using regular expressions, or regex, which search through incoming data to find a match to the defined parsing rule. *See, e.g.*,

Cribl Docs: Stream, "Event Breakers," https://docs.cribl.io/stream/event-breakers/ ("As a stream of data moves into the engine, a rule's filter expression is applied."); *see also* Cribl Docs: Edge, "Data Preview," https://docs.cribl.io/edge/data-preview.

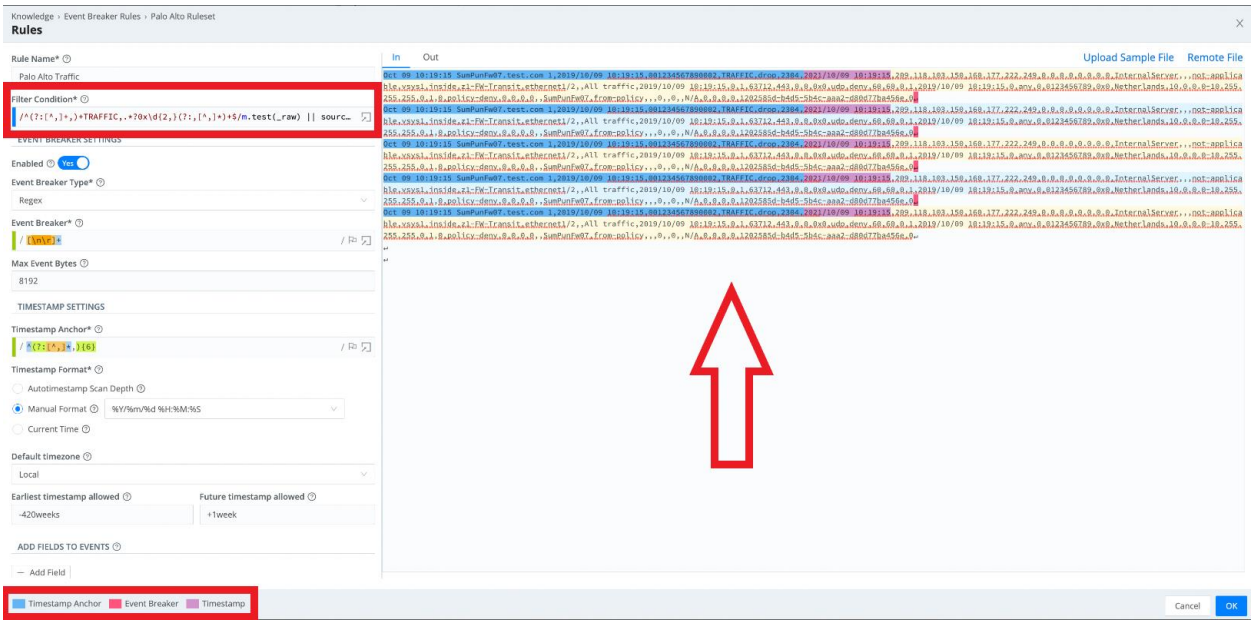


Cribl Docs: Stream, "Event Breakers," https://docs.cribl.io/stream/event-breakers (annotations added; displaying parsing rules for Event Breakers, including user-defined parsing rules)

182. On information and belief, Cribl, through its Stream and Edge software, parses the selected sample of raw data using the stored parsing rule and generates a set of searchable, time-stamped events that includes raw data, in a manner that satisfies element [1c] of the '206 Patent.

183. For example, the Event Breakers incorporated into Data Preview—after finding data that matches their stored parsing rule—take the matching portion of data and generate an event that corresponds to the match. *See, e.g.*, Cribl Docs: Stream, "Event Breakers," https://docs.cribl.io/stream/event-breakers/; Cribl Docs: Edge, "Event Breakers," https://docs.cribl.io/edge/event-breakers. The matching portion of data is then placed into the event, and the event is given a timestamp. After the event has been timestamped, it is placed into the set of searchable, timestamped events that is displayed to the user through the Data Preview interface. *See, e,g.*, Cribl Docs: Stream, "Data Preview," https://docs.cribl.io/stream/data-preview

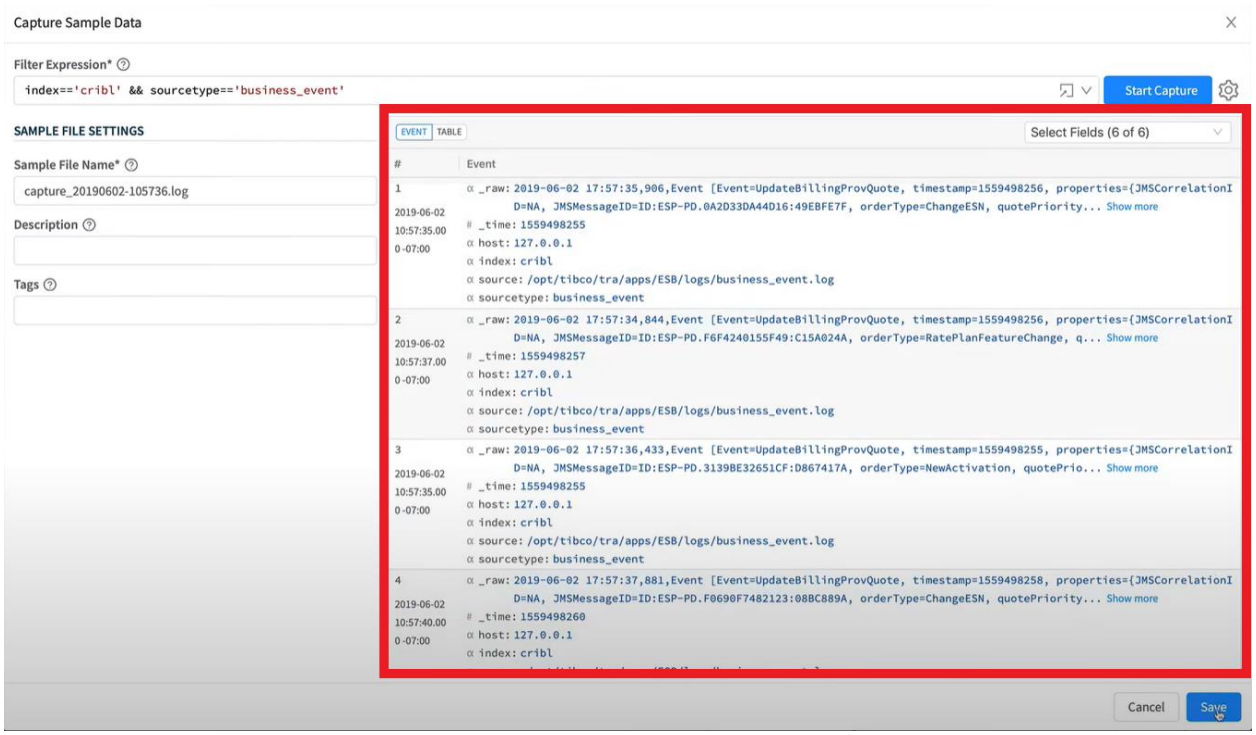
("Preview works by taking a set of sample events and passing them through the Pipeline, while displaying the inbound and outbound results in a separate pane."); *see also* Cribl Docs: Edge, "Data Preview," https://docs.cribl.io/edge/data-preview.



Cribl Docs: Stream, "Event Breakers," https://docs.cribl.io/stream/event-breakers (annotations added).

184. On information and belief, Cribl, through its Stream and Edge software, causes display of a preview of at least a portion of the set of searchable, timestamped events, in a manner that satisfies element [1d] of the '206 Patent.

185. For example, after the set of sample data has been parsed into the set of time-stamped events, Cribl, through its Stream and Edge software, displays the sample events in the Data Preview graphical user interface. *See, e.g.*, https://www.youtube.com/watch?v=hsfyafZ55Oo at 9:32.



https://www.youtube.com/watch?v=hsfyafZ55Oo at 9:32 (annotations added).

186. On information and belief, Cribl, through its Stream and Edge software, processes at least some raw data not in the selection, in response to user input, using the parsing rule corresponding to the match, in a manner that satisfies element [1e] of the '206 Patent.

187. For example, after the user has provided input that the user is satisfied with how the data appears in the Data Preview interface, Cribl applies the stored parsing rule found in the Event Breaker to the full raw data stream and parses new data—*i.e.*, data not in the collected sample—according to the stored parsing rule. *See, e.g.*, https://www.youtube.com/watch?v=hsfyafZ55Oo at 9:32; *see also*, *e.g.*, Cribl Docs: Stream, "Data Preview," https://docs.cribl.io/stream/data-preview ("Preview works by taking a set of sample events and passing them through the Pipeline, while displaying the inbound and outbound results in a separate pane. Any time a Function is modified, added, or removed, the Pipeline changes, and so does its displayed output.").

188. On information and belief, Cribl, through its Stream and Edge software, performs the method described in the '206 Patent using one or more computing devices, in a manner that satisfies element [1f] of the '206 Patent.

189. For example, Cribl installs Stream and Edge onto computing devices it controls in its Cribl.Cloud service, "where Cribl assumes responsibility for managing the infrastructure" of the Cribl.Cloud servers, and performs the patented method on said computing devices. Cribl Docs: Stream, "Cribl.Cloud Launch Guide," https://docs.cribl.io/stream/deploy-cloud ("This SaaS version, whether free or paid, places the Leader and the Edge Node in Cribl.Cloud, where Cribl assumes responsibility for managing the infrastructure."); *see also* Cribl Docs: Edge, "Cribl.Cloud Launch Guide," https://docs.cribl.io/edge/deploy-cloud. Furthermore, Cribl uses computers with its Stream and Edge software, as the software can only be operated after installation on a computing device. *See, e.g.*, Cribl Docs: Stream, "Deployment Types," https://docs.cribl.io/stream/deploy-types; Cribl Docs: Edge, "Deployment Planning," https://docs.cribl.io/edge/deploy-planning.

190. Cribl's infringement is literal, under the doctrine of equivalents, or both, and its infringement is also willful. The demonstration of Cribl's infringement of claim 1 of the '206 Patent, above, is exemplary and non-limiting.

191. Cribl had actual knowledge and constructive knowledge of the '443 Patent since as early as the issue date of the '206 Patent, as described earlier in Paragraphs 85–89 and 110–114 (which Splunk incorporates by reference here).

192. On information and belief, Cribl has been and is now indirectly infringing the '206 Patent in violation of 35 U.S.C. § 271(b) at least by instructing, encouraging, implementing, and/or directing others how to use Stream and Edge in ways that directly infringe the '206 Patent,

including claim 1, through its educational and promotional materials, support activities, as well as its service and consulting activities. Cribl has committed and continues to commit affirmative acts that cause infringement of one or more claims of the '206 Patent with knowledge of the '206 Patent and knowledge or willful blindness that the induced acts constitute infringement of one or more claims of the '206 Patent. By way of example, as set forth above, Cribl publishes on its website and on YouTube instructions that, when followed in conjunction with use of Cribl's Stream and Edge, infringe one or more claims of the '206 Patent.

193. On information and belief, Cribl contributes to the infringement of at least claim 1 of the '206 Patent by others, including its customers, distributors, and authorized resellers in violation of 35 U.S.C. § 271(c). Cribl has committed and continues to commit affirmative acts that contribute to the infringement by others, including, but not limited to, the sale, offer for sale, and/or import by Cribl of Stream and Edge in the United States, with knowledge of the '206 Patent and knowledge that Stream and Edge have no substantial non-infringing uses. Stream and Edge are especially made for or adapted for use to infringe, are not staple articles of commerce, and are not suitable for substantial non-infringing use. By way of example, Cribl sells Stream and Edge to customers who use Stream and Edge in an infringing manner, as set forth above. Cribl Data Preview is especially made for or adapted for use to infringe the '206 Patent because, on information and belief, Data Preview is designed to perform actions in response to the user interacting with the user interface, accept samples of data, and make data processing changes direct to the Pipelines that are processing data not in the sample entered into Data Preview.

194. Cribl will continue to infringe, induce infringement of, and contribute to infringement of the '206 Patent, causing irreparable harm to Splunk for which there is no adequate remedy at law, unless enjoined by this Court. Cribl's infringement has caused and continues to

cause irreparable harm to Splunk in the form of loss of business opportunities, lost sales, loss of market share, loss of goodwill, and the loss of Splunk's exclusive right to practice its inventions.

195. As a result of Cribl's willful infringement of the '206 Patent, Splunk has suffered damages and is owed no less than a reasonable royalty under 35 U.S.C. § 284 as a remedy. On information and belief, Cribl has known that its activities concerning Stream and Edge infringed one or more claims of the '206 Patent since at least March 2017.

196. On information and belief, Cribl has made no attempt to design around the claims of the '206 Patent.

197. On information and belief, Cribl does not have and has not had a reasonable basis for believing that the claims of the '206 Patent were invalid.

198. On information and belief, Cribl's Stream and Edge are available to businesses and individuals throughout the United States and in this judicial District. On information and belief, Cribl has committed acts of infringement in this District, including by inducing infringement within the State of Delaware.

COUNT IV: INFRINGEMENT OF THE '467 PATENT BY CRIBL

199. Splunk incorporates by reference as though fully set forth herein the allegations found in Paragraphs 1-198.

200. On information and belief, Cribl has been and is now directly infringing the '467 Patent in violation of 35 U.S.C. § 271(a) at least by making, using, selling, offering for sale, and/or importing into the United States, at least Stream and Edge, through which Cribl practices one or more claims of the '467 Patent, including at least claim 1.

201. Claim 1 recites (bracketed enumerations added):

> [1pre] A computer-implemented method of implementing a multi-tenant dual-queue system comprising:

> [1a] receiving, by a data service, live data associated with an entity;
>
> [1b] based on determining that a dual-queue node assigned to the entity is uninstantiated on the data service, dynamically instantiating the dual-queue node assigned to the entity, by initializing a live data queue and a stale data queue for the dual-queue node, wherein the initialized live data queue is enabled to receive the live data for processing and the initialized stale data queue is enabled to store a persistent backup of the live data; and
>
> [1c] routing the live data to the dual-queue node.

202. By way of non-limiting example, Cribl has infringed claim 1 of the '467 Patent by committing the following infringing acts without authorization, consent, permission or a license from Splunk.

203. On information and belief, Stream and Edge are substantially similar and are identical in all material aspects with regards to the subject matter of the '467 Patent and the other Patents-in-Suit, as discussed in Paragraph 124 above.

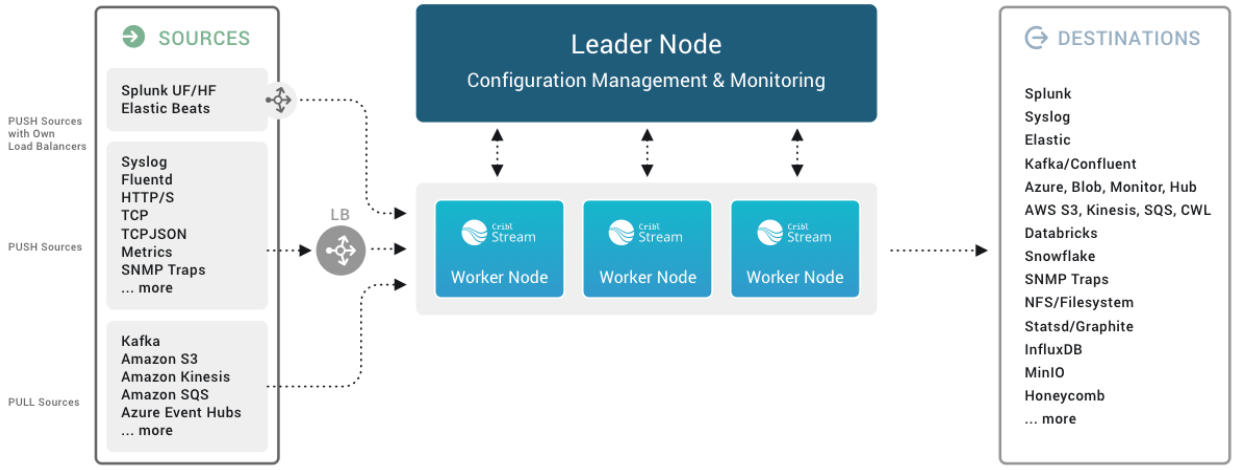
204. On information and belief, and to the extent the preamble is limiting, Cribl, through its Stream and Edge software, performs a computer-implemented method of implementing a multi-tenant dual-queue system, in a manner that satisfies element [1pre] of the '467 Patent.

205. For example, Cribl's Stream and Edge software is deployed on computers. *See, e.g.*, Cribl Docs: Stream, "Deployment Types," https://docs.cribl.io/stream/deploy-types; Cribl Docs: Stream, "Cribl.Cloud Launch Guide," https://docs.cribl.io/stream/deploy-cloud/; Cribl Docs: Edge, "Deployment Planning," https://docs.cribl.io/edge/deploy-planning. Further, Cribl implements a multi-tenant dual-queue system through Persistent Queues in Stream and Edge. *See, e.g.*, Cribl Docs: Stream, "Persistent Queues," https://docs.cribl.io/stream/persistent-queues; *see also* Cribl Docs: Edge, "Persistent Queues," https://docs.cribl.io/edge/persistent-queues. "Cribl Stream's persistent queuing (PQ) feature helps minimize data loss if a downstream receiver is

unreachable. PQ provides durability by writing data to disk for the duration of the outage, and forwarding it upon recovery. . . . an in-memory buffer helps [Stream] absorb temporary imbalances between inbound and outbound data rates. . . . Only when this buffer is full will [Stream] impose backpressure upstream [to the Persistent Queues]." *See, e.g.*, Cribl Docs: Stream, "Persistent Queues," https://docs.cribl.io/stream/persistent-queues; *see also* Cribl Docs: Edge, "Persistent Queues," https://docs.cribl.io/edge/persistent-queues.

206. On information and belief, Cribl, through its Stream and Edge software, receives live data associated with an entity using a data service, in a manner that satisfies element [1a] of the '467 Patent.

207. For example, Stream and Edge receive live data from connected sources. *See, e.g.*, Cribl Docs: Stream, "Basic Concepts," https://docs.cribl.io/stream/basic-concepts/; Cribl Docs: Edge, "Basic Concepts," https://docs.cribl.io/edge/basic-concepts.



Cribl Docs: Stream, "Basic Concepts," https://docs.cribl.io/stream/basic-concepts.

208. On information and belief, Cribl, through its Stream and Edge software, dynamically instantiates a dual-queue node by initializing a live data queue and a stale data queue for the dual-queue node, where the live data queue is enabled to receive the live data and the stale

data queue is enabled to store a persistent backup of the live data, in a manner that satisfies element [1b] of the '467 Patent.

209. For example, Stream and Edge, through a feature called Persistent Queues, dynamically instantiate dual-queue nodes in response to instructions enabling the feature. *See, e.g.*, Cribl Docs: Stream, "Persistent Queues," https://docs.cribl.io/stream/persistent-queues; *see also* Cribl Docs: Edge, "Persistent Queues," https://docs.cribl.io/edge/persistent-queues. The Persistent Queue option is selected in the user interface, and a Persistent Queue is assigned to an entity. *See, e.g.*, Cribl Docs: Stream, "Persistent Queues," https://docs.cribl.io/stream/persistent-queues; *see also* Cribl Docs: Edge, "Persistent Queues," https://docs.cribl.io/edge/persistent-queues.

210. After the feature is enabled and a Persistent Queue is assigned to the Node, an in-memory queue and a Persistent Queue are initialized. *See, e.g.*, Cribl Docs: Stream, "Persistent Queues," https://docs.cribl.io/stream/persistent-queues ("Persistent Queues Supplement In-Memory Queues"); *see also* Cribl Docs: Edge, "Persistent Queues," https://docs.cribl.io/edge/persistent-queues. The in-memory queue is configured to receive live data for processing, and is first to receive the data after the incoming data reaches the Node. *See, e.g.*, Cribl Docs: Stream, "Persistent Queues," https://docs.cribl.io/stream/persistent-queues; *see also* Cribl Docs: Edge, "Persistent Queues," https://docs.cribl.io/edge/persistent-queues. The Persistent Queue is configured to receive data and store it to disk instead of storing the data in memory, thus creating a persistent backup of the incoming data that is not lost if power to the Nodes is disabled or if Stream and Edge are reset or rebooted. *See, e.g.*, Cribl Docs: Stream, "Persistent Queues," https://docs.cribl.io/stream/persistent-queues ("PQ [Persistent Queues]

provide[] durability by writing data to disk . . . ."); *see also* Cribl Docs: Edge, "Persistent Queues," https://docs.cribl.io/edge/persistent-queues.

211. On information and belief, Cribl, through its Stream and Edge software, routes the live data to the dual-queue node, in a manner that satisfies element [1c] of the '467 Patent.

212. For example, as explained above, Stream and Edge first receive data through the standard data input track and feed data into the in-memory buffer before delivering data to the Persistent Queue. *See, e.g.*, Cribl Docs: Stream, "Persistent Queues," https://docs.cribl.io/stream/persistent-queues; *see also* Cribl Docs: Edge, "Persistent Queues," https://docs.cribl.io/edge/persistent-queues.

213. Cribl's infringement is literal, under the doctrine of equivalents, or both, and its infringement is also willful. The demonstration of Cribl's infringement of claim 1 of the '467 Patent, above, is exemplary and non-limiting.

214. Cribl had actual knowledge and constructive knowledge of the '443 Patent since as early as the issue date of the '467 Patent, as described earlier in Paragraphs 85–89 and 110–114 (which Splunk incorporates by reference here).

215. On information and belief, Cribl has been and is now indirectly infringing the '467 Patent in violation of 35 U.S.C. § 271(b) at least by instructing, encouraging, implementing, and/or directing others how to use Stream and Edge in ways that directly infringe the '467 Patent, including claim 1, through its educational and promotional materials, support activities, as well as its service and consulting activities. Cribl has committed and continues to commit affirmative acts that cause infringement of one or more claims of the '467 Patent with knowledge of the '467 Patent and knowledge or willful blindness that the induced acts constitute infringement of one or more claims of the '467 Patent. By way of example, as set forth above, Cribl publishes on its website

and on YouTube instructions that, when followed in conjunction with use of Cribl's Stream and Edge, infringe one or more claims of the '467 Patent.

216. On information and belief, Cribl contributes to the infringement of at least claim 1 of the '467 Patent by others, including its customers, distributors, and authorized resellers in violation of 35 U.S.C. § 271(c). Cribl has committed and continues to commit affirmative acts that contribute to the infringement by others, including, but not limited to, the sale, offer for sale, and/or import by Cribl of Stream and Edge in the United States, with knowledge of the '467 Patent and knowledge that Stream and Edge have no substantial non-infringing uses. Stream and Edge are especially made for or adapted for use to infringe, are not staple articles of commerce, and are not suitable for substantial non-infringing use. By way of example, Cribl sells Stream and Edge to customers who use Stream and Edge in an infringing manner, as set forth above. Cribl Persistent Queues are especially made for or adapted for use to infringe the '467 Patent because, on information and belief, Persistent Queues are designed to receive data after data is received at the in-memory queue and designed to receive data as a backup to the in-memory queue.

217. Cribl will continue to infringe, induce infringement of, and contribute to infringement of the '467 Patent, causing irreparable harm to Splunk for which there is no adequate remedy at law, unless enjoined by this Court. Cribl's infringement has caused and continues to cause irreparable harm to Splunk in the form of loss of business opportunities, lost sales, loss of market share, loss of goodwill, and the loss of Splunk's exclusive right to practice its inventions.

218. As a result of Cribl's willful infringement of the '467 Patent, Splunk has suffered damages and is owed no less than a reasonable royalty under 35 U.S.C. § 284 as a remedy. On information and belief, Cribl has known that its activities concerning Stream and Edge infringed one or more claims of the '467 Patent since at least December 2017.

219. On information and belief, Cribl has made no attempt to design around the claims of the ’467 Patent.

220. On information and belief, Cribl does not have and has not had a reasonable basis for believing that the claims of the ’467 Patent were invalid.

221. On information and belief, Cribl’s Stream and Edge are available to businesses and individuals throughout the United States and in this judicial District. On information and belief, Cribl has committed acts of infringement in this District, including by inducing infringement within the State of Delaware.

COUNT V: INFRINGEMENT OF THE ’312 PATENT BY CRIBL

222. Splunk incorporates by reference as though fully set forth herein the allegations found in Paragraphs 1-221.

223. On information and belief, Cribl has been and is now directly infringing the ’312 Patent in violation of 35 U.S.C. § 271(a) at least by making, using, selling, offering for sale, and/or importing into the United States, at least Stream and Edge, through which Cribl practices one or more claims of the ’312 Patent, including at least claim 1.

224. Claim 1 recites (bracketed enumerations added):

> [1pre] A method for improving machine data analysis, comprising:
>
> > [1a] creating a set of searchable events by segmenting raw time series machine data received from at least one data source in an information technology environment into searchable events, the raw time series machine data reflecting activity in the information technology environment, each searchable event including at least a portion of the segmented raw time series machine data thereby allowing application of time-based search phrases across at least a portion of events in the set of searchable events to search the segmented raw time series machine data in the at least a portion of the events;

> [1b] detecting whether time information is present in the raw time series machine data of an event in the set of searchable events;
>
> [1c] in response to detecting that the time information is present in the event:
>
> extracting the time information from the raw time series machine data of the event;
>
> [1d] determining a time zone in the extracted time information;
>
> [1e] generating an offset by normalizing the extracted time information using the determined time zone;
>
> [1f] generating a time stamp based on the offset; and
>
> [1g] associating the generated time stamp with the event, thereby enabling the event to be searched using the generated time stamp;
>
> [1h] in response to detecting that the time information is not present in the event:
>
> calculating a time stamp for the event using one or more stored time stamps, wherein the one or more stored time stamps are time stamps stored from one or more earlier processed events selected on a periodic basis in order to facilitate time stamp creation; and
>
> [1i] associating the calculated time stamp with the event, thereby enabling the event to be searched using the created time stamp;
>
> [1j] wherein the method is performed by one or more computing devices.

225. By way of non-limiting example, Cribl has infringed claim 1 of the ’312 Patent by committing the following infringing acts without authorization, consent, permission or a license from Splunk.

226. On information and belief, Stream and Edge are substantially similar and are identical in all material aspects with regards to the subject matter of the '312 Patent and the other Patents-in-Suit, as discussed in Paragraph 124 above.

227. On information and belief, and to the extent the preamble is limiting, Cribl, through its Stream and Edge software, performs a method for improving machine data analysis, in a manner that satisfies element [1pre] of the '312 Patent.

228. For example, Cribl states that Stream and Edge use methods to improve machine data analysis. *See, e.g.*, Cribl Docs: Stream, "About Cribl Stream," https://docs.cribl.io/stream/about ("Cribl Stream helps you process data – logs, instrumentation data, application data, metrics, etc. – in real time, and deliver them to your analysis platform of choice."; Cribl Docs: Edge, "About Cribl Edge," https://docs.cribl.io/edge/about ("Cribl Edge helps you collect and process observability data – logs, metrics, application data, etc. – in real time, from you Linux machines, apps, microservices etc., and deliver them to Cribl Stream or any supported destination."

229. On information and belief, Cribl, through its Stream and Edge software, creates a set of searchable events by segmenting raw time series machine data received from at least one data source in an information technology environment into searchable events, the raw time series machine data reflecting activity in the information technology environment, each searchable event including at least a portion of the segmented raw time series machine data thereby allowing application of time-based search phrases across at least a portion of events in the set of searchable events to search the segmented raw time series machine data in the at least a portion of the events, in a manner that satisfies element [1a] of the '312 Patent.

230. For example, as described earlier, Cribl invokes Event Breakers to "help break incoming streams of data into discrete events." Cribl Docs: Stream, "Event Breakers," https://docs.cribl.io/stream/event-breakers; *see also* Cribl Docs: Edge, "Event Breakers," https://docs.crib.io/edge/event-breakers. Event Breakers intake raw time series machine data and apply breaker rules to incoming data to segment the data into events. Cribl Docs: Stream, "Event Breakers," https://docs.cribl.io/stream/event-breakers ("Rulesets are collections of Event Breaker rules . . . . Rules define configurations needed to break down a stream of data into events."); *see also* Cribl Docs: Edge, "Event Breakers," https://docs.cribl.io/edge/event-breakers. Cribl configures Event Breakers to apply time-based search phrases, including by applying regular-expression-based rules or by searching for an existing timestamp. *E.g.*, Cribl Docs: Stream, "Event Breakers," https://docs.cribl.io/stream/event-breakers ("You can use the Timestamp breaker to break events at the beginning of any line in which Cribl Stream finds a timestamp."); *see also* Cribl Docs: Edge, "Event Breakers," https://docs.cribl.io/edge/event-breakers. The generated events include portions of raw data segmented by the Event Breaker.

231. On information and belief, Cribl, through its Stream and Edge software, detects whether time information is present in the raw time series machine data of an event in the set of searchable events, in a manner that satisfies element [1b] of the '312 Patent.

232. For example, Event Breakers perform timestamping on machine data, first by detecting time information already present in the data that has been synthesized into events. Cribl Docs: Stream, "Event Breakers," https://docs.cribl.io/stream/event-breakers ("After events are synthesized out of streams, Cribl Stream will attempt timestamping. First, a timestamp anchor will be located inside the event. Next, starting there, the engine will try to do one of the following: . . . Scan up to a configurable depth into the event and autotimestamp . . . ."); *see also* Cribl Docs:

Edge, "Event Breakers," https://docs.cribl.io/edge/event-breakers. The Event Breaker "scan[s] up to a configurable depth into the event" and searches for time information. *See* Cribl Docs: Stream, "Event Breakers," https://docs.cribl.io/stream/event-breakers ("This timestamping executes the same basic algorithm as the Auto Timestamp Function and the C.Time.timestampFinder() native method."); Cribl Docs: Stream, "Auto Timestamp," https://docs.cribl.io/stream/auto-timestamp-function ("By default, Cribl Stream will inspect the first 150 characters [of an event], and will extract the first valid timestamp it sees."); *see also* Cribl Docs: Edge, "Event Breakers," https://docs.cribl.io/edge/event-breakers.

233. On information and belief, Cribl, through its Stream and Edge software, extracts the time information from the raw time series machine data of the event in response to detecting that the time information is present in the event, in a manner that satisfies element [1c] of the '312 Patent.

234. For example, after time information has been detected, the Event Breaker extracts that time information. *See* Cribl Docs: Stream, "Event Breakers," https://docs.cribl.io/stream/event-breakers ("This timestamping [the autotimestamping performed by an Event Breaker] executes the same basic algorithm as the Auto Timestamp Function and the C.Time.timestampFinder() native method."); Cribl Docs: Stream, "Auto Timestamp," https://docs.cribl.io/stream/auto-timestamp-function ("By default, Cribl Stream will inspect the first 150 characters [of an event], and *will extract the first valid timestamp it sees*." (emphasis added)); *see also* Cribl Docs: Edge, "Event Breakers," https://docs.cribl.io/edge/event-breakers.

235. On information and belief, Cribl, through its Stream and Edge software, determines a time zone in the extracted time zone information, in a manner that satisfies element [1d] of the '312 Patent.

236. For example, when performing the scan of the events for time information, the Event Breaker searches for a time zone. *See, e.g.*, Cribl Docs: Stream, "Auto Timestamp," https://docs.cribl.io/stream/auto-timestamp-function ("%Z - time zone offset, such as -0700, -07:00, -07, or Z."; specifying configuration of search function to extract time zone information); Cribl Docs: Edge, "Auto Timestamp," https://docs.cribl.io/edge/auto-timestamp-function.

237. On information and belief, Cribl, through its Stream and Edge software, generates an offset by normalizing the extracted time information using the determined time zone, in a manner that satisfies element [1e] of the '312 Patent.

238. For example, the Event Breaker applies the determined time zone to extracted time information, and generates a time zone offset based on that determined time zone. *See* Cribl Docs: Stream, "Auto Timestamp," https://docs.cribl.io/stream/auto-timestamp-function:

"Cribl Stream will grab the first part of the event, and will settle on the first matching value to display for time:

- _time 1569006235
- GMT: Friday, 20 September 2019, 7:03:55 PM GMT
- Your Local Time: Friday, 20 September 2019 PDT, 12:03:55 AM *GMT -07:00*"

See also Cribl Docs: Edge, "Auto Timestamp," https://docs.cribl.io/edge/auto-timestamp-function.

239. On information and belief, Cribl, through its Stream and Edge software, generates a time stamp based on the generated offset, in a manner that satisfies element [1f] of the '312 Patent.

240. For example, after the offset has been generated, the Event Breaker applies the timestamp to the event. *See, e.g.*, Cribl Docs: Stream, "Event Breakers,"

https://docs.cribl.io/event-breakers ("After events are synthesized out of streams, Cribl Stream will attempt timestamping. First, a timestamp anchor will be located inside the event. Next, starting there, the engine will try to do one of the following: . . . scan up to a configurable depth into the event and autotimestamp, or . . . timestamp the event with the current time."); *see also* Cribl Docs: Edge, "Event Breakers," https://docs.cribl.io/edge/event-breakers.

241. On information and belief, Cribl, through its Stream and Edge software, associates the generated time stamp with the event, thereby enabling the event to be searched using the generated time stamp, in a manner that satisfies element [1g] of the '312 Patent.

242. For example, once the timestamp has been applied, the timestamp is associated with the event. *See, e.g.*, Cribl Docs: Stream, "Event Breakers," https://docs.cribl.io/stream/event-breakers.

243. On information and belief, Cribl, through its Stream and Edge software, in response to detecting that the time information is not present in the event, calculates a time stamp for the event using one or more stored time stamps, wherein the one or more stored time stamps are time stamps stored from one or more earlier processed events selected on a periodic basis in order to facilitate time stamp creation, in a manner that satisfies element [1h] of the '312 Patent.

244. For example, the Event Breaker, when it fails to extract time information from an event, calculates a timestamp from events previously processed by the Event Breaker by calculating a time offset based on the previously stored timestamps:

> Notice how only the first line [in the working dataset] has a full timestamp, all other lines have offsets off of that. To properly assign accurate timestamp to events that follow Event 1 (Line 1) we have to use a cool property of Auto Timestamp (use Last Event's Time) and then two other functions, namely Regex Extract and Eval. . . . Configure Auto Timestamp to use Last Event's Time if it can't extract a valid timestamp. This effectively means that all events will "inherit" Event 1's time. Use Regex Extract to extract the offset of all events, except for Event 1. . . . Use Eval to add the offset to the _time field of each event.

Dritan Bitincka, "Extracting Timestamps from Messy Logs," CRIBL BLOG, https://cribl.io/blog/extracting-timestamps-from-messy-logs/ (describing use of the Auto Timestamp function, which operates the same way as the timestamping performed by the Event Breaker, as described earlier). Thus, the Event Breaker determines that the event lacks time information, takes a previous timestamp, calculates a new timestamp for the event based on the previously saved timestamp, and associates the new calculated timestamp with the event.

245. On information and belief, Cribl, through its Stream and Edge software, associates the calculated time stamp with the event, thereby enabling the event to be searched using the created time stamp, in a manner that satisfies element [1i] of the '312 Patent.

246. For example, after the timestamp has been applied, the timestamp is associated with the event. *See, e.g.*, Cribl Docs: Stream, "Event Breakers," https://docs.cribl.io/stream/event-breakers.

247. On information and belief, Cribl, through its Stream and Edge software, performs the method using one or more computing devices, in a manner that satisfies element [1j] of the '312 Patent.

248. For example, Cribl installs Stream and Edge onto computing devices it controls in its Cribl.Cloud service, "where Cribl assumes responsibility for managing the infrastructure" of the Cribl.Cloud servers, and performs the patented method on said computing devices. Cribl Docs: Stream, "Cribl.Cloud Launch Guide," https://docs.cribl.io/stream/deploy-cloud ("This SaaS version, whether free or paid, places the Leader and the Edge Node in Cribl.Cloud, *where Cribl assumes responsibility for managing the infrastructure*." (emphasis added)); *see also* Cribl Docs: Edge, "Cribl.Cloud Launch Guide," https://docs.cribl.io/edge/deploy-cloud. Furthermore, Cribl uses computers with its Stream and Edge software, as the software can only be operated after

installation on a computing device. *See, e.g.*, Cribl Docs: Stream, "Deployment Types," https://docs.cribl.io/stream/deploy-types; Cribl Docs: Edge, "Deployment Planning," https://docs.cribl.io/edge/deploy-planning.

249. Cribl's infringement is literal, under the doctrine of equivalents, or both, and its infringement is also willful. The demonstration of Cribl's infringement of claim 1 of the '312 Patent, above, is exemplary and non-limiting.

250. Cribl had actual knowledge and constructive knowledge of the '312 Patent since as early as the issue date of the '312 Patent, as described earlier in Paragraphs 85–89 and 110–114 (which Splunk incorporates by reference here).

251. On information and belief, Cribl has been and is now indirectly infringing the '312 Patent in violation of 35 U.S.C. § 271(b) at least by instructing, encouraging, implementing, and/or directing others how to use Stream and Edge in ways that directly infringe the '312 Patent, including claim 1, through its educational and promotional materials, support activities, as well as its service and consulting activities. Cribl has committed and continues to commit affirmative acts that cause infringement of one or more claims of the '312 Patent with knowledge of the '312 Patent and knowledge or willful blindness that the induced acts constitute infringement of one or more claims of the '312 Patent. By way of example, as set forth above, Cribl publishes on its website and on YouTube instructions that, when followed in conjunction with use of Cribl's Stream and Edge, infringe one or more claims of the '312 Patent.

252. On information and belief, Cribl contributes to the infringement of at least claim 1 of the '312 Patent by others, including its customers, distributors, and authorized resellers in violation of 35 U.S.C. § 271(c). Cribl has committed and continues to commit affirmative acts that contribute to the infringement by others, including, but not limited to, the sale, offer for sale, and/or

import by Cribl of Stream and Edge in the United States, with knowledge of the '312 Patent and knowledge that Stream and Edge have no substantial non-infringing uses. Stream and Edge are especially made for or adapted for use to infringe, are not staple articles of commerce, and are not suitable for substantial non-infringing use. By way of example, Cribl sells Stream and Edge to customers who use Stream and Edge in an infringing manner, as set forth above. Cribl Event Breakers are especially made for or adapted for use to infringe the '312 Patent because, on information and belief, Event Breakers are designed to generate timestamped event streams from raw data with time zone information incorporated into the event stream.

253. Cribl will continue to infringe, induce infringement of, and contribute to infringement of the '312 Patent, causing irreparable harm to Splunk for which there is no adequate remedy at law, unless enjoined by this Court. Cribl's infringement has caused and continues to cause irreparable harm to Splunk in the form of loss of business opportunities, lost sales, loss of market share, loss of goodwill, and the loss of Splunk's exclusive right to practice its inventions.

254. As a result of Cribl's willful infringement of the '312 Patent, Splunk has suffered damages and is owed no less than a reasonable royalty under 35 U.S.C. § 284 as a remedy. On information and belief, Cribl has known that its activities concerning Stream and Edge infringed one or more claims of the '312 Patent since at least April 2019.

255. On information and belief, Cribl has made no attempt to design around the claims of the '312 Patent.

256. On information and belief, Cribl does not have and has not had a reasonable basis for believing that the claims of the '312 Patent were invalid.

257. On information and belief, Cribl's Stream and Edge are available to businesses and individuals throughout the United States and in this judicial District. On information and belief,

Cribl has committed acts of infringement in this District, including by inducing infringement within the State of Delaware.

COUNT VI: COPYRIGHT INFRINGEMENT PURSUANT TO 17 U.S.C. § 501, *ET SEQ.* (S2S SOURCE CODE) BY CRIBL AND CLINT SHARP

258. Splunk incorporates by reference as though fully set forth herein the allegations found in Paragraphs 1-257.

259. Splunk is the owner of all exclusive and substantial rights and privileges in the U.S. Copyright Registrations set forth above in Paragraphs 21 and 35. True and correct copies of the corresponding copyright registration certificates are attached hereto as Exhibit A.

260. As described above, Clint Sharp and Cribl copied Splunk's copyrighted material and/or substantial portions of Splunk's copyrighted material.

261. For example, Clint Sharp copied Splunk's copyrighted source code for S2S, created a derivative of that code (go-S2S), and posted it online.

262. On information and belief, Mr. Sharp encouraged and induced Cribl to copy this derivative of Splunk's copyrighted S2S code into the source code for Cribl's software, including at least Stream and Edge. On information and belief, Mr. Sharp did so with knowledge that go-S2S was an unlicensed derivative of Splunk's copyrighted S2S source code. On information and belief, each new version of Cribl's Stream and Edge software has included copies of this unlicensed derivative of Splunk's copyrighted S2S source code, and/or further derivatives thereof.

263. When Cribl's Stream and Edge software are executed, further unlicensed copies of Splunk's copyrighted S2S source code are created.

264. Accordingly, Mr. Sharp and Cribl have infringed and contributed to the infringement of Splunk's copyright in its S2S source code.

265. Mr. Sharp's and Cribl's infringement related to the S2S source code includes, at least:

a. Direct and contributory infringement of Splunk's exclusive right to reproduce its copyrighted works pursuant to 17 U.S.C. § 106(1);

b. Direct and contributory infringement of Splunk's exclusive right to prepare derivative works based on copyrighted works pursuant to 17 U.S.C. § 106(2);

c. Direct and contributory infringement of Splunk's exclusive right to distribute copies of its copyrighted works pursuant to 17 U.S.C. § 106(3).

266. Mr. Sharp's and Cribl's infringement was and continues to be willful and intentional.

267. Mr. Sharp and Cribl will continue to infringe and contribute to infringement of Splunk's copyright in its S2S source code and derivatives thereof, causing irreparable harm to Splunk for which there is no adequate remedy at law, unless enjoined by this Court. Mr. Sharp's and Cribl's infringement has caused and continues to cause irreparable harm to Splunk in the form of loss of business opportunities, lost sales, loss of market share, loss of goodwill, and the loss of Splunk's exclusive rights to reproduce its copyrighted works, prepare derivative works based on its copyrighted works, and distribute copies of its copyrighted works.

COUNT VII: COPYRIGHT INFRINGEMENT PURSUANT TO 17 U.S.C. § 501, *ET SEQ.* (SPLUNK ENTERPRISE) BY CRIBL

268. Splunk incorporates by reference as though fully set forth herein the allegations found in Paragraphs 1-267.

269. Splunk is the owner of all exclusive and substantial rights and privileges in the U.S. Copyright Registrations set forth above in Paragraph 21. True and correct copies of the corresponding copyright registration certificates are attached hereto as Exhibit A.

270. The only license that permitted Cribl to use Splunk Enterprise software for commercial software development and distribution is the TAP Agreement, which was terminated at least as of November 2, 2021.

271. As described above, Cribl makes and has made unlicensed copies of the copyrighted Splunk Enterprise software, which constitutes an infringement of Splunk's copyright in the Splunk Enterprise software.

272. For example, on information and belief, Cribl executes Splunk Enterprise in order to develop its software, including Stream and Edge, both of which extend the features and functionality of Splunk Enterprise, despite having no license to do so. Every time Cribl executes Splunk Enterprise in connection with the development of its software, it makes an unlicensed copy of Splunk Enterprise.

273. By way of further example, Cribl executes Splunk Enterprise in order to market its Stream and Edge software. Every time Cribl executes Splunk Enterprise to market its own software, it makes an unlicensed copy of Splunk Enterprise.

274. Cribl's infringement related to the Splunk Enterprise software includes at least direct infringement of Splunk's exclusive right to reproduce its copyrighted works pursuant to 17 U.S.C. § 106(1).

275. Cribl's infringement was and continues to be willful and intentional.

276. Cribl will continue to infringe Splunk's copyrights in Splunk Enterprise, causing irreparable harm to Splunk for which there is no adequate remedy at law, unless enjoined by this Court. Cribl's infringement has caused and continues to cause irreparable harm to Splunk in the form of loss of business opportunities, lost sales, loss of market share, loss of goodwill, and the loss of Splunk's exclusive right to reproduce its copyrighted works.

COUNT VIII: VIOLATION OF THE DIGITAL MILLENNIUM COPYRIGHT ACT PURSUANT TO 17 U.S.C. § 1202 (COPYRIGHT MANAGEMENT INFORMATION) BY CLINT SHARP

277. Splunk incorporates by reference as though fully set forth herein the allegations found in Paragraphs 1-276.

278. Clint Sharp violated the Digital Millennium Copyright Act ("DMCA") by knowingly providing and distributing copyright management information ("CMI") that is false, with the intent to induce, enable, facilitate, or conceal copyright infringement, in violation of 17 U.S.C. § 1202(a)(1)-(2).

279. Clint Sharp violated the DMCA by, without the authority of Splunk, intentionally removing or altering CMI and distributing Splunk source code and Splunk-derived source code with removed or altered CMI, knowing that it had been removed or altered without the authority of Splunk, and knowing or having reasonable grounds to know that it would induce, enable, facilitate, or conceal an infringement, in violation of 17 U.S.C. § 1202(b)(1)-(3).

280. As noted above, the copied S2S source code is protected by the U.S. Copyright Registrations set forth above in Paragraphs 21 and 35, including at least TXu 2-335-442.

281. As described above, Clint Sharp created the go-S2S source code by copying copyrighted Splunk source code, which contained Splunk copyright headers indicating authorship and ownership information reflecting Splunk's copyright in this code. Mr. Sharp's derivative go-S2S code, however, did not include headers indicating Splunk's authorship and ownership of the copyright in the go-S2S code; Mr. Sharp therefore provided false CMI and intentionally removed or altered CMI in creating the go-S2S code, without the authority of Splunk.

282. Mr. Sharp distributed code containing false, removed, and altered CMI for the entire duration of time that he maintained the go-S2S source code repository online, and at least

until December 2021. Any time Mr. Sharp's go-S2S source code repository was accessed, Mr. Sharp distributed code containing this false, removed, and altered CMI.

283. Mr. Sharp also provided and distributed code containing false CMI by uploading an open-source MIT license to the go-S2S github repository, falsely identifying Mr. Sharp as the author and/or owner of the copyright in the go-S2S code, and falsely providing open-source terms for use of the go-S2S code, despite its derivation from Splunk's source code.

284. Mr. Sharp distributed code containing this false CMI from December 2018 at least until December 2021. Any time Mr. Sharp's go-S2S source code repository was accessed, Mr. Sharp distributed code containing this false, removed, and altered CMI.

285. On information and belief, Mr. Sharp knowingly and intentionally removed or altered the CMI and knowingly and intentionally provided and distributed code containing false CMI, knowing that the CMI was removed or altered without the authority of Splunk, and knowing and intending to induce, enable, facilitate, or conceal copyright infringement, including at Cribl.

286. Mr. Sharp will continue to violate the DMCA, causing irreparable harm to Splunk for which there is no adequate remedy at law, unless enjoined by this Court. Mr. Sharp's violations of the DMCA have caused and continue to cause irreparable harm to Splunk in the form of loss of business opportunities, lost sales, loss of market share, and loss of goodwill.

COUNT IX: VIOLATION OF THE DIGITAL MILLENNIUM COPYRIGHT ACT PURSUANT TO 17 U.S.C. § 1201 (ANTI-CIRCUMVENTION) BY CRIBL

287. Splunk incorporates by reference as though fully set forth herein the allegations found in Paragraphs 1-286.

288. Cribl's actions, as described above, constitute direct circumvention of technical protection measures in the Splunk Enterprise software that effectively control access to a copyrighted work (Splunk Enterprise), in violation of 17 U.S.C. § 1201(a)(1) and (2). Cribl

manufactures, offers to the public, provides, and otherwise traffics in software and information—such as Stream and Edge and related documentation—that it markets and provides for use in circumventing these technological measures. 17 U.S.C. § 1201(a)(2)(C).

289. As noted above, Splunk Enterprise is protected by at least the U.S. Copyright Registrations set forth in Paragraph 21.

290. Splunk employs at least two separate technical protection measures to effectively control access to Splunk Enterprise.

291. As a first example, Splunk Enterprise refuses access to client software that attempts to communicate via the S2S protocol and is unable to authenticate itself with a special code phrase that is not documented.

292. As a second example, Splunk Enterprise controls access to Splunk Enterprise instances based on a client's possession of encrypted certificates that establish identity and authorization to access a given Splunk Enterprise instance.

293. Cribl has developed its software to circumvent these technical protection measures in order to access Splunk Enterprise.

294. For example, Cribl obtained Splunk's code phrase and added it to its software, such that Cribl's software can access a Splunk Enterprise instance via the S2S protocol, circumventing Splunk Enterprise's authentication mechanism related to this code phrase.

295. By way of further example, Cribl obtains credential information from Splunk TLS certificates and uses that information to access Splunk Enterprise instances so that Cribl's software can access a Splunk Enterprise instance, circumventing Splunk Enterprise's authentication mechanism related to encrypted certificates.

296. Cribl markets and provides its software for use in circumventing these technical protection measures. For example, Cribl markets its software's ability to "speak… S2S," *see* Exhibit C (https://cribl.io/blog/3-ways-logstream-can-improve-your-data-agility/), and to authenticate via Splunk certificates. *See* Exhibit G (https://docs.cribl.io/stream/usecase-splunk-cloud-integrations/).

297. Cribl will continue to violate the DMCA, causing irreparable harm to Splunk for which there is no adequate remedy at law, unless enjoined by this Court. Cribl's violations of the DMCA have caused and continue to cause irreparable harm to Splunk in the form of loss of business opportunities, lost sales, loss of market share, and loss of goodwill.

COUNT X: BREACH OF CONTRACT BY CRIBL

298. Splunk incorporates by reference as though fully set forth herein the allegations found in Paragraphs 1-297.

299. On or about August 6, 2018, Splunk and Cribl executed a TAP Agreement, attached hereto as Exhibit B.

300. The TAP Agreement formed a valid contract in exchange for consideration, including the mutual commitments made by Splunk and Cribl to each other, and actions that Splunk and Cribl took, including Splunk's provision of software and other licenses to Cribl, and Cribl's agreement to be bound by the terms of the TAP Agreement. Splunk complied with its obligations and the conditions of this contract with Cribl.

301. The TAP Agreement explicitly prohibits certain activity. For example, TAP partners have no right to: "(a) copy any Splunk Software (except as required to run the Splunk Software and for reasonable backup purposes); (b) modify, adapt, or create derivative works of the Splunk Software; . . . (d) decompile, disassemble or reverse engineer the Splunk Software, or determine or attempt to determine any source code, algorithms, methods or techniques embodied

in the Splunk Software, except to the extent expressly permitted by applicable law notwithstanding a contractual prohibition to the contrary; . . . [or] (f) attempt to disable or circumvent any license key or other technological mechanisms or measures intended to prevent, limit or control use or copying of, or access to, any materials included in the Splunk Software." Exhibit B at Section 4.

302. Any use of the Splunk Software that is not in accordance with the TAP Agreement is expressly prohibited. Exhibit B at Section 4(h).

303. As described above, on information and belief, Cribl materially breached the TAP Agreement by engaging in wrongful conduct, including without limitation reverse engineering Splunk Enterprise software in violation of Section 4(d) of the TAP Agreement in an attempt to determine source code, algorithms, methods or techniques embodied in that software, *e.g.*, those related to the S2S protocol.

304. Cribl also breached the TAP Agreement by, on information and belief, developing derivative works of Splunk Enterprise in violation of Section 4(b) of the TAP Agreement, and by circumventing technological mechanisms and measures intended to limit and control access to Splunk Enterprise in violation of Section 4(f).

305. Remedies at law are not adequate to fully compensate Splunk for the irreparable injuries that Splunk has suffered as a direct and proximate result of Cribl's breaches of the TAP Agreement, which have permitted Cribl to develop and market software that competes with Splunk's software, and whose sales have led and will lead to the erosion of Splunk's market and revenue. Accordingly, Splunk seeks an injunction to prevent Cribl's improper and unauthorized use of Splunk Enterprise and any other Splunk software.

COUNT XI: TORTIOUS INTERFERENCE WITH PROSPECTIVE BUSINESS RELATIONS UNDER DELAWARE LAW BY CRIBL

306. Splunk incorporates by reference as though fully set forth herein the allegations found in Paragraphs 1-305.

307. Splunk has and had an expectancy in continuing and advantageous economic relationships with purchasers and licensees of Splunk Enterprise and other Splunk software.

308. These relationships had the probability of future economic benefit in the form of profitable software licenses. Had Cribl refrained from engaging in the unlawful and wrongful conduct described herein, there is a reasonable probability that customers of Splunk Enterprise and other Splunk software would have initiated or expanded their contracts and licenses with Splunk.

309. Cribl was aware of these expectancies and intentionally interfered with them by conduct that was wrongful beyond the fact of the interference itself, including, for example, by: (a) targeting and obtaining the business of customers with whom Splunk is or was engaged in business, including by misleading customers regarding Cribl's Splunk-related functionality (including its ability to "speak S2S"), which Cribl did not disclose was derived from Cribl's widespread unlawful and unfair practices regarding misappropriated Splunk confidential documents, infringement of Splunk's copyrights, and circumvention of Splunk's technological protection measures; (b) targeting and obtaining the business of customers based on its use of misappropriated confidential Splunk business and customer information; (c) targeting Splunk's former employees for hiring using misappropriated Splunk confidential documents and information, and encouraging Splunk employees to provide Cribl with confidential Splunk documents and information; and (d) using misappropriated Splunk documents and information for competitive advantage with respect to Cribl's sales efforts and technology development efforts. Cribl's misappropriation of Splunk's confidential business information was part of a persistent

campaign of unfair competition by Cribl that involved systematic, concerted, and unlawful efforts to move business and technology from Splunk to Cribl by using Splunk's information and documents about its personnel, customers, sales, and technology.

310. As a direct and proximate result of Cribl's actions, the above-described expectancies have been actually disrupted.

311. As a direct and proximate result of Cribl's actions, Splunk has suffered damages, including without limitation loss of revenue or licenses that Splunk would have obtained but for Cribl's acts, reputational damage with its customers, loss of business relationships, and loss of goodwill. Splunk has suffered irreparable injury as a result of Cribl's tortious interference because some or all of these damages are not monetarily quantifiable.

COUNT XII: UNFAIR COMPETITION UNDER DELAWARE LAW BY CRIBL

312. Splunk incorporates by reference as though fully set forth herein the allegations found in Paragraphs 1-311.

313. Cribl has engaged in unfair and/or wrongful business acts or practices in its competition with Splunk, including, for example by: (a) targeting and obtaining the business of customers with whom Splunk is or was engaged in business, including by misleading customers regarding Cribl's Splunk-related functionality (including its ability to "speak S2S"), which Cribl did not disclose was derived from Cribl's widespread unlawful and unfair practices regarding misappropriated Splunk confidential documents, infringement of Splunk's copyrights, and circumvention of Splunk's technological protection measures; (b) targeting and obtaining the business of customers based on its use of misappropriated confidential Splunk business and customer information; (c) targeting Splunk's former employees for hiring using misappropriated Splunk confidential documents and information, and encouraging Splunk employees to provide Cribl with confidential Splunk documents and information; and (d) using misappropriated Splunk

documents and information for competitive advantage with respect to Cribl's sales efforts and technology development efforts. Cribl's misappropriation of Splunk's confidential business information was part of a persistent campaign of unfair competition by Cribl that involved systematic, concerted, and unlawful efforts to move business and technology from Splunk to Cribl by using Splunk's information and documents about its personnel, customers, sales, and technology.

314. Cribl committed these unfair and/or wrongful business acts or practices in an effort to gain unfair competitive advantage over Splunk in competing for current and prospective licensees of Splunk's Enterprise software, in competing for employees, and in its attempt to develop software competitive with Splunk's offerings. Cribl's actions interfered with Splunk's reasonable expectancy of entering into valid business relationships with customers and with employees.

315. As a direct and proximate result of the aforementioned acts, Splunk has suffered injury in fact, including without limitation loss of revenue or licenses that Splunk would have obtained but for Cribl's acts, reputational damage with its customers as well as potential and actual employees, loss of business relationships, and loss of goodwill. Splunk has suffered irreparable injury as a result of Cribl's unfair competition because some or all of these damages are not monetarily quantifiable.

PRAYER FOR RELIEF

WHEREFORE, Splunk respectfully requests the following relief:

(a) judgment in Splunk's favor and against Cribl and Clint Sharp on all causes of action alleged herein;

(b) judgment declaring that Cribl has infringed each of the '443, '438, '206, '467, and '312 Patents;

(c) judgment declaring that Cribl's infringement of the '443, '438, '206, '467, and '312 Patents has been willful;

(d) a grant of a permanent injunction pursuant to 35 U.S.C. § 283 enjoining Cribl and all of its officers, agents, servants, representatives, employees, associates, attorneys, parent and subsidiary corporations, affiliates, assigns and successors in interest, and all persons acting by, through, or in concert with any of them, from further acts of patent infringement;

(e) judgment declaring that Cribl and Clint Sharp have infringed Splunk's copyright in the S2S source code;

(f) judgment declaring that Cribl has infringed Splunk's copyrights in Splunk Enterprise;

(g) judgment declaring that Cribl's and Clint Sharp's infringement of Splunk's copyrights in the S2S source code and Splunk Enterprise has been willful;

(h) a grant of a permanent injunction pursuant to 17 U.S.C. § 502 enjoining and restraining Cribl and Clint Sharp and all of their officers, agents, servants, representatives, employees, associates, attorneys, parent and subsidiary corporations, affiliates, assigns and successors in interest, and all persons acting by, through, or in concert with any of them, from infringing Splunk's copyrights in the S2S source code and Splunk Enterprise;

(i) judgment declaring that Clint Sharp has violated the DMCA (17 U.S.C. § 1202);

(j) judgment declaring that Cribl has violated the DMCA (17 U.S.C. § 1201);

(k) a grant of a permanent injunction pursuant to 17 U.S.C. § 1203 enjoining and restraining Cribl and Clint Sharp and all of their officers, agents, servants, representatives, employees, associates, attorneys, parent and subsidiary corporations, affiliates, assigns and

successors in interest, and all persons acting by, through, or in concert with any of them, from committing further DMCA violations;

(l) judgment that Cribl has breached the TAP Agreement;

(m) a grant of a permanent injunction enjoining and restraining Cribl and all of its officers, agents, servants, representatives, employees, associates, attorneys, parent and subsidiary corporations, affiliates, assigns and successors in interest, and all persons acting by, through, or in concert with any of them, from making improper and unauthorized use of Splunk Enterprise and any other Splunk software;

(n) judgment that Cribl has tortiously interfered with Splunk's prospective business relations;

(o) a grant of permanent injunction enjoining and restraining Cribl and all of its officers, agents, servants, representatives, employees, associates, attorneys, parent and subsidiary corporations, affiliates, assigns and successors in interest, and all persons acting by, through, or in concert with any of them, from further interfering with Splunk's prospective business relations;

(p) judgment that Cribl has engaged in unfair competition;

(q) a grant of permanent injunction enjoining and restraining Cribl and all of its officers, agents, servants, representatives, employees, associates, attorneys, parent and subsidiary corporations, affiliates, assigns and successors in interest, and all persons acting by, through, or in concert with any of them, from engaging in further unfair competition;

(r) judgment that this is an exceptional case under 35 U.S.C. § 285 and other applicable laws;

(s) actual or compensatory damages in an amount to be determined at trial, including trebling of all damages awarded with respect to willful infringement of the '443, '438, '206, '467,

and '312 Patents under 35 U.S.C. § 284, and in no event less than a reasonable royalty for Cribl's patent infringement;

(t) an accounting of all of Cribl's and Clint Sharp's profits derived from their infringing activity, DMCA violations, tortious interference with prospective business relations, and unfair competition;

(u) either actual damages and any additional profits attributable to Cribl's and Clint Sharp's copyright infringement and DMCA violations, or statutory damages, in an amount to be determined at trial, pursuant to 17 U.S.C. §§ 504 and 1203;

(v) actual or compensatory damages in an amount to be determined at trial resulting from Cribl's tortious interference with Splunk's prospective business relations and unfair competition;

(w) punitive damages resulting from Cribl's conduct having been committed willfully, maliciously, and so carelessly as to indicate a wanton disregard for Splunk's rights;

(x) costs and non-attorneys' fees incurred in connection with this action pursuant to 35 U.S.C. § 284, 17 U.S.C. §§ 505 and 1203, and other applicable laws;

(y) attorneys' fees incurred in connection with this action pursuant to 35 U.S.C. § 285, 17 U.S.C. §§ 505 and 1203, and other applicable laws;

(z) pre- and post-judgment interest pursuant to 35 U.S.C. § 284 and other applicable laws; and

(aa) such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Splunk requests a trial by jury of all issues so triable by right.

Dated: October 5, 2022

FISH & RICHARDSON P.C.

By: */s/ Susan E. Morrison*

Susan E. Morrison (#4690)
222 Delaware Ave., 17th Floor
Wilmington, DE 19801
Telephone: (302) 652-5070
morrison@fr.com

Frank E. Scherkenbach (*pro hac vice forthcoming*)
Andrew G. Pearson (*pro hac vice forthcoming*)
Adam Kessel (*pro hac vice forthcoming*)
Kevin Su (*pro hac vice forthcoming*)
Kayleigh E. McGlynn (*pro hac vice forthcoming*)
Daniel H. Wade (*pro hac vice forthcoming*)
One Marina Park Drive
Boston, MA 02210
Telephone: (617) 542-5070

Olivia Nguyen (*pro hac vice forthcoming*)
500 Arguello Street, Suite 400
Redwood City, CA 94063
Telephone: (650) 839-5070

Attorneys for Plaintiff
SPLUNK INC.