

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

<b>PACSEC3, LLC,</b>	)	
<b>Plaintiff,</b>	)	
	)	<b>Civil Action No. 2:22-cv-00055-JRG-RSP</b>
<b>v.</b>	)	<b>(Lead Case)</b>
	)	
<b>FORESCOUT TECHNOLOGIES, INC.,</b>	)	<b>JURY TRIAL DEMANDED</b>
<b>Defendant.</b>	)	

---

<b>PACSEC3, LLC,</b>	)	
<b>Plaintiff,</b>	)	
	)	<b>Civil Action No. 2:22-cv-00056- JRG-RSP</b>
<b>v.</b>	)	<b>(Consolidated Case)</b>
	)	
<b>SPLUNK, INC.,</b>	)	<b>JURY TRIAL DEMANDED</b>
<b>Defendant.</b>	)	

**PLAINTIFF’S CORRECTED FIRST AMENDED  
COMPLAINT FOR PATENT INFRINGEMENT**

PacSec3, LLC (“PacSec”) files this Corrected First Amended Complaint and demand for jury trial seeking relief from patent infringement of the claims of U.S. Patent No. 7,523,497 (“the ‘497 patent”) (referred to as the “Patent-in-Suit”) by Splunk, Inc. (“Splunk”). This Corrected First Amended Complaint is filed before Defendant has answered or otherwise plead in an effort to prevent motion practice and by agreement of the parties.

**I. THE PARTIES**

1. Plaintiff PacSec3, LLC is a Texas Limited Liability Company with its principal place of business located in Harris County, Texas.

2. On information and belief, Splunk is a corporation organized under the laws of the State of Delaware with an office at 6860 Dallas Pkwy, Plano, TX 75024. On information and belief, SPLUNK sells and offers to sell products and services throughout Texas, including in this judicial

district, and introduces products and services that perform infringing methods or processes into the stream of commerce knowing that they would be sold in Texas and this judicial district. SPLUNK can be served with process through their registered agent, National Registered Agents, Inc., 1999 Bryan St., Suite 900, Dallas, TX 75201 or wherever they may be found.

## **II. JURISDICTION AND VENUE**

3. This Court has original subject-matter jurisdiction over the entire action pursuant to 28 U.S.C. §§ 1331 and 1338(a) because Plaintiff's claim arises under an Act of Congress relating to patents, namely, 35 U.S.C. § 271.

4. This Court has personal jurisdiction over Defendant because: (i) Defendant is present within or has minimum contacts within the State of Texas and this judicial district; (ii) Defendant has purposefully availed itself of the privileges of conducting business in the State of Texas and in this judicial district; and (iii) Plaintiff's cause of action arises directly from Defendant's business contacts and other activities in the State of Texas and in this judicial district.

5. Venue is proper in this district under 28 U.S.C. §§ 1391(b) and 1400(b). Defendant has committed acts of infringement and has a regular and established place of business in this District. Further, venue is proper because Defendant conducts substantial business in this forum, directly or through intermediaries, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct and/or deriving substantial revenue from goods and services provided to individuals in Texas and this District.

## **III. INFRINGEMENT - Infringement of the '497 Patent**

6. On April 21, 2009, U.S. Patent No. 7,523,497 (“the ‘497 patent”, included as an attachment) entitled “PACKET FLOODING DEFENSE SYSTEM,” was duly and legally issued by the U.S. Patent and Trademark Office. PacSec3, LLC owns the ‘497 patent by assignment.

7. The ‘497 patent relates to a novel and improved manner and system of defense to a data packet flood attack.

8. SPLUNK offers for sale, sells and manufactures one or more firewall systems that infringes one or more claims of the ‘497 patent, including one or more of claims 7-12 and 16, literally or under the doctrine of equivalents. Defendant put the inventions claimed by the ‘497 Patent into service (i.e., used them); but for Defendant’s actions, the claimed-inventions embodiments involving Defendant’s products and services would never have been put into service. Defendant’s acts complained of herein caused those claimed-invention embodiments as a whole to perform, and Defendant’s procurement of monetary and commercial benefit from it.

9. Support for the allegations of infringement may be found in the following preliminary table:

<b>US7523497 B2 Claim 7</b>	<b>Splunk® Enterprise</b>
---------------------------------	---------------------------

7. A method of providing packet flooding defense for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said method comprising the steps of:



Free Splunk



SPLUNK PLATFORM

# Splunk® Enterprise

Search, analysis and visualization for actionable insights from all of your data.

Estimate Savings

© 2005-2022 Splunk Inc. All rights reserved.

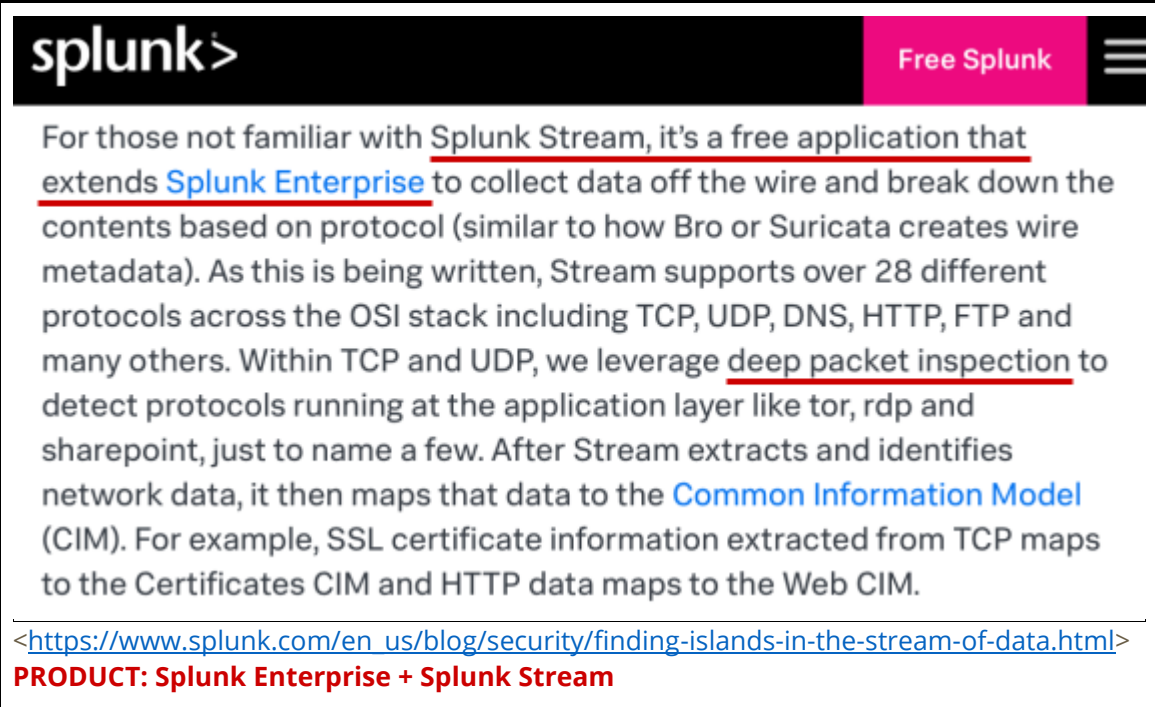
<https://www.splunk.com/>

Splunk® Enterprise has a method of providing packet flooding defense for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets.

The reference includes subject matter disclosed by the claims of the patent after the priority date.

US7523497 B2  
Claim 7

Splunk® Enterprise

<p>determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer; said path comprising all routers in said network via which said packets are routed to said computer;</p>	 <p>The screenshot shows the Splunk logo and a navigation bar with 'Free Splunk' and a menu icon. The main content is a blog post titled 'Finding Islands in the Stream of Data' which discusses Splunk Stream as a free application that extends Splunk Enterprise to collect data off the wire and break down the contents based on protocol. It mentions that Stream supports over 28 different protocols across the OSI stack, including TCP, UDP, DNS, HTTP, and FTP. It also notes that Stream uses deep packet inspection to detect protocols running at the application layer, such as tor, rdp, and sharepoint. The post concludes by stating that after Stream extracts and identifies network data, it maps that data to the Common Information Model (CIM), with examples like SSL certificate information mapping to the Certificates CIM and HTTP data mapping to the Web CIM. A URL is provided at the bottom: &lt;a href='\"https://www.splunk.com/en_us/blog/security/finding-islands-in-the-stream-of-data.html\"&gt;https://www.splunk.com/en_us/blog/security/finding-islands-in-the-stream-of-data.html&lt;/a&gt;. Below the URL, the text 'PRODUCT: Splunk Enterprise + Splunk Stream' is displayed in red.</p>
<p>US7523497 B2 Claim 7</p>	<p>Splunk® Enterprise</p>

Deep Packet Inspection (DPI) is a fundamental technique used by firewalls to inspect headers and the payload of network packets before passing them down the network subject to security rules. DPI provides information about the source and destination of the packet, the protocol, other IP and TCP/UDP header information, and the actual data. In the Common Information Model, deep packet inspection data is typically mapped to the **Network Traffic Data model**.

## Visibility

DPI provides raw information of everything transmitted over a network, including things that aren't necessarily part of or difficult to extract from a log, such as database query results. PCAP data can also be used to provide and identify:

- DNS session analysis for malicious domain communications from each endpoint
- Abnormal amounts of traffic or sessions
- Abnormal amounts of domain and host communications
- Known malicious traffic from a host
- Expired SSL certification analysis
- Abnormal host communications (internal and external)

<[https://lantern.splunk.com/Data\\_Descriptors/Data\\_Types/Network/Deep\\_packet\\_inspection\\_data](https://lantern.splunk.com/Data_Descriptors/Data_Types/Network/Deep_packet_inspection_data)>  
 The reference describes determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer; said path comprising all routers in said network via which said packets are routed to said computer..

US7523497 B2  
 Claim 7

Splunk® Enterprise

classifying data packets received at said host computer into wanted data packets and unwanted data packets by path;

The screenshot shows the Splunk logo and a 'Free Splunk' button. The main text reads: "When it comes to hunting, Stream complements other data sets you may already be collecting. "But wait!," you say, "I can't collect all the wire data in my network. I don't want to overwhelm my analysts and I certainly don't have the disk space, and also 10k other reasons..." In this case, you're in luck, because Stream allows for protocols to be selectively captured. For example, if you only want to gather FTP and NOT HTTPS, you can do that. Not only can you select the protocols to capture, you can specify individual protocol fields to capture within a specific protocol, apply filters, and even aggregate values to get certain statistics. You can also use the estimate function to preview your event count and ingest for a specific protocol before you start collecting."

	<p>&lt;<a href="https://www.splunk.com/en_us/blog/security/finding-islands-in-the-stream-of-data.html">https://www.splunk.com/en_us/blog/security/finding-islands-in-the-stream-of-data.html</a>&gt;  <b>PRODUCT: Splunk Enterprise + Splunk Stream</b></p>
<p>US7523497 B2 Claim 7</p>	<p><b>Splunk® Enterprise</b></p>
	<p>Deep Packet Inspection (DPI) is a fundamental technique used by firewalls to inspect headers and the payload of network packets before passing them down the network subject to security rules. DPI provides information about the source and destination of the packet, the protocol, other IP and TCP/UDP header information, and the actual data. In the Common Information Model, deep packet inspection data is typically mapped to the <b>Network Traffic Data model</b>.</p> <p><b>Visibility</b></p> <p><u>DPI provides raw information of everything transmitted over a network, including things that aren't necessarily part of or difficult to extract from a log, such as database query results. PCAP data can also be used to provide and identify:</u></p> <ul style="list-style-type: none"> <li>• DNS session analysis for malicious domain communications from each endpoint</li> <li>• <u>Abnormal amounts of traffic or sessions</u></li> <li>• Abnormal amounts of domain and host communications</li> <li>• Known malicious traffic from a host</li> <li>• Expired SSL certification analysis</li> <li>• Abnormal host communications (internal and external)</li> </ul> <p>&lt;<a href="https://lantern.splunk.com/Data_Descriptors/Data_Types/Network/Deep_packet_inspection_data">https://lantern.splunk.com/Data_Descriptors/Data_Types/Network/Deep_packet_inspection_data</a>&gt;  The reference describes classifying data packets received at said host computer into wanted data packets and unwanted data packets by path.</p>
<p>US7523497 B2 Claim 7</p>	<p><b>Splunk® Enterprise</b></p>

<p>associating a maximum acceptable processing rate with each class of data packet received at said host computer; and</p>	<pre> maxSockets = &lt;integer&gt; * The number of HTTP connections that the HTTP event collector input   accepts simultaneously. * Set this setting to constrain resource usage. * If you set this setting to 0, the input automatically sets it to   one third of the maximum allowable open files on the host. * If this value is less than 50, the input sets it to 50. If this value   is greater than 400000, the input sets it to 400000. * If set to a negative value, the input does not enforce a limit on   connections. * Default: 0  maxThreads = &lt;integer&gt; * The number of threads that can be used by active HTTP transactions. * Set this to constrain resource usage. * If you set this setting to 0, the input automatically sets the limit to   one third of the maximum allowable threads on the host. * If this value is less than 20, the input sets it to 20. If this value is   greater than 150000, the input sets it to 150000. * If the 'maxSockets' setting has a positive value and 'maxThreads'   is greater than 'maxSockets', then the input sets 'maxThreads' to be equal   to 'maxSockets'. * If set to a negative value, the input does not enforce a limit on threads. * Default: 0             </pre> <p><a href="https://docs.splunk.com/Documentation/Splunk/8.2.6/Admin/Inputsconf">https://docs.splunk.com/Documentation/Splunk/8.2.6/Admin/Inputsconf</a>  The reference describes associating a maximum acceptable processing rate with each class of data packet received at said host computer.  <b>PRODUCT: Splunk Enterprise + Splunk Stream</b></p>
<p><b>US7523497 B2 Claim 7</b></p>	<p><b>Splunk® Enterprise</b></p>
<p>allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets.</p>	<pre> sslCommonNameToCheck = &lt;commonName1&gt;, &lt;commonName2&gt;, ... * A list of SSL Common Names to match against certificates that incoming   HTTPS connections present to this instance. * If you configure this setting and also set 'requireClientCert' to "true",   splunkd limits most inbound HTTPS connections to hosts that use   a cert with one of the listed common names. * The most important scenario to use this setting is distributed search. * This feature does not work with the deployment server and client   communication over SSL. * This setting is optional. * Default: empty string (no common name checking)             </pre> <p><a href="https://docs.splunk.com/Documentation/Splunk/8.2.6/Admin/Inputsconf">https://docs.splunk.com/Documentation/Splunk/8.2.6/Admin/Inputsconf</a>  The reference describes allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets.  <b>PRODUCT: Splunk Enterprise + Splunk Stream</b></p>

These allegations of infringement are preliminary and are therefore subject to change.



16. SPLUNK has and continues to induce infringement from at least the filing date of the lawsuit. SPLUNK has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., DDOS protection systems) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 7-12 and 16 of the '497 patent, literally or under the doctrine of equivalents. Splunk, from at least the filing date of the lawsuit, has continued to encourage and instruct others on how to use the products showing specific intent. Moreover, Defendant has known of the '497 patent and the technology underlying it from at least the filing date of the lawsuit.<sup>1</sup> For clarity, direct infringement is previously alleged in this complaint.

17. SPLUNK has and continues to contributorily infringe from at least the filing date of the lawsuit. SPLUNK has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., DDOS protection systems) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 7-12 and 16 of the '497 patent, literally or under the doctrine of equivalents. Splunk, from at least the filing date of the lawsuit, has continued to encourage and instruct others on how to use the products showing specific intent. Further, there are no substantial noninfringing uses for Defendant's products and services. Moreover, Defendant has known of the '497 patent and the technology underlying it from at least the filing date of the lawsuit.<sup>2</sup> For clarity, direct infringement is previously alleged in this complaint.

---

<sup>1</sup> Plaintiff reserves the right to amend and add inducement pre-suit if discovery reveals an earlier date of knowledge.

<sup>2</sup> Plaintiff reserves the right to amend and add inducement pre-suit if discovery reveals an earlier date of knowledge.

18. SPLUNK has caused and will continue to cause PacSec3 damage by direct and indirect infringement of (including inducing infringement of) the claims of the '497 patent.

**IV. JURY DEMAND**

PacSec3 hereby requests a trial by jury on issues so triable by right.

**V. PRAYER FOR RELIEF**

WHEREFORE, PacSec3 prays for relief as follows:

- a. enter judgment that Defendant has infringed the claims of the '497 patent through selling, offering for sale, manufacturing, and inducing others to infringe by using and instructing to use DDOS protection systems;
- b. award PacSec3 damages in an amount sufficient to compensate it for Defendant's infringement of the Patents-in-Suit in an amount no less than a reasonable royalty or lost profits, together with pre-judgment and post-judgment interest and costs under 35 U.S.C. § 284;
- c. award PacSec3 an accounting for acts of infringement not presented at trial and an award by the Court of additional damage for any such acts of infringement;
- d. declare this case to be "exceptional" under 35 U.S.C. § 285 and award PacSec3 its attorneys' fees, expenses, and costs incurred in this action;
- e. a decree addressing future infringement that either (i) awards a permanent injunction enjoining Defendant and its agents, servants, employees, affiliates, divisions, and subsidiaries, and those in association with Defendant from infringing the claims of the Patents-in-Suit, or (ii) awards damages for future infringement in lieu of an injunction in an amount consistent with the fact that for future infringement the Defendant will be an

adjudicated infringer of a valid patent, and trebles that amount in view of the fact that the future infringement will be willful as a matter of law; and

- f. award PacSec3 such other and further relief as this Court deems just and proper.

Respectfully submitted,

**Ramey LLP**

/s/William P. Ramey

William P. Ramey, III

Texas Bar No. 24027643

[wramey@rameyfirm.com](mailto:wramey@rameyfirm.com)

Kyril V. Talanov

Texas State Bar No. 24075139

[ktalanov@rameyfirm.com](mailto:ktalanov@rameyfirm.com)

5020 Montrose Blvd., Suite 800

Houston, Texas 77006

(713) 426-3923 (telephone)

(832) 900-4941 (fax)

*Attorneys for PacSec3, LLC*

**CERTIFICATE OF SERVICE**

Pursuant to the Federal Rules of Civil Procedure and LR5, I hereby certify that all counsel of record who have appeared in this case are being served on this day of May 5, 2022, with a copy of the foregoing via email and ECF filing.

/s/ William P. Ramey, III

William P. Ramey, III