A Risk Assessment of EU Cross-Border Data Transfers to the Splunk Cloud Service

Whitepaper | October 2020

Version 1

Disclaimer

This document is intended for informational purposes. Splunk reserves the right to make changes and updates to the contents contained herein. Splunk will periodically review and update this document to reflect any such changes and will notice a new publication date at the time of any updated publication.

Introduction

In June 2020, the European Court of Justice (ECJ) invalidated the EU-U.S. Privacy Shield as an adequacy mechanism for the cross-border transfer of Personal Data. In its decision, the ECJ concluded that U.S. law failed to adequately protect EU Personal Data, as U.S. Government surveillance programs could access EU Personal Data without adequate individual recourse. The ECJ further determined that, while the Standard Contractual Clauses (SCCs) remain a valid adequacy mechanism for cross-border data transfer, companies should evaluate the protections around transfers to determine whether Personal Data transferred pursuant to the SCCs meets EU data protection standards.

This Whitepaper is designed to assist Splunk customers with their evaluation of the protections provided by Splunk for cross-border data transfers to the Splunk Cloud Service. The paper is divided into three parts to address areas of concern raised by the ECJ: 1) the risk of access to your personal data under U.S. Government surveillance law; 2) the technical privacy and security controls used by Splunk to protect your data; and 3) how Splunk protects your data throughout the supply chain of sub-processors it uses to provide the Splunk Cloud Service.

Part I: Risk Assessment of Data Access in the U.S.

What is the purpose of this risk assessment?

Splunk is committed to transparency and to helping its customers understand how Splunk handles and secures customer data. In the wake of the ECJ's decision in *Schrems II*, Splunk conducted an individualized analysis regarding the sufficiency of its cross-border data transfer mechanisms to confirm that it has protections in place designed to address the concerns raised by the ECJ regarding U.S. surveillance law. We set forth below why it is unlikely that Splunk would receive an order based on U.S. surveillance regulations, and how even if it did, Splunk's security measures would protect the data and render it unreadable.

Is Splunk a likely target of U.S. surveillance law?

No. Splunk processes machine data about IT systems and assets, including how they perform and are secured. This is not the type of information that U.S. surveillance laws are designed to address, nor is this the kind of information U.S. officials seek. U.S. surveillance laws and authorities target contact information, e.g., email addresses and phone numbers, to help them intercept real time communications. Splunk is not a communications carrier, nor is it designed to systematically collect or transmit this type of information.

What is machine data?

Splunk products process and transfer metadata generated by websites, applications, servers, networks, mobile and other devices, including clickstream and transaction information, network activity, and other forms of metadata. This data is not easily readable on its own and is the reason why our customers need Splunk to make sense of it.

Machine data is critical to our customers' operations, but it is not the type of information that is the target of U.S. surveillance law. In more than 15 years since its inception, Splunk has not received any orders from the U.S. government pursuant to the Foreign Intelligence Surveillance Act (FISA).

What type of organizations are usually the target of FISA and U.S. surveillance authorities?

In *Schrems II,* the ECJ criticized the U.S. Government's ability to obtain information from a U.S.-based Electronic Communication Service Provider (ECSP) under Section 702 of FISA. Splunk is ***not*** an ECSP and it has never received orders under Section 702. While data processed in Splunk could include email addresses or phone numbers input by its customers, the processing would be ad hoc and indiscriminate: there is no systematic collection of this information by Splunk. Therefore, if the U.S. Government seeks this kind of information, it would likely subpoena the telecommunications carrier directly.

What type of communications are U.S. surveillance authorities interested in?

Section 702 is directed at the ***content*** of communications (e.g., emails and telephone calls) and metadata associated with them. The U.S. government may only acquire communications that are to or from a person targeted for surveillance. Thus, transfers of data would not be collected under Section 702 ***unless they are to or from such a person***. Given the nature of the machine data Splunk processes, it is unlikely to contain the types of communications targeted by Section 702 collection, nor would this be of any foreign intelligence value—as it is ***not a person to person communication***. Because Splunk products do not provide communication services to the public and instead process machine data generated by IT systems and applications, it would be highly unlikely that Splunk services would ever become the target of surveillance under Section 702 of FISA.

What about data collected under Executive Order 12333?

Another criticism under *Schrems II* is that information could be collected in transit from the EU to the U.S. by U.S. intelligence agencies under Executive Order 12333 (EO 12333). EO 12333 collection refers to collection of foreign intelligence that takes place under the inherent authority of the President of the United States as Commander-in-Chief, without statutory or judicial regulation. EO 12333 collections are targeted collections that take place outside of the United States and do not involve United States persons. In particular, the ECJ focused on the possibility that intelligence agencies could collect data that is in transit from the EU to the U.S. from transatlantic cables, and that such collection could occur in bulk (i.e., without targeting specific communications). To protect against such eavesdropping, Splunk encrypts customer data in transit, rendering the data indecipherable in the extraordinary event that it is captured as part of a U.S. government EO 12333 collection. Moreover, because EO 12333 affords no compulsive power, the government would not have authority under EO 12333 to require Splunk to produce the decryption key, even if the key was held in the United States. Nor does there appear to be any other authority to compel a company that is transmitting data to produce a decryption key to aid in collection under EO 12333.

Does Splunk encrypt customer data?

Splunk employs robust security by encrypting customer data in transit, including data flowing across transatlantic cables, and at rest to prevent unauthorized access by third parties. Splunk encryption standards currently include:

- TLS 1.2+ (in transit) and AES 256 (at rest)
- Industry standard encryption tools vetted to meet Splunk's security standards
- Splunk vendors are required to encrypt data in transit

Most importantly, without the encryption key, encrypted customer data is effectively immune from warrantless collection—and Splunk would not handover such encryption keys without legal process forcing such handover. Currently, Splunk is not aware of any instances in which U.S. intelligence agencies have sought an encryption key from an organization like Splunk, and it is considered highly unlikely that this would occur.

What if Splunk were to receive a national security order to provide data?

As described above, Splunk believes it is unlikely to receive national security orders targeting its customers' data. Nevertheless, should Splunk receive such an order, Splunk would evaluate the legal process served on it, and if appropriate, will challenge orders that it believes are inconsistent with GDPR obligations, are beyond the permissible scope of the legal authority relied upon, or are otherwise unlawful. Moreover, if an order is received, Splunk will adhere to its contractual obligations and the requirements of the GDPR by notifying its customer to the extent permitted by law.

Part II: Risk Assessment of Splunk's Technical Controls

Splunk Cloud is a platform that provides customers the ability to search, monitor and analyze machine-generated data across their organization. While Splunk's Cloud Security Addendum (CSA) details the technical and administrative controls used to protect customer data (otherwise referred to as "Customer Content" in Splunk agreements and the CSA), this section provides a more detailed look into how customer data is secured end-to-end through the different access points used by the Service.

Stage 1: Ingesting data into Splunk Cloud

Customers send their data into Splunk Cloud in three primary ways via: 1) a Splunk Universal Forwarder; 2) the Splunk Cloud API; or 3) the Splunk HTTP Event Collector (HEC).

A Splunk Universal Forwarder is installed on a customer's data source, collects data from the customer's environment, and forwards it to the customer's Splunk Cloud instance.[1] The Universal Forwarder protects customer data using encryption in transit (currently TLS 1.2+) and through signed digital certificates that link the customer's Universal Forwarder to their unique Splunk Cloud instance.[2]

The Splunk Cloud API sends data directly into a customer's Splunk Cloud instance from customer endpoints that support API connectivity, encrypts customer data in transit, and is default set to "off". The API must be manually turned "on" by Splunk upon customer request, and is configured by the customer to send data to their Splunk Cloud instance using an authentication token.

[1] https://docs.splunk.com/Documentation/Forwarder/8.0.6/Forwarder/Abouttheuniversalforwarder

[2] https://docs.splunk.com/Documentation/Splunk/8.0.6/Security/ConfigureSplunkforwardingtousethedefaultcertificate

The Splunk HEC sends customer data from customer web applications directly to the customer's Splunk Cloud instance.[3] Like the Splunk API, data is encrypted in transit and HEC is only turned on by Splunk at the customer's request. Splunk HEC uses an authentication token generated by the customer to link the HEC to their Splunk Cloud instance.

In short, customer data is protected during the data ingestion process by encryption in transit and a second layer of authentication certificates and tokens linking the data source to the customer's Splunk instance.

Stage 2: Using data within Splunk Cloud

For customers who purchased encryption at rest, customer data is protected within Splunk Cloud using, at a minimum, the Advanced Encryption Standard (AES-256). [4] When a customer sends a command to perform a task (e.g., a search) on their data, the task is run in the AWS or GCP hosting location assigned to their Splunk Cloud. To manage their Splunk Cloud instance, including viewing search results, a customer accesses their Splunk Cloud instance using the Splunk Web interface.[5] The Splunk Web interface utilizes HTTPS encryption in transit.

Stage 3: Splunk monitors for unauthorized access to your data

Splunk continuously monitors your instance to detect and investigate suspicious activity.[6] Splunk employs Host-based Intrusion Detection, which logs and monitors access attempts and uses automatic alerts to trigger investigation and incident management procedures in certain cases. Splunk's monitoring of customers' Splunk Cloud instances is not limited to external threats but also includes authorized internal access by Splunk employees and contractors.

Stage 4: Splunk's access to your data

In limited circumstances in order to provide the Hosted Service, Splunk may require access to your data. As discussed in this section, in such an event, your data is protected in multiple ways, including from Splunk.

A. **Support program activities.** Technical support can range from answering a simple question to helping a customer configure their Splunk Cloud instance, which generally does not require access to customer data. During Support, a customer may generate a diagnostic file (diag file) and send it to their Support representative to help diagnose the problem. Diag files give Splunk support insight into how a Splunk instance is configured and operating.[7] If created according to Splunk's documented instructions, diag files do not contain customer data; for additional protection, Customers also have the ability to redact or anonymize data within the diag file prior to sending to Splunk.[8] Diag files are uploaded to Splunk using the Splunk Support portal[9] and are encrypted in transit and at rest while stored at Splunk.

---

[3] https://docs.splunk.com/Documentation/Splunk/latest/Data/UsetheHTTPEventCollector
[4] https://docs.splunk.com/Documentation/SplunkCloud/8.0.2001/Service/SplunkCloudservice
[5] https://docs.splunk.com/Documentation/SplunkCloud/8.0.2006/User/Admintasks
[6] https://www.splunk.com/en_us/legal/splunk-data-security-and-privacy.html
[7] Diag files are more commonly generated with Splunk Enterprise (On-prem) but may also be generated for Splunk Cloud. https://docs.splunk.com/Documentation/Splunk/8.0.5/Troubleshooting/Generateadiag
[8] https://docs.splunk.com/Documentation/Splunk/8.0.5/Troubleshooting/Generateadiag
[9] https://docs.splunk.com/Documentation/Splunk/8.0.5/Troubleshooting/Generateadiag#Upload_a_file_to_Splunk_Support

If a customer requests their Splunk Support representative access their data, access is granted on an ephemeral basis that auto-expires. For details on how that access is limited, logged, monitored and audited, please refer to the Splunk Cloud SOC2 report.

To provide 24/7 support, Splunk utilizes a follow-the-sun model, providing Support representatives in different time zones across the world. The names and locations of Support sub-processors are set forth in the list of sub-processors on Splunk's Privacy Policy.[10] Splunk sub-processors use a secure virtual desktop infrastructure (VDI)[11] to access Splunk systems. Through the VDI, Splunk can control, log, monitor, and audit its sub-processor's access in the same way it does for Splunk employees, and if necessary, revoke their access immediately. Sub-processors who provide support to Splunk Cloud customers do so following the same process described in the Splunk Cloud SOC2 report.

B. **Configuration and implementation services.** Splunk Cloud Operations engineers configure customer instances and perform tasks to keep the customer's instance running.[12] In the unlikely event that Splunk Cloud Operations would require access to Customer Content, that access is provided only upon a specific need and authorized, logged, monitored and audited under the process described in the Splunk Cloud SOC2 report.

In short, Splunk protects your data end-to-end using a combination of encryption, digital certificates, security tokens, monitoring for unauthorized access, and controlling, monitoring, logging and auditing authorized access.

Part III: Risk Assessment of Splunk's Sub-processors and Onward Transfers

Splunk relies on sub-processors to help provide various aspects of the Splunk Cloud Service, including such things as:

- Bug reporting
- Customer billing and accounting
- Data analytics
- Enterprise services
- Infrastructure-as-a-Service
- IT infrastructure and data center solution services
- Marketing automation
- Mobile analytics
- Staffing and support services
- Technical support services

[10] https://www.splunk.com/en_us/legal/privacy/privacy-policy.html#splunk-shares
[11] For information on how VDIs work, see https://aws.amazon.com/workspaces/?workspaces-blogs.sort-by=item.additionalFields.createdDate&workspaces-blogs.sort-order=desc
[12] Splunk Cloud provides 100% uptime availability. Splunk's engineers work around-the-clock, so our customers don't have to: https://www.splunk.com/en_us/legal/splunk-cloud-service-level-schedule.html

A complete list of Splunk's sub-processors may be found here. In addition, customers may sign up to receive notifications about changes to Splunk's sub-processor list here.

Splunk's sub-processor review process

Maintaining the privacy, security and confidentiality of customer data is a priority at Splunk. Splunk's vendor review process is a multi-stakeholder initiative between Splunk's Legal, Global Security, IT and Procurement teams. The process is composed of targeted policies, processes, and assessment tools to evaluate the vendors within Splunk's data ecosystem and help Splunk meet its regulatory compliance obligations. Sub-processors are evaluated prior to onboarding. Splunk's vendors must pass a robust vetting process that is proportional to the services offered and the sensitivity of the data involved. Notable review elements include a deep dive into the vendor's products and services, security information, privacy information, systems and integration information, and other relevant documentation. Annual reassessments are performed for certain high-risk vendors. Reassessments are also performed when there's a material change in the vendor's data processing activities.

Splunk only shares access to customer data with vendors who have a "need-to-know" and who are subject to appropriate controls including, but not limited to, administrative controls, data encryption, remote VPN, and asset monitoring. In addition, Splunk relies on industry-standard data protection agreements to hold its vendors accountable, including the Splunk Data Protection Agreement (DPA) and Splunk's Information Security Addendum (ISA). Further, to the extent permitted by law, Splunk agrees in its Splunk General Terms for its Cloud Service that it will notify customers of any law enforcement requests it may receive for access to customer data.

Splunk's response to the Privacy Shield invalidation

Splunk relies on SCCs to support cross-border data transfers to the U.S. Splunk's Data Protection team has amended Splunk's DPA to include SCCs for legacy customer DPA's that may not include them. Splunk's amendment may be found here. Further, we have reviewed the sub-processors in our in-product ecosystem to ensure that the appropriate flow-downs are in place. Splunk continues to evaluate the ECJ's decision, the recent invalidation of the Swiss-U.S. Privacy Shield Framework, and their impact on Splunk.