Privacy and Security in the Splunk Cloud Platform

Nov. 2023

Customer FAQ

Splunk is committed to transparency with our customers regarding how we process and secure personal data in the Splunk Cloud Platform ("SCP"). As part of that commitment, this FAQ provides helpful information about the privacy and security controls we implement and is a resource to help customers complete data protection impact assessments. For more detailed information about Splunk's privacy, security, and compliance programs, please visit Splunk Protects.

General Description: SCP

What does SCP do?

SCP is a cloud-based service for processing and indexing machine-generated data to provide customers with insights into the performance and security of their IT infrastructure and other important components in our customers' resiliency posture.

What are log files?

Every time something happens within an electronic device (i.e., an event), the device notes the event in a log. For example, when a user logs into a network server, the server may "see" the following: "on X date, at Y time, user jsmith logged in and typed the correct password." These actions are recorded into a file ("log file") that could be ingested by organizations into SCP. Log files are created on all types of devices, such as network servers, routers, firewalls, laptops, mobile phones, smart watches, and others. In short, log files can be created to record activity on any system or machine that processes data.

Log files denote important information about how IT systems or collections of individual devices within them are performing and whether their security may be at risk. For example, using SCP, customers can analyze log files from network file servers to determine whether their network hard drive is performing erratically and needs to be replaced before it fails. As another example, customers can set up alerts in SCP to notify them of hundreds of unsuccessful logins from a single IP address, which may suggest that a brute force attack has occurred on a user account.

Personal Data Processed in SCP

What categories of personal data are processed in SCP?

Log files typically only contain minor elements of personal data, such as a user ID or IP address. SCP does not require personal data to function for its intended purposes.[1] Customers need not ingest personal data as part of log files to make use of SCP. In a typical use case, customers configure SCP so log files contain only certain, specifically required elements of personal data, such as a customer-internal user ID or IP address needed to alert for potential security issues. In unstructured log files, identifying an individual can be difficult without corroborating, external information that is not normally ingested into SCP. Additionally, customers can

[1] Note that Splunk user IDs for a customer's representatives operating their SCP service are required. Often, customers select email addresses to serve as Splunk user IDs.

self-manage their data (including personal data) within SCP by applying privacy-enhancing techniques, such as hashing, redaction, or suppression, before or after the data is ingested into SCP. For more, see guidance provided in the SCP Service Description.

Does the personal data processed in SCP include special categories of personal data?

Log files rarely contain special categories of personal data as defined under Article 9 of the GDPR (i.e., those that are more sensitive), or sensitive information or data types defined under PCI or HIPAA. Customers are responsible for ensuring that submission of any special categories of personal data, or other sensitive information or data, complies with applicable laws and contract terms.

Who can access personal data processed in SCP, and from where?

In a limited set of scenarios, Splunk may access customer data that is ingested into SCP. One example is for the operation of SCP, which includes updating, securing, and troubleshooting our services, as well as providing support. Another example is to operate our business, which includes analyzing SCP's performance and meeting our legal obligations in the areas of export controls and sanctions compliance. Splunk has implemented the principle of least-privileged access for such scenarios, and carefully monitors any access to customer data (see section titled, "Splunk Monitors Access," below, for more information).

Splunk also engages sub-processors to support the operation of SCP and our related services at a global scale. Prior to engaging with a sub-processor, Splunk evaluates the sub-processor's security, privacy and resiliency practices. A list of Splunk's sub-processors is posted at Splunk Offerings Sub-processors, which includes the sub-processors' locations and processing activities. Customers may also sign up to receive notifications of any changes to Splunk's sub-processors through our Data Protection Notification Portal. While processing is performed globally, customers can choose the region where their data is hosted (for example, data hosting can be limited to within the EEA).

International data transfers and transfer impact assessments

Splunk may transfer data from the EEA to so-called Third Countries, and from the UK to other countries. In such cases, Splunk currently relies on the standard contractual clauses pursuant to European Commission Decision 2021/914/EU including the modules for controller-processor with our customers and the modules for processor-processor with our sub-processors, or on the clauses updated from time to time or replaced by the UK's Information Commissioner's Office.

Splunk has reviewed the European Data Protection Board's guidance regarding supplementary measures for international data transfers and the specific questions raised by NOYB in their questionnaire regarding international data transfers post-Schrems II. We have published a white paper and issued responses to this questionnaire on our website. Please see A Risk Assessment of EU Cross-Border Data Transfers and Splunk's Responses to the European Center for Digital Rights (NOYB) Questions. Splunk provides these materials in compliance with our obligations under Article 28(f) of the GDPR to assist customers that are controllers in completing a transfer impact assessment.

What is Splunk's policy regarding law enforcement requests?

If faced with requests by government agencies and other third parties for customer data, Splunk makes reasonable efforts to refer the matter to customer. Splunk only discloses customer data if legally necessary, and requires proper domestication for any such request. Further details are in the Splunk Data Request Guidelines.

Protecting Personal Data Processed in SCP

Security Measures

Splunk's security and privacy programs meet the highest standards in the industry and are further set forth in the SCP Security Addendum. This includes organizational and technical measures such as:

- GDPR-required "data breach" notification
- Policies, practices and training
- Access and user management
- Governance and audit management
- Password management and authentication controls
- Encryption
- Threat and vulnerability management
- Logging and monitoring
- Secure software development
- Network security, physical security, human resources security
- Business continuity and disaster recovery plans
- Asset management and disposal
- Splunk vendor security
- Annual third-party audits for ISO 27001, SOC2 Type2, HIPAA/PCI-DSS, FedRAMP, IL5

Encryption

SCP employs robust security by encrypting customer data in transit (including data flowing across transatlantic cables). Customers can also purchase additional encryption at rest (AES 256 standard) at the application layer for additional security.[2] Splunk encryption standards currently include:

- TLS 1.2+ (in transit)
- Industry standard encryption tools vetted to meet Splunk's security standards
- A requirement that Splunk sub-processors encrypt data in transit
- Regular rotation and monitoring of encryption keys

Further, if customers select Amazon Web Services (AWS) to host their SCP service, AWS Key Management Service (KMS) will be used to create and maintain a primary encryption key to secure data on customers' SCP deployments. KMS is a fully managed service, backed by Federal Information Processing Standards (FIPS) 140 hardware security modules, and is also supported on PCI and HIPAA deployments. With this model, Splunk is responsible for management of the keys, including all creation, rotation, and revocation operations.

For customers that wish to have additional safeguards, Splunk also offers Enterprise Managed Encryption Keys (EMEK) as an optional capability for customers purchasing encryption at rest. By leveraging this capability, the customers' SCP service administrators can grant and subsequently rotate, revoke, or disable access to customers' complete data set while maintaining the same degree of real-time data encryption and decryption operations that comes with the managed-service model. EMEK gives customers the flexibility of managing the encryption key themselves, ensuring that customers maintain control of their SCP deployment. Please see Secure Data with Enterprise Managed Encryption Keys - Splunk Documentation for more information.

Access Controls and Monitoring

SCP allows customers to set various security parameters in their SCP service, including access controls. For details, see Use Access Control to Secure Splunk Data and About Configuring Role-based User Access.

[2] For customers that select Google Cloud Platform (GCP) to host their SCP service, encryption at rest at the application layer is included.

Splunk continuously monitors activity across SCP, including customers' SCP services, to detect and investigate suspicious activity. Splunk employs an intrusion detection system, which logs and monitors access attempts and uses automatic alerts to trigger investigation and incident management procedures in certain cases.

Splunk also has a range of organizational and technical controls in place to prevent and detect unauthorized access. Splunk has policies and standards for Splunk employees to access customer data. Access is granted based on job roles and requirements, or for specific tasks where access is required. Requests for access are documented in Splunk's implemented approval systems, which include periodic reviews of each individual's access levels on a set cadence. Where granted, access is limited in scope and time as appropriate based on job scope and responsibilities. Splunk logs and monitors access 24/7, and maintains numerous sophisticated alerts to detect both insider threat scenarios and external security issues. Splunk regularly undergoes audits by internal and external auditors on these controls.

If customers request support for issues that cannot be replicated in a non-production environment, Splunk may require access to the customers' environments to support their requests. In this scenario, the customers must explicitly authorize access to their SCP service to Splunk through support tickets. Access is managed under the principle of "least privilege", using scoped and/or ephemeral access tokens to help ensure that access is granted only insofar as is required to resolve the customers' specific issues. If needed, secure Virtual Desktop Infrastructure (VDI) is used for such access, which has Data Loss Prevention (DLP) controls built in (such as disabled USB and limited internet ingress/egress, among others).

Privacy by Design

SCP development incorporates privacy-by-design principles, and numerous built-in features enable privacy.

- **Data Collection**. Customers can restrict data collection from only allowed IP addresses by using the Administrative Configuration Service (ACS). For more details, please see Admin Config Service Manual.

- **Data Anonymization**. SCP supports the use of advanced anonymization, pseudonymization, obfuscation, and tokenization techniques ("anonymization") to remove confidential data from the data that customers index into SCP. Customers can anonymize parts of confidential fields to protect privacy while providing enough remaining data for use in event tracking. For more details, please see Getting Data In.

  During support, a customer may generate a diagnostic file (diag file) and send it to Splunk's support representative to help diagnose the problem. Diag files give Splunk's support personnel insight into how a customer's SCP service is configured and operating. If created according to Splunk's documented instructions, diag files do not contain customer data or include personal data. For additional protection, customers also can redact or anonymize data within the diag file through the functionality of the SCP service prior to sending a diag file to Splunk.

- **Data Deletion, Return, and Portability**. SCP has functionality to retain, delete or export (return) data. Customers choose how long to retain their data by setting retention schedules after which data is deleted in accordance with contract terms, including personal data, within SCP. Customers can tailor retention options by country and for any duration required (additional fees may apply).

- **Data Subject Requests**. SCP is equipped with self-help capabilities to enable customers to address data subject requests via the data deletion, return, and portability functions described above.

- **Data Segregation**. While the SCP service may be multi-tenant, logical separation of customer data is enforced to avoid commingling of different customers' data.

Data Hosting Location

As of Nov. 2023, Splunk offers the following data hosting locations for SCP. Customers have the option to limit data hosting to the EEA or the UK. For more details and a current list of data hosting locations, please see SCP Service Description.

AWS regions:

- US (Oregon, Virginia, GovCloud-West, GovCloud-East)
- UK (London)
- Europe (Dublin, Frankfurt, Paris, Stockholm)
- Asia Pacific (Mumbai, Seoul, Singapore, Sydney, Tokyo)
- Canada (Central)

Google Cloud regions:

- US (Iowa)
- UK (London)
- Europe (Belgium, Frankfurt)
- Asia Pacific (Singapore, Sydney)
- Canada (Montreal)