splunk> turn data into doing

UK Cloud Security Principles: Splunk Cloud Platform and Splunk Observability Cloud

Dec. 2023

Disclaimer

This document sets out Splunk's response for Splunk® Cloud Platform (Splunk Cloud) and the Splunk Observability Cloud (Observability Cloud) in response to the UK National Cyber Security Centre's (NCSC) Cloud Security Principles. These principles were first published as guidance for the UK public sector to evaluate cloud services. Splunk reserves the right to make changes and updates to its practices, services, systems, and environments. Splunk will periodically review and update this document to reflect any such changes and will provide a new publication date at the time of any updated publication.

Table of Contents

Introduction

Splunk is dedicated to keeping its customers' data secure and private. Splunk is committed to adhering to global and industry compliance initiatives. Further details about Splunk's data privacy and security practices can be found at Splunk Protects.

In this document, Splunk responds to each of the UK National Cyber Security Centre's Cloud Security Principles. These Principles were first published as guidance for the UK public sector to evaluate cloud services. However, the Principles also provide useful information about Splunk's security for all customers regardless of geography or sector.

This document is intended for anyone considering adoption of, or already using, Splunk Cloud Platform (Splunk Cloud) or Splunk Observability Cloud (Observability Cloud) within the UK public sector or those who wish to understand more about them.

Responses to the NCSC Cloud Security

Principle 1: Data in transit protection

Principle Goals	Splunk's Response
User data transiting networks should be adequately protected against tampering and eavesdropping. Data in transit protection should be achieved through a combination of: • Encryption – denying the attacker the ability to read or modify data • Network protection – denying the attacker the ability to intercept data • Authentication – denying the attacker the ability to impersonate the service **Goals** Customers should be sufficiently confident that: • Data in transit is protected between the end users device(s) and the service • Data in transit is protected internally within the service • Data in transit is protected between the service and other services (e.g. where APIs are exposed) **Customers should prefer a cloud provider that:** • encrypts all customer-data in transit by default • pre-configures data in transit encryption, and defaults to the latest industry standards	**A. Splunk Cloud** Customers send their data to Splunk Cloud via: (1) the Splunk Universal Forwarder; (2) the Splunk Cloud API; or (3) the Splunk HTTP[s] Event Collector (HEC). By design, each method for data transit is defaulted to "off" upon install and requires configuration by (or at the request of) the customer to enable it. The Splunk Universal Forwarder (SUF) is installed on a customer's data source but must be manually enabled by the customer prior to use. The SUF collects data from the customer's environment and forwards it to the customer's Splunk Cloud instance. The SUF protects customer data in transit with TLS 1.2+ encryption (connections less than 1.2 are rejected in alignment with current NCSC guidance) and through signed digital certificates that link the customer's Universal Forwarder to their unique Splunk Cloud instance. The Splunk Cloud API sends data directly to a customer's Splunk Cloud instance from customer endpoints that support API connectivity, encrypts customer data in transit (also TLS 1.2+), 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. The Splunk HEC sends customer data from customer web applications directly to the customer's Splunk Cloud instance. Like the Splunk API, data can be 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. In addition, within and as between Splunk services, if applicable, data is encrypted by Splunk to further enhance the security of its operations using TLS. Customers can also deploy their own

• uses standardised, well-understood algorithms and protocols (such as TLS and IPsec) to protect data • makes it easy to implement good data in transit protections in your application	client-side SSL certificates to provide an additional layer of protection beyond TLS. **B. Observability Cloud** Customers send their data to Observability Cloud via: (1) direct integration with the Cloud Infrastructure-as-a-Service (IaaS) providers currently supported by the service, which are (Amazon Web Services (AWS), Google Cloud Platform (GCP)) and (2) using an OpenTelemetry collector. With Observability Cloud, customers can forward, for example, Infrastructure Monitoring (IM) metadata and metrics from their AWS, GCP and Azure infrastructure to Observability Cloud via an API. System authentication between Observability Cloud and the IaaS provider is managed by using: 1) an IAM/Project Viewer service account or 2) secure tokens created by the IaaS provider within their admin console. Observability Cloud provides supported integrations for Kubernetes, Linux, and Windows data sources by deploying the Splunk OpenTelemetry Collector to export metrics and logs from hosts and containers to Observability Cloud. Authentication between the OpenTelemetry Collector and the Observability Cloud API are managed using secure access tokens created in the Observability Cloud admin console. User data files are encrypted in transit by default using TLS 1.2+ encryption for web communication sessions.

Principle 2: Asset protection and resilience

Customer data, and the assets storing or processing it, should be protected.

Data types that are often overlooked include credentials, configuration data, derived metadata and logs. These must also be appropriately protected.

Aspects to consider:

- Physical location and legal jurisdiction
- Data centre security
- Data encryption
- Data sanitisation and equipment disposal
- Physical resilience and availability

Principle 2.1: Physical location and legal jurisdiction

Principle Goals	Splunk's Response
Goals Customers should be confident they know **where their data is**, and **who can access that data**. This should include derivatives of the data, such as verbose logs and machine learning models,	A. Splunk Cloud Splunk Cloud customers can store data in one of the following regions[1]: AWS regions: • US (Oregon, Virginia, GovCloud-West, GovCloud-East)

[1] A current list is located in the Splunk Cloud Platform Service Description.

unless sensitive aspects have been intentionally excluded or removed. Customers should understand: ● In which countries customer data will be stored, processed, and managed ● Which legal jurisdiction(s) customer data will be subject to, and whether this is acceptable ● The rights that the service provider will have to access and use customer data ● The legal circumstances under which customer data could be accessed without customer consent, and how this affects customer compliance with UK legislation	● UK (London) ● Europe (Dublin, Frankfurt, Paris, Stockholm) ● Asia Pacific (Mumbai, Seoul, Singapore, Sydney, Tokyo) ● Canada (Central) GCP regions: ● US (Iowa) ● UK (London) ● Europe (Belgium, Frankfurt) ● Asia Pacific (Singapore, Sydney) ● Canada (Montreal) Customers have the option of selecting the available region they require. If a customer needs to store data in more than one region, the customer can purchase multiple subscriptions. Data in Splunk Cloud goes through the data lifecycle according to the types of volume and index configurations set by the customer. The Customer controls the nature and type of data input into the service and the period of retention. The customer, or Splunk as needed to run Splunk Cloud and as permitted by contract, may access the data stored in the customer's designated region from outside that region or a customer may obtain after-hours support from Splunk support staff outside the designated region. A customer may also choose to use features of Splunk Cloud to allow access to or transfer of data across regions, at their option. B. Observability Cloud Data in Observability Cloud is stored in one of the following regions[2] (selected by the customer). ● AWS - US (Oregon (us-west-2), Virginia (us-east-1)) ● AWS - EU (Dublin (eu-west-1)) ● AWS - Asia Pacific (Sydney (ap-southeast-2), Tokyo (ap-northeast-1)) ● GCP - US (Oregon (us-west-1)) The customer controls the nature and type of metric data input into the service. Standard data retention for the various parts of Observability are posted here. Customers may set extended retentions or archive logs as described on the same page. The customer, or Splunk as permitted by contract or otherwise necessary to provide the service, may access the data stored in the customer's designated region from outside that region or a customer may obtain after-hours support from Splunk support staff outside the designated region. **Further Reading** ● A Risk Assessment of EU Cross-Border Data Transfers to the Splunk Cloud Service ● Splunk's Responses to the European Center for Digital Rights (noyb) questions regarding international data transfers ● Splunk Offerings Sub-processors

[2] A current list is located in the Splunk Observability Cloud service description.

Principle 2.2: Data centre security

Principle Goals	Splunk's Response
Goals Customers should be confident that the physical security measures employed by the provider are sufficient to protect against unauthorised access, tampering, theft, or reconfiguration of systems, when considered alongside data at rest protections.	Splunk Cloud and Observability Cloud are provided through AWS and GCP IaaS platforms. For more information on AWS and GCP IaaS platforms' data centre security, see https://aws.amazon.com/compliance/data-center/controls/ and https://www.google.com/about/datacenters/data-security/, respectively.

Principle 2.3: Data encryption

Principle Goals	Splunk's Response
Goals • Cloud service customer data should be adequately protected from unauthorised access by parties with physical access to infrastructure, when considered alongside data at rest protections provided by encryption • Cloud providers should encrypt all customer data at rest within the service, using an appropriate encryption algorithm and mode, as described below • Customers should prefer a cloud provider that encrypts all data at rest by default, including any metadata derived from that data • For this encryption, a symmetric encryption algorithm should be used in a mode of operation that provides both confidentiality (to prevent unauthorised reading of the data) and integrity (to prevent un-noticed tampering of the encrypted data) • Even a good algorithm will be vulnerable to attack if it's not used in a good mode of operation. So, both the algorithm and mode of operation used should be approved for general use. For	Splunk Cloud provides data encryption at rest using Advanced Encryption Standard (AES) 256-bit encryption at the container level and offers as a premium service enhancement for purchase AES 256-bit encryption at the file level. Splunk manages the encryption keys using a key management system to help ensure the secure generation, storage, distribution and destruction of encryption keys. Customers may elect to self-manage encryption keys using Splunk's Enterprise Managed Encryption Key Program. Observability Cloud encrypts at rest customer credentials to third-party systems integrated with Observability Cloud using Advanced Encryption Standard (AES) 256-bit encryption by default. Splunk uses a key management system to help ensure the secure generation, storage, distribution and destruction of encryption keys for Observability Cloud.

example, an algorithm from NIST-SP-800-131A, and a suitable mode of operation from NIST-SP-800-38. At the time of writing, these include the symmetric algorithm AES, and the modes of operation GCM and XTS. You may see these described as AES-GCM or AES-XTS.	

Principle 2.4: Data sanitisation and equipment disposal

Principle Goals	Splunk's Response
Goals The process of provisioning, migrating and de-provisioning resources should not result in unauthorised access to customer data. Customers should be confident that: • Customer data is erased when resources are moved or re-provisioned, or when requested it to be erased • Storage media which has held customer data is sanitised or securely destroyed at the end of its life	For both Splunk Cloud and Observability Cloud, Splunk maintains an inventory of cloud infrastructure assets that it regularly updates and reconciles. Documented, standard build procedures are used to install and maintain production servers. Splunk also has documented data disposal policies, including procedures for the secure disposal of customer data ingested by Splunk to protect customer data throughout its lifecycle. After expiration or termination of the customer's agreement (Agreement), Splunk will return or securely destroy customer data in accordance with the terms of the Agreement (including supporting documentation). Further, if the customer leverages Splunk's Enterprise Managed Encryption Key (EMEK) Program, once the Enterprise-Managed key is deleted, the data is unusable and in effect "sanitised". Any customer data stored electronically in Splunk's backup or email systems will be deleted over time in accordance with Splunk's records management practices. Splunk retains customer data stored in its cloud computing services for at least thirty (30) days after the expiration or termination of the Agreement. As the product is hosted on AWS and GCP IaaS, Splunk relies upon the IaaS provider to sanitise or destroy the physical media at end of life. Information on AWS and GCP media destruction policies may be found below. Splunk has documented asset and data disposal policies for the secure disposal of each. In addition, Splunk has policies and procedures covering the termination of accounts and credentials upon their decommissioning. AWS: https://aws.amazon.com/compliance/data-center/controls/ GCP: https://cloud.google.com/security/deletion/

Principle 2.5: Physical resilience and availability

Principle Goals	Splunk's Response
Goals Cloud customers should be sufficiently confident that: • The availability commitments of the service, including their ability to recover from outages, meets customer business needs • Whether the provider's resilience processes have any implications for data residency • Customers can protect their data from ransomware attacks	Splunk Cloud's Service Level Schedule, which provides specific uptime commitments, can be found here. Observability Cloud's Service Level Schedule, which similarly provides specific uptime commitments, can be found here Splunk Cloud and Observability Cloud deploy data backup, replication, and recovery systems/technologies to support resilience and protection of customer-ingested data. For further details, see Splunk Cloud Platform documentation on Splunk maintenance responsibilities and Splunk Observability Cloud service description. Splunk maintains a documented Business Continuity (BC) and Disaster Recovery (DR) program that is designed to manage significant disruptions to Splunk's critical business functions (including business operations as well as infrastructure), including those supporting the delivery of Splunk Cloud and Observability Cloud. Splunk management updates and approves the BC/DR program policy and standard annually. Splunk personnel perform annual disaster recovery tests. Test results are documented and corrective actions are noted. Supporting documentation is available to subscribers of Splunk's Customer Audit Program. Data backup, replication, and recovery systems/technologies are deployed to support resilience and protection of customer data. Backup systems are configured to encrypt backup media. As noted in Splunk Cloud's SOC 2 Type II report, Splunk Cloud backups are across availability zones within the same region, therefore addressing data residency needs. As discussed in response to Principle 5 (Operational security) below, Splunk employs numerous security tactics, including vulnerability management (and configuration and change management to prevent unexpected alterations to security properties) to minimise vulnerabilities that could be exploited in ransomware attacks. For Splunk Cloud, customers who have purchased encryption at rest may supplement with their own primary encryption key as part of the EMEK feature. Splunk also uses its own and others' resilience tools for protective monitoring, and incident management in response to concerning detected anomalies, in case of potential threats of such exploitation.

Principle 3: Separation between customers

Principle Goals	Splunk's Response
Separation techniques ensure a customer's service can't access or affect the service (or data) of another. Cloud customers rely on security boundaries implemented by the cloud provider to ensure that: • Customers can control who can access their data, and how	Splunk Cloud and Observability Cloud are both SaaS models that rely upon IaaS providers as set forth above. Each SaaS service enforces logical separation of customer data as further described in response to Principle 9 (Secure user management), below, and runs in a secured environment on a stable operating system and in a network that is hardened to industry standards using a default-deny firewall policy, which permits access of only customer-designated IP

• The service is robust enough to defend against another customer having malicious code in their instance of the service Large cloud services, such as cloud platforms, may offer many different services. These services might each take a different approach to separation. **Goals** Customers should be able to explain how they have implemented security separation within their service. This includes the security boundaries in: • compute (such as containerisation, Functions-as-a-Service, and IaaS) • storage • data flows and networking If a SaaS or PaaS service is built on top of other PaaS or IaaS services (such as in a third-party cloud), the cloud provider should explain which separation properties are inherited from the underlying components and infrastructure. Customers should be confident that for each service used, it is known which separation mechanisms are used and that they are appropriate for specific needs.	addresses and services. Customer deployments are regularly scanned for host- and application-level threats. In addition, for systems containing customer data, an external vendor conducts security penetration tests on the corporate and cloud environments at least annually to detect network and application security vulnerabilities. Critical findings from these tests are evaluated, documented and assigned to the appropriate teams for remediation. Splunk also conducts internal penetration tests periodically and remediates findings as appropriate. See further Principle 5.2 (Protective monitoring), below.

Principle 4: Governance framework

Principle Goals	Splunk's Response
A governance framework is vital to co-ordinate and direct the management of the service. An effective governance framework will ensure that procedural, personnel, physical, and technical controls continue to work through the lifetime of a service. It should also respond to changes in the service, technological developments, and the appearance of new threats. **Goals** Customers should be confident that the service has a governance framework	Splunk's Chief Information Security Officer (CISO) leads Splunk's security program. The CISO office develops, reviews and approves, together with appropriate stakeholders, Splunk's Security Policies (defined below). Splunk maintains a security program that: (a) complies with industry recognised information security standards; (b) includes administrative, technical and physical safeguards designed to protect the confidentiality, integrity and availability of customer data; and (c) is appropriate to the nature, size and complexity of Splunk's business operations. Splunk also maintains security policies, standards and methods (Security Policies) designed to safeguard the processing of customer data by employees and contractors. Splunk Security Policies are available to employees via the corporate intranet. Splunk reviews,

and processes which are appropriate for intended use. **Customers should look for good governance practices, including:** ● A clearly identified, and named, board representative (or a person with the direct delegated authority) who is responsible for the security of the cloud service. This is typically someone with the title 'Chief Security Officer', 'Chief Information Officer' or 'Chief Technical Officer'. ● A documented framework for security governance, with policies governing key aspects of information security relevant to the service. ● Security and information security are part of the service provider's financial and operational risk reporting mechanisms, ensuring that the board would be kept informed of security and information risk. ● Processes to identify and ensure compliance with applicable legal and regulatory requirements.	updates and approves Security Policies annually to maintain their continuing relevance and accuracy. Employees receive information and education about Splunk's Security Policies during onboarding and annually thereafter. New employees are required to complete security training as part of the new hire process and receive annual and targeted training (as needed and appropriate to their role) thereafter to help maintain compliance with Splunk's Security Policies, as well as other corporate policies, such as the Splunk Code of Business Conduct and Ethics (Code of Conduct). This includes requiring Splunk employees to annually re-acknowledge the Code of Conduct and other Splunk policies as appropriate. Splunk conducts periodic security awareness campaigns to educate personnel about their responsibilities and provide guidance to create and maintain a secure workplace. Splunk manages cybersecurity risks in accordance with its Risk Assessment Standard Operating Procedure, which defines how Splunk identifies, prioritises and manages risks to its information assets and the likelihood and impact of them occurring. Splunk management reviews documented risks to understand their potential impact to the business, determine appropriate risk levels and treatment options. Mitigation plans are implemented to address material risks to business operations, including data protection. Splunk operates a robust enterprise risk management program, and security-focused risk management program that includes maintenance of a register of security risks and related remediation. As appropriate, the members of Splunk's Executive Leadership Team and Board of Directors review entries. Splunk's Board of Directors has a Cybersecurity & Data Responsibility Committee specifically focused on these issues. Splunk maintains a comprehensive security program designed to protect the confidentiality, integrity and availability of customer data in accordance with the highest industry standards. Splunk Cloud has been certified by independent third-party auditors to meet the International Organization for Standardization's information security standard 27001 (ISO 27001) and both Splunk Cloud and Observability Cloud undergo annual Service Organization Controls 2 (SOC 2) Type II audits. For premium Splunk Cloud services, such as the PCI Data Security Standard (PCI DSS) service and Health Insurance Portability and Accountability Act (HIPAA) Security Rules and Health Information Technology for Economic and Clinical Health (HITECH) Breach Notification Requirements service, and for Observability Cloud services such as the Health Insurance Portability and Accountability Act (HIPAA) Security Rules service, Splunk maintains an internal audit compliance program and Splunk is audited annually to confirm its ongoing compliance. Splunk is UK Cyber Essentials (UKCE) and UK Cyber Essentials Plus (UKCE+) certified. Splunk employs a full-time Data Protection Officer (DPO) who is responsible for overseeing the processing of data at Splunk in compliance with applicable legal and regulatory requirements. The office of the DPO and Splunk's Government Affairs team maintain processes for nominating, tracking, and assessing proposed and pending legal and regulatory requirements, in order to anticipate and prepare for such requirements in advance.

Principle 5: Operational security

Services must be operated and managed in a way to impede, detect or prevent attacks.

Good operational security should not require complex, bureaucratic, time consuming or expensive processes. The aspects to consider are:

1. Vulnerability management
2. Protective monitoring
3. Incident management
4. Configuration and change management – the customer should ensure that changes to the system have been properly tested and authorised. Changes should not unexpectedly alter security properties

Principle 5.1: Vulnerability management

Principle Goals	Splunk's Response
Service providers should have a management process in place to identify, triage and mitigate vulnerabilities. Services which don't, will quickly become vulnerable to attack using publicly known methods and tools. **Goals** Customers should have confidence that: • Customers know the service provider's timescales for deploying security updates and other mitigations, and are happy with them • Cloud provider takes responsibility for applying security updates to all software and hardware, including where they rely on external dependencies (or a third-party supply chain) • Potential new threats, vulnerabilities, or exploitation techniques that could affect customer cloud service are proactively assessed and corrective action is taken Customers should prefer a provider that: • Attempts to identify vulnerabilities in off-the-shelf components used by the service deployed on top of the cloud platform • automatically applies mitigations	Splunk identifies, triages, and mitigates vulnerabilities through three aspects of its Global Security business unit: a Product Security organisation focused on secure development lifecycles and ongoing product security; a Security Assurance Program for keeping Splunk's products and infrastructure hardened, secure, and regularly tested for vulnerabilities; and a Security Operations Office for monitoring and responding to threats. For more on Splunk's Product Security functions, see Principle 7 (Secure development). Splunk's Security Assurance program incorporates a penetration testing program, threat and vulnerability management program, and an application security testing program. The Threat and Vulnerability Management program includes continuous monitoring for vulnerabilities that are acknowledged by vendors, reported by researchers, or discovered internally through penetration testing, static and dynamic application security testing, or otherwise by Splunk employees. Product security vulnerabilities can be reported here. Splunk issues quarterly Security Advisories at Splunk Product Security where customers can also sign up to receive RSS feeds of product security announcements. Splunk follows industry standard CVSS ratings of vulnerabilities and assigns appropriate CVE's to confirmed vulnerabilities. For more information about vulnerability practices, see Splunk's Responsible Disclosure Standards. For systems containing customer data, an external vendor conducts security penetration tests on the corporate and cloud environments at least annually to detect network and application security vulnerabilities. Critical and high-risk findings from these tests are evaluated, documented and assigned to the appropriate teams for remediation within planned timelines. In addition, Splunk conducts internal penetration tests periodically and remediates findings as appropriate. Splunk follows industry best practices to discover and remediate vulnerabilities before release. Splunk addresses vulnerabilities

	reported by third parties using a risk-based approach, which may include the following activities: • Promptly evaluating potential security vulnerabilities • Rating and prioritising confirmed vulnerabilities using CVSS • Assigning CVEs to confirmed security vulnerabilities • Issuing major/minor releases incorporating cumulative vulnerability fixes for critical-risk, high-impact vulnerabilities • Expediting maintenance releases for affected, supported versions

Principle 5.2: Protective monitoring

Principle Goals	Splunk's Response
The cloud provider should monitor for attacks, misuse, and malfunction to help it detect successful and unsuccessful attacks against the service as a whole, or the parts of the service that it runs on the customer's behalf. This will allow it to quickly respond to potential compromises of your environment and data. **Goals** Customers should have confidence that: • The service generates adequate audit events to support effective identification of suspicious activity • These events are analysed to identify potential compromises or inappropriate use of the customer's your service • The service provider takes prompt and appropriate action to address incident	Monitoring tools and services are used to monitor systems across Splunk, including Splunk Cloud and Observability Cloud, for application, infrastructure, network and storage events, and performance and utilisation. Event data is aggregated and stored using appropriate security measures aligned to Splunk's cloud certification program requirements (e.g., SOC2). Splunk's third-party certification reports detailing the relevant controls are available on demand through Splunk's Customer Trust Portal. Logs are stored in accordance with Splunk's data retention policy. Splunk Incident Command teams continuously review alerts and follow up on suspicious events as appropriate, following detailed incident response plans created and managed under the Splunk Incident Response Framework (SIRF). For more on incident management, see Principle 5.3 (Incident management), below.

Principle 5.3: Incident management

Principle Goals	Splunk's Response
The cloud provider should have **pre-planned incident management processes in place, to make it more**	The Splunk Incident Response Framework (SIRF) establishes the actions and procedures that help Splunk prepare for and respond to security incidents, including how to initiate responsive action,

likely that effective and prompt decisions are made when incidents occur. The processes needn't be complex or require large amounts of description, but good incident management will minimise the impact to users of security, reliability and environmental issues with a service. **Goals** Customers should have confidence that: • Incident management processes are in place for the service and are actively deployed in response to security incidents • Pre-defined processes are in place for responding to common types of incident and attack • A defined process and contact route exists for reporting of security incidents by consumers and external entities • Security incidents of relevance to the customer will be reported in acceptable timescales and formats	remediate any consequences, and document lessons learned for iteration and improvement of internal processes. Splunk tests its SIRF using a combination of planned reviews, live simulations (tabletop exercises) and periodic training. SIRF workflows and practices are also designed to tie into business continuity and disaster recovery (BC/DR) operations as necessary. Documentation on Splunk's BC/DR program is available to customers on demand through Splunk's Customer Trust Portal.

Principle 5.4: Configuration and change management

Principle Goals	Splunk's Response
The cloud provider should know what assets make up their service along with their configurations and dependencies, allowing them to identify and manage changes which could affect the security of the service and fully mitigate vulnerabilities that they are aware of. **Goals** Customer should be confident that: • The status, location and configuration of service components (both hardware and software) are tracked throughout their lifetime • Changes to the service are assessed for potential security impact, then managed and tracked through to completion	Splunk maintains an inventory of Splunk Cloud and Observability Cloud infrastructure assets that it regularly updates and reconciles. Documented, standard build procedures are used for installation and maintenance of production servers. Splunk follows documented change management procedures for application, infrastructure and product-related changes. Changes undergo review and testing, including security and code reviews, regression testing and user acceptance testing before approval for implementation. Splunk's protective security monitoring processes scan to detect any unauthorised changes to deployed service components and their configuration, and Splunk's incident management processes are designed to prevent any attempts to perform such unauthorised changes (see Principle 5.2 (Protective monitoring) and Principle 5.3 (Incident management) above). Splunk deploys changes during maintenance windows for Splunk Cloud, which are set forth in the relevant Maintenance Policy, and for

• Unauthorised changes to the deployed service components and their configuration will be detected and prevented • The cloud provider will give the customer appropriate notice before making changes that affect how the customer uses the service or ability to use the service	Observability Cloud, which are set forth in the relevant Maintenance Policy.

Principle 6: Personnel security

Audit and constrain the actions of service provider personnel.

Where service provider personnel have access to your data and systems, you need to have **enough confidence in their trustworthiness, and the technical measures in place that audit and constrain the actions of those personnel**.

Effective personnel controls should be a balance of:

- the provider demonstrating how they gain enough confidence in their people
- technical controls that minimise the likelihood and impact of accidental or malicious compromise by service provider personnel

Principle 6.1: people and security culture

Principle Goals	Splunk's Response
The cloud provider should subject personnel to security screening and regular security training. Personnel in these roles should understand their responsibilities. Providers should make clear how they screen and manage personnel within privileged roles. **Goals** Customers should be confident that: • The minimum number of people have access to the data, or could affect the use of the service • The provider has implemented a positive security culture across their organisation • the level of security screening conducted on service provider staff or contractors that have access to customer data, or have the ability to affect the service, is appropriate	As part of the onboarding process, Splunk personnel sign confidentiality agreements, acknowledge Splunk's Acceptable Use Policy, and are subject to criminal background and other verification checks in accordance with local laws and as appropriate for their role. New employees are required to complete security training as part of the new hire process. Thereafter, they receive annual training and targeted training (as needed and appropriate to their role) to help maintain compliance with Splunk's Security Policies, as well as other corporate policies, such as the Code of Conduct. Splunk conducts periodic security awareness campaigns, exercises, and tests to educate personnel about their responsibilities and provide guidance to create and maintain a secure workplace. Splunk scans corporate and cloud environments to detect for any internal security misconfigurations or other security policy, standard, or method misalignments, and monitors customer Splunk Cloud and Observability Cloud instances for both internal (including staff and contractors) and external threats.

Principle 6.2: technical controls for service administration

Principle Goals	Splunk's Response
Personnel security should combine background checks and procedural controls with technical measures designed to detect and minimise the impact of a malicious insider. **Goals** Customers should be confident that: ● An administrator accessing customer data, or making changes that affect the customer's use of the service, will be reliably logged and monitored ● Customers will be alerted if the cloud provider's personnel perform an action on the cloud service that could (accidentally or otherwise) expose them to customer data Customers should prefer a cloud provider that employs technical controls to reduce the likelihood of accidental or malicious compromise by cloud provider personnel. **Controls should include:** ● Administrators and privileged users are only given minimal administrative capabilities temporarily, in response to a specific issue (additional privileges should be requested when necessary) ● Requests for additional privileges are tied either to a customer support ticket, or an internal change request ● Access to systems or interfaces that could provide access to customer data is only granted if the customer has given explicit time-limited permission for that access (this applies on a case-by-case basis)	As stated in the Splunk Cloud Platform Security Addendum and the Splunk Observability Cloud Security Addendum, Splunk personnel sign confidentiality agreements, acknowledge Splunk's Acceptable Use Policy, undergo background verification checks, and participate in new-hire, annual, and role-specific security and Splunk Code of Business Conduct and Ethics training. Splunk access control procedures include access levels tied to job functions roles and to specific, limited purposes such as updating, securing, and troubleshooting our services; operating our business including by analysing the performance of our services, and maintaining legal compliance. Splunk employs documented access approval systems and procedures to regularly review access rights. For support cases, Splunk seeks and documents customer approval. Access is managed under the principle of "least privilege", using scoped/ephemeral access tokens, and requiring use of security Virtual Desktop Infrastructures (VDIs) with Data Loss Prevention (DLP) controls as needed. Splunk continuously logs and monitors access (including for insider threat scenarios) along with other key system activity to support security and availability monitoring of systems and services, on a 24x7 basis. See Principle 5.2 (Protective monitoring), above. Automated alerts of detected intrusion/access attempts trigger investigations and incident management procedures as needed. See Principle 5.3 (Incident management), above. **Further reading** ● Splunk Cloud Platform Privacy and Security Fact Sheet

Principle 7: Secure development

Principle Goals	Splunk's Response
Cloud services should be designed, developed and deployed in a way that minimises and mitigates threats to their security. Cloud services which aren't designed, developed, and deployed in a secure way may be vulnerable to security issues which could compromise your data, cause loss of service, or enable other malicious activity. **Goals** Customers should be sufficiently confident that: ● The provider uses a software development lifecycle in line with NCSC secure software development and deployment guidance, at a standard appropriate for the sensitivity of the data ● The provider has built a culture of secure development, including secure development training, code review of all deployed changes, and curation of well-understood libraries for solving security-critical problems ● The provider automates the integration and deployment pipeline used to deliver their cloud services, to enforce security, consistency, and a detailed audit trail ● The provider clearly separates their production environment from testing or development environments ● The provider risk-manages the supply chain of internal and third-party software libraries used in their code, only using supported external software ● The provider monitors the external software's security advisories and pulls in any security fixes promptly ● Configuration and secrets management processes are in place to ensure the integrity of	Splunk's Software Development Life Cycle (SDLC) methodology governs the acquisition, development, implementation, configuration, maintenance, modification, and management of software components. For major and minor product releases, Splunk uses a risk-based approach when applying its standard SDLC methodology, which includes such things as performing security architecture reviews, open source security scans, code review, static and dynamic application security testing, network vulnerability scans, and external penetration testing. Splunk scans packaged software to ensure it is free from trojans, viruses, malware, and other malicious threats. Splunk trains its relevant personnel on secure development. Splunk performs security code review for critical features if needed and performs code review for all features in the development environment. Splunk utilises a code versioning control system to maintain the integrity and security of application source code. Privileged access to the source code repository is reviewed periodically and limited to authorised employees. Splunk logically separates environments used for development and testing from production environments. For further information, see the Splunk Cloud Platform Security Addendum and the Splunk Observability Cloud Security Addendum. For more on vulnerability management, see Splunk's response to Principle 5.1 (Vulnerability management), above. For supply chain security, see Splunk's response to Principle 8 (Supply chain security), below.

the cloud service throughout development, testing and deployment • The provider maintains their services over time and responds to new and evolving threats	

Principle 8: Supply chain security

Principle Goals	Splunk's Response
Third party supply chains should support all of the security principles which the service claims to implement. Cloud services rely upon third party products and services. Consequently, if this principle is not implemented, supply chain compromise can undermine the security of the service and affect the implementation of other security principles. **Goals** Customers should be sufficiently confident that they understand: • How customer data is shared with (or made accessible to) third party suppliers and their supply chains, including the circumstances under which that data is shared • Which customer data, and metadata derived from that data, is shared with, or made accessible to third party supplies and their supply chains • How the service provider's hardware and software procurement processes place security requirements on third party suppliers • How the service provider manages security risks from third party suppliers • How the service provider manages the conformance of their suppliers with security requirements	**Vendor Risk Management** Splunk relies on vendors to provide different aspects of the Splunk Cloud and Observability Cloud services, including such things as: • Bug reporting • Customer billing and accounting • Data analytics • Enterprise services • Infrastructure-as-a-Service • IT infrastructure and data centre solution services • Mobile analytics • Staffing and support services • Technical support services A complete list of Splunk's sub-processors that process personal data may be found here. Customers may sign up to receive notifications about changes to Splunk's sub-processor list here. 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 align them with Splunk's security, legal and regulatory obligations. Vendors are evaluated prior to onboarding. Identified security risks are managed through Splunk's risk management program. Vendors must pass a robust vetting process that is calibrated to the services provided and the sensitivity of the data involved. It may include such things as a review of features and functionality from a security and privacy perspective, assessments of security and privacy program maturity, review of data elements processed, location of processing activities, data security in transit and at rest, data sharing ecosystems, etc. Annual reassessments are performed for certain high-risk vendors. Reassessments are also performed when there is a material change in the vendor's data processing activities. Additionally, key vendors are queried in the face of identified material threats and vulnerabilities.

	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. Splunk's agreements with vendors impose security and privacy obligations on them that are necessary for Splunk to maintain its security posture for Splunk products and services, and hold vendors to the Splunk Supplier Code of Conduct. **Further Reading** • Splunk Offerings Sub-processor list • Splunk Cloud Platform Security Addendum • Splunk Observability Cloud Security Addendum • Splunk Protects • Splunk Cloud Platform Privacy and Security Fact Sheet

Principle 9: Secure user management

Principle Goals	Splunk's Response
Cloud providers should make the tools available to securely manage access to their service. Cloud providers should make the tools available for customers to securely manage customer access to their services, preventing unauthorised access and alteration of customer resources, applications, and data. **Goals** Customers should be sufficiently confident that: • There is a single, well-defined user account model • The customer understands the mechanisms used to authorise access to customer data and services, including accesses to management interfaces • The customer is aware of all of the mechanisms by which the cloud provider would accept management or support requests from the customer (telephone, web portal, email etc.) • The customer can apply granular access control, according to the 'principle of least privilege', enabling both 'standard' and 'administrative' user accounts	Currently, Splunk Cloud supports using authentication tokens in Splunk Cloud with the Microsoft Azure and Okta Security Assertion Markup Language (SAML) identity providers (IdPs), as well as other providers that support attribute query requests (AQR); these methods let Splunk Cloud retrieve information about users directly from the IdP. When customers configure Splunk Cloud to use SAML as an authentication scheme, customers let Splunk Cloud query these IdPs to confirm that tokens customers create in Splunk Cloud for authentication are valid. Splunk Cloud also supports authentication tokens when it uses either the native or Lightweight Directory Access Protocol (LDAP) authentication schemes. For more about authentication tokens, how they work, and how customers enable or disable them individually or globally, see Set up authentication with tokens. In Splunk Cloud, customers can use role based user access. This way, they can determine what permissions and capabilities users have through the roles that they hold. Observability Cloud supports using team access restrictions, limited tokens, and customised permissions for detectors, dashboard groups, and dashboards to reinforce security. See Authentication and Security for more details. Observability Cloud lets customers restrict access to certain features to specific groups of users using role-based access control. Customers can assign roles to users.

• Other customers cannot access, modify or otherwise affect other customer's service configuration **Customers should prefer a cloud provider that:** • Makes access control easy to manage at scale, throughout the customer's organisation • Makes it easy to see the access permissions applied to all resources • Uses one access control mechanism for all authorisation decisions • Helps the customer to remove permissions that are not being used • Lets the customer apply time-bounded permissions for highly privileged accesses	

Principle 10: Identity and authentication

Principle Goals	Splunk's Response
Access to service interfaces should be constrained to authenticated and authorised individuals. Services and data should only be accessible to an authenticated and authorised identity, which may be either a user or a service identity. To apply effective access control as described in Principle 9: secure user management, you must have confidence in the authentication method used to determine the identity performing the access. Weak authentication to these interfaces may enable unauthorised access to your systems, resulting in the theft or modification of your data, changes to your service, or a denial of service. Importantly, authentication should occur over secure channels, as described in Principle 1: data in transit protection. **Goals**	**Users and Authentication** Splunk customers can configure account policies that require unique usernames, minimum password length, and regular password resets. Customers are responsible for creating and administering user accounts, the roles assigned to them, the authentication method they use, and the global password policies that apply. Role based access settings can also be applied to restrict access to specific capabilities, indices and resources. "Roles" give Splunk Cloud and Observability Cloud users access to features in the service, and permission to perform tasks and searches. Each user account is assigned one or more roles. Splunk uses the Admin role and system user roles to perform essential monitoring, maintenance, and security activities, as well as any agreed support and professional services activities. These activities are performed in accordance with a comprehensive security program designed to protect the confidentiality, security and availability of customer data in accordance with high industry standards. Splunk Cloud has been certified by independent third-party auditors to meet SOC2 Type II and ISO 27001 security standards; Observability Cloud is audited to SOC2 Type II security standards. See Splunk Cloud and Observability Cloud compliance and certifications for more information. As noted in Principle 9 (Secure user management) above, user accounts can be authenticated using Identity Providers (IdP) such as LDAP and AD. Splunk Cloud and Observability Cloud support SAML authentication for SSO. Depending on the version and IdP, token based authentication is supported.

Customers should be sufficiently confident that: • It is understood how access to external interfaces is authenticated • The cloud provider has a modern password policy and requires multi-factor authentication (MFA) for user accesses • The cloud provider performs equally robust authentication of service identities as it does for users • Authentication of users will integrate with existing processes for managing joiners, movers, and leavers • Processes are available for managing the lifecycle of service credentials **Customers should prefer a cloud provider that:** • takes active measures to identify and revoke breached credentials • gives users of the service confidence that they are connecting to the authentic service • prompts administrators to re-verify themselves using MFA when performing high privilege actions	**Further Reading** • Manage Splunk Cloud users and roles • Configure SAML single sign-on (SSO) to Splunk Cloud • Securing Splunk Cloud • Splunk Cloud Platform Service Details • Splunk Cloud SOC 2 Type II (available via the Splunk Customer Trust Portal) • Manage users and teams (Splunk Observability Cloud) • About SSO integrations for Splunk Observability Cloud • Create and manage authentication tokens using Splunk Observability Cloud • Splunk Observability Cloud service description • Observability Cloud SOC 2 Type II (available via the Splunk Customer Trust Portal)

Principle 11: External interface protection

Principle Goals	Splunk's Response
All external or less trusted interfaces to the service should be identified and defended. Defensive measures may include application programming interfaces (APIs), web consoles, command line interfaces (CLIs), or direct connect services. Also, the cloud provider's administration interfaces, the interfaces you use to access the service, and any interfaces to your services built on top of the cloud service. If some of the interfaces exposed are private (such as management interfaces) then the impact of compromise may be	Splunk Cloud and Observability Cloud user interfaces are accessible via the internet but access is controlled as set forth in Principle 9 (Secure user management) above. Additionally, for details about protection of customer data sent to Splunk, monitoring for application, infrastructure, network and storage events, and user authentication, see Splunk's response to Principes 1 (Data in transit protection), 5.2 (Protective monitoring), and 10 (Identity and authentication) above, respectively. **Further Reading** • Splunk Cloud SOC 2 Type II (available via the Splunk Customer Trust Portal) • Observability Cloud SOC 2 Type II (available via the Splunk Customer Trust Portal)

more significant. You can use different models to connect to cloud services which expose your enterprise systems to varying levels of risk. **Goals** Customers should be sufficiently confident that: • It is understood what physical and logical interfaces to customer information exist, and how access to customer data is controlled • The service identifies and authenticates users to an appropriate level over those interfaces (as described in Principle 10) **Customers should prefer a cloud provider that:** • Shows the customer which interfaces or services are exposed to the internet, highlighting those exposed without authentication • Makes it easy to understand which defences are in place to protect each external interface to customer data or customer use of the service • Provides easy to use defences against common attacks for the interfaces and components customers use to build their services	

Principle 12: Secure service administration

Principle Goals	Splunk's Response
Cloud providers should recognise the high value of administration systems. The design, implementation, and management of the cloud provider's administration systems used by the customer cloud provider should follow enterprise good practice, whilst recognising their high value to attackers. Systems used by the vendor for administration of their cloud services will	Splunk thoroughly assesses critical systems before they are integrated into our SDLC environments. This evaluation ensures that only systems with robust security measures in place are onboarded into our development environment. Post-onboarding, Splunk's dedicated security teams continuously scan these systems for any new vulnerabilities. This ongoing vigilance allows for immediate detection and remediation of identified security issues, thereby maintaining the integrity of our development process. Critical systems integrated into our SDLC are designed to generate detailed audit events. These events provide a granular view of all

have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data. **Goals** **Customers should be sufficiently confident that the cloud provider:** • Builds and maintains trust in the devices it uses to administer the service, with regular and thorough, security assessments • Protects its administration interfaces • Risk-manages its administration using tiers • Uses privilege access management, including 'just in time' and 'just enough' administration • Uses administration interfaces that produce detailed audit information, which is checked regularly for anomalous or unexpected behaviour **Customers should prefer a cloud provider that:** • Uses layered controls and processes to manage service administration, avoiding the browse-up anti-pattern	activities undertaken by its privileged and regular users and help identify potential security anomalies. Splunk Cloud logs are stored in a secure location with limited access controlled by logical access controls. Access is restricted to administrators who do not have the ability to delete or modify logs. Logs are reconciled against the inventory of in-scope devices, and alerts are configured in the event of log failure. Administrative access privileges to Splunk Cloud systems are restricted to user accounts accessible by authorised personnel. Prior to issuing system credentials and granting Splunk Cloud system access for new users whose accounts are administered by Splunk are registered and authorised. Administrative access privileges to Splunk Cloud are restricted to user accounts accessible by authorised personnel. For Observability Cloud, administrative access to production environments (including VPN, AWS and GCP management consoles, application and database servers, databases, and the production access provisioning tool) are restricted to authorised individuals with demonstrated need. Administrative access privileges to Observability Cloud systems are restricted to user accounts accessible by authorised personnel. Prior to issuing system credentials and granting Observability Cloud system access for new users whose accounts are administered by Splunk are registered and authorised. Administrative access privileges to Observability Cloud are restricted to user accounts accessible by authorised personnel. **Further Reading** • Splunk Protects • Specific Terms for Splunk Offerings • Splunk Cloud Platform Security Addendum • Splunk Cloud SOC 2 Type II (available via the Splunk Customer Trust Portal) • Splunk Cloud User Manual: Administer Splunk Cloud • Splunk Observability Cloud Security Addendum • Administer Splunk Observability Cloud • Observability Cloud SOC 2 Type II (available via the Splunk Customer Trust Portal)

Principle 13: Audit information and alerting for customers

Providers should supply logs needed to monitor access to your service, and the data held within it.

Customers should be able to identify security incidents and should have the information necessary to determine how and when they occurred.

This will require:
- audit information
- security alerts

Principle 13.1: audit information

Principle Goals	Splunk's Response
Goals	**Logging and Monitoring**

Customers should be provided with the audit data needed to investigate incidents related to use of the service and the data held within it. The type of audit information available to the customer will have a direct impact on the customers ability to respond to inappropriate or malicious activity within reasonable timescales. **Customers should be sufficiently confident that:** • They are aware of the audit information that will be provided, how, and when it will be made available, the format of the data, and the retention period associated with it • The audit information available will meet the customer's needs for investigating misuse or incidents • The cloud provider will supply relevant audit information for actions taken by its personnel that affect the customer's service (or the data held within it) • Audit information cannot be deleted by the customer or the cloud provider during a defined retention period **The customer should prefer a cloud provider that:** • Either enables all audit information services by default, or makes them easy to enable • Provides APIs and tooling to query, process, and archive audit information • Implements a RBAC role for auditors to review logs without needing wider privileges	Splunk uses monitoring tools and services, including Splunk's own security and observability products and services such as Splunk Cloud and Observability Cloud, to monitor systems across Splunk Cloud and Observability Cloud for application, infrastructure, network and storage events, performance and utilisation. Event data is aggregated and stored using appropriate security measures designed to prevent tampering, and logs are stored in accordance with Splunk's data retention policy. The Splunk Global Security team reviews alerts and follows up on suspicious events as appropriate. Customers may also use Splunk Cloud and Observability Cloud to investigate incidents themselves. **Further Reading** • Splunk Admin Manual • Splunk Cloud Monitoring Console (CMC) Release Notes • Use Splunk Enterprise to Audit Your System Activity • Audit Splunk Activity • Search for Audit Events • Set up and administer Splunk Observability Cloud

Principle 13.2: security alerts

Principle Goals	Splunk's Response
Goals **Customers should be provided with alerts when the cloud provider detects attacks against your data, or your use of their services.** The cloud provider should be your first line of defence for identifying and preventing common attacks.	As noted above, Splunk uses monitoring tools and services, including Splunk's own security and observability products and services such as Splunk Cloud and Observability Cloud, to monitor systems across Splunk Cloud and Observability Cloud for attacks against data. The Splunk Global Security team reviews alerts and follows up on suspicious events as appropriate. Splunk notifies customers of security breaches leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to customer data in accordance with applicable laws and regulations and with the terms of

The customer should be sufficiently confident that: • The cloud provider will alert you when they identify attacks against, or vulnerabilities in, the customers' use of their services • The cloud provider will alert the customer when the cloud provider detects attempted or successful compromise of customer data held in the cloud provider's services • The cloud provider will send their alerts promptly to a recipient of the customer's choosing, through an automated means The customer should prefer a cloud provider that: • Will alert the customer when their configuration of cloud provider's services results in security issues • Will make it easy to receive and respond to alerts automatically	the Spunk Cloud and Observability Cloud Security Addenda or as otherwise agreed between Splunk and customers. Customers may select recipients to receive such security notices through the Splunk Support Portal. Splunk also maintains a Responsible Disclosure Program that includes notifications of security issues including vulnerabilities. Customers may use Splunk Cloud and Observability Cloud to alert themselves of suspicious events themselves. **Further Reading** • Splunk Admin Manual • Alerting Manual • Set up and administer Splunk Observability Cloud • Send alert notifications to third-party services using Splunk Observability Cloud

Principle 14: Secure use of the service

Cloud providers should make it easy for customers to adequately protect their data.

The cloud provider should make it easy for customers to meet their responsibilities to adequately protect customer data.

Customers should consider:

- Whether the service is secure by design and by default
- **What help the provider gives you to meet your responsibilities**

Principle 14.1: Security by design and by default

Principle Goals	Splunk's Response
Goals The cloud provider should make it easy for customers to use their services in a way that is defended against common attacks. **The customer should be sufficiently confident that:** • It is known which goals from Principles 1-13 are met by the cloud provider's default configuration	Splunk Cloud offers an array of security configurations, as does Observability Cloud, to configure access. Each cloud service secures and encrypts customer configurations and data ingestion points using industry-standard encryption algorithms. Customers are responsible for selecting the desired security configurations and options provided by Splunk, and may elect to take additional measures to achieve the level of security they require. In the case of Splunk Cloud, we have also developed a roadmap for customers to follow to help secure their configurations.

• It is known what the customer needs to do to the cloud provider's configuration to meet the remaining goals • Data and services are not accessible to unauthenticated users, by default • The cloud provider takes responsibility for improving their service's default configuration, to respond to new threats (this may include altering the configuration of existing customers, as well as changing the starting point for new customers) **The customer should prefer a cloud provider that:** • Meets all of the goals described in Principles 1-13 by design, or in its default configuration • Makes configurable security-enhancing features opt-out, and not opt-in • Defends against common network-based attacks (such as DDoS) against the service and your hosted workloads by default, as described in Principle 11: external interface protection	

Principle 14.2: Help customers meet their security responsibilities

Principle Goals	Splunk's Response
Goals Customers should be confident that: • All service configuration can be set and audited using infrastructure as code, or via an API • There is a single place where the customer can see all deployed resources across all services and regions offered by that cloud platform • All service configurations are visible and intuitive to humans, so that they can easily audit what services they are using, where	Splunk Cloud customers can use the Admin Config Service (ACS) API to administer their service, including setting configurations and managing their service. Customers can see the knowledge objects within their deployment using the **All configurations** settings menu from Splunk web. Other resources such as indexes and data inputs can also be seen from their respective settings menu in the same Splunk web console. Observability Cloud customers can use various APIs to administer their service, including setting configurations and managing their service. Customers can see various deployment details for their Observability Cloud service. If a customer has multiple Splunk products they will need to use the Splunk Log Observer Connect Observability Cloud product to view and search data across those resources. Various dashboards offered by Splunk enable customers to audit the security and integrity of their data in Splunk Cloud.

their data is, and how those services are configured	**Further Reading** • Splunk Admin Manual • Splunk Cloud Monitoring Console (CMC) Release Notes • Use Splunk Enterprise to Audit Your System Activity • Audit Splunk Activity • Search for Audit Events • Set up and administer Splunk Observability Cloud

Conclusion

This document has provided detailed responses to each of the principles and goals defined by the UK government Cloud Security Principles. This is intended to illustrate how the Splunk Cloud and Observability Cloud service offerings meet or exceed the requirements for cloud service adoption by the UK public sector.