Splunk and Financial Services Customers

White Paper | May 2024

Splunk and Resilience for Customers in the Financial Services Sector

Splunk's real-time analytics platform and related services allow customers to monitor, search, analyze and visualize large volumes of **technology infrastructure data**. Splunk's financial services customers use our products and services to help improve their resilience profiles: customers can use our services to proactively identify and mitigate threats, performance issues, and outages. The output of Splunk's offerings provide customers with valuable insights on how to improve the resilience of their technology infrastructure. Splunk's offerings differ from those of some other cloud or SaaS vendors that may host or process enterprise data for customers, as Splunk's offerings instead enable our customers to **understand *machine operational information*** generated by customers' use of those vendors' systems and by customer's own technology infrastructure.

Splunk's approach to Financial Services Regulations

Splunk recognizes that our financial services customers are subject to increasingly prescriptive rules and regulations applicable to outsourcing, cloud services, and third-party risk management, such as the EBA Guidelines on Outsourcing Arrangements, EU's Digital Resilience Act (DORA) or the UK's Critical Third Party Supervision regime (CTP), and similar requirements from the United States, Canada, Australia, Singapore, and Japan. There are differing approaches between national and supra-governmental regulators in key financial markets, but a common thread in all is recognizing an increased reliance by financial services customers on technology vendors and outsourced service providers. The regulations are therefore broadly aligned to ensure that financial services customers can rely on these vendors and service providers, while still discharging their regulatory responsibilities, protecting the interests of their own clients, and ensuring the stability of financial markets and consumers.

We understand that financial services customers need to maintain a common compliance posture across their technology vendors and outsourced service providers. In this White Paper, we provide insight into how Splunk addresses the specific obligations imposed on our financial services customers relating to outsourcing and cloud services. The list of regulations that Splunk has considered when building its financial services program is annexed to this document. Additional rules relating to data protection requirements are addressed in the Splunk Privacy Fact Sheet and the Splunk White Paper and FAQ: EU Cross-Border Transfers, and those should be reviewed in conjunction with this White Paper.

Table of Contents

1. Security and Compliance with Global Industry Standards

Splunk maintains appropriate technical and organizational measures, and proactively manages risks in relation to our offerings. Splunk has developed a common controls framework that takes into account multiple recognized global and industry compliance frameworks and that map to our policies, procedures and standards. We continuously review and evolve our security profile. Customers can find more information on Splunk's commitments to global and industry compliance standards at: Compliance at Splunk.

Our Customer Trust Portal contains supporting documentation on the above framework. Specifically, it includes information on how Splunk helps our customers satisfy their regulatory compliance requirements by providing assurance in relation to alignment of Splunk's offerings with recognized industry standards, as audited by independent third parties, including:

- ISO/IEC 27001
- SOC2 Type II
- PCI-DSS
- HIPAA
- FedRAMP [moderate]
- FIPS 140-2 Certification

Our measures include administrative, technical, and organizational safeguards and controls to protect customer data against destruction, loss, alteration, or unauthorized disclosure or access. In terms of administrative and organizational controls, we maintain information security policies and procedures and conduct ongoing security awareness training. We have also developed and continue to maintain and update a threat and vulnerability management program, including threat-led penetration testing (TLPT), incident response framework, and third party (vendor) risk management program. Splunk's employees are trained and tested at regular intervals on these topics. Further information can be found at: Corporate Security at Splunk.

Details of our approach to product security, both on-prem and in the cloud, including access controls, authentication, data obfuscation, segregation and encryption, threat and vulnerability management, intrusion detection and incident response, can be found at: Product Security at Splunk and Cloud Security at Splunk.

Splunk engages independent third parties to conduct penetration tests to ensure that we receive an objective and accurate report of security systems and possible areas of improvement. Redacted penetration testing affirmation letters are available to existing customers under NDA.

Splunk supports financial entities in pooled testing with an independent, industry-recognized vendor to perform threat-led penetration tests to proactively test against the most critical and immediate cyberthreats that may occur. Splunk has a robust system of identifying such threats based on publicly available information, our own experiences and expertise, and other sources.

In addition to technical and organizational measures, Splunk also offers contractual measures to our customers. We integrate these concepts into our agreements, including the Information Security Addendum, Splunk Cloud Platform Security Addendum, and Splunk Observability Security Addendum.

2. Business Continuity and Resilience

Splunk maintains an enterprise-level business continuity and disaster recovery program, framed by our Business Continuity (BC) and Disaster Recovery (DR) Management Policy and related Standard. The BC/DR Policy and Standard detail how Splunk manages our program, reflects best practices, and is aligned with industry standards.

To ensure the BC/DR Policy and Standard continue meeting Splunk's objectives, Splunk periodically conducts business impact analyses across our business units to identify our critical business functions. Identified owners of our critical business functions then develop function-specific BC/DR plans setting out processes and procedures for continuing and/or recovering operations, systems, and data.

Our BC/DR Policy and Standard, as well as function-specific BC/DR plans, are reviewed and updated on a regular basis for ongoing relevance. They are also tested at least annually for effectiveness (including recovery timeframes (RTO) and recovery points (RPO)), and Splunk personnel are trained on them regularly as well.

The goal of these plans and ongoing efforts is to minimize potential interruptions to our critical business functions (and those of our subcontractors which support these functions), in particular those that may impact the availability of our offerings to customers. Customers can access Splunk's current BC/DR Policy and Standard, as well as BC/DR testing attestations, via our Customer Trust Portal.

Splunk's resilience profile is further bolstered by our backup policies and practices. For Splunk Cloud, Splunk Observability, and Splunk Intelligence Management, those backup policies and practices are assessed annually against SOC2 Type II. Customers may view the detailed SOC2 Reports, which provide further details and confirmation of the backup policies and descriptions of relevant controls used to maintain them, via our Customer Trust Portal.

3. Ethics, Compliance and Corporate Responsibility

As a global company, employer, and good corporate citizen, Splunk is committed to our ethical and legal responsibilities, as well as giving consideration to

societal and environmental issues, including governance thereof.

Splunk's commitments and requirements in respect of business conduct and ethics are detailed in the Splunk Code of Conduct and Ethics. Our Legal Resources and Policies site links to information and policies on compliance topics such as export controls, anti-slavery commitments, privacy, and intellectual property. Splunk's environmental and social positions and related governance program are described at our Global Impact site.

4. Subcontracting

While responsibility for the delivery of Splunk's offerings remains with Splunk, Splunk engages subcontractors to support and provision the Splunk's offerings. A list of subcontractors is included in Splunk's Financial Services Addendum. Splunk also posts and regularly updates our list of subcontractors at: Splunk Offerings Sub-processors.

Customers can register on Splunk's notification portal to receive email updates on changes to existing sub-processors and subcontractors and this process enables customers to maintain visibility and oversight of Splunk's supply chain, in line with EBA Outsourcing Guidelines, GDPR and DORA. Customers are given rights to object to the use of a new sub-processor or subcontractor in connection with customers' use of Splunk's offerings by using the process described in Splunk's Financial Services Addendum.

Splunk maintains appropriate oversight of our subcontractors through our third-party vendor management program, which include (a) securing contracts with each subcontractor that include the flow-down of key obligations including geographic location, integrity, security, privacy, and confidentiality, (b) assessment/ audit rights over subcontractors to allow Splunk to continuously monitor and manage those subcontractors' compliance with Splunk's requirements and evaluate any associated risks, and (c) ensuring that our subcontractors comply with our values and meet our expectations in terms of ethical and legally responsible business by requiring them to abide by our Supplier Code of Conduct.

5. Pre-Sales Assessments; Performance Management and Monitoring

Splunk assists financial services customers in meeting their obligation to manage and monitor the performance of our vendors in three ways:
(a) In the pre-contracting phase, customers may conduct assessments. This includes reviewing the documentation posted on Splunk's website such as Splunk Protects, which features information on our privacy, security, compliance, and accessibility posture, and in our Customer Trust Portal, which houses our compliance certifications, reports and attestations, and standard questionnaires on topics such as security and accessibility. If necessary, Splunk is also available to answer reasonable requests for information.

(b) During the course of the business relationship, Splunk keeps customers informed of our performance in various ways. For example, Splunk agrees to qualitative and quantitative service levels which are specific to the Offerings as well as associated service credits, as posted online (see the Splunk Cloud Service Level Schedule as an example) or otherwise made available to customers. Customers may also view posted system status (availability) information on our cloud-based offerings and subscribe to have such information emailed to designated customer representatives. By subscribing for these alerts, customers will be alerted when Splunk performs service updates and routine maintenance tasks on cloud-based offerings, with information on what is being updated and why, with workable windows scheduled with customers as needed. Please see Splunk Cloud maintenance information for an example of how Splunk works with customers on maintenance windows. Customers are also informed of updates and fixes to our cloud-based offerings in release notes published in Splunk Documentation (for example, release notes for the Splunk Cloud Platform).

(c) Finally, Splunk ensures customers are promptly notified of urgent issues that could impact the performance of our services to customers during the business relationship. For example, customers may view security advisories regarding product vulnerabilities and our remediations or recommendations for customer actions to reduce risk. Customers may also subscribe to be informed of such advisories, as well as request periodic updates as part of Splunk's support programs. In the case of security incidents or incidents impacting customers or customer data unavailability, loss, or misdirection, Splunk sends prompt email notices as contractually and legally required to the "Security Contacts" designated by the customer in the Splunk Support Portal.

6. Customer Audit Program

Customers may verify that Splunk continues to maintain the standards Splunk commits to in our contracts with customers via periodic audits under Splunk's Customer Audit Program. After customers have purchased and implemented our services, Splunk offers 3 audit options to customers, based on their needs, as follows:

(a) Basic Audit: The Basic Audit is document-based only, and is available at no cost to customers. This includes access to updated versions of documents reviewed during the pre-sales assessment cycle, as well as additional, more sensitive documents (such as third-party compliance certificates) that may not have been available before customers entered into an active order for services from Splunk. The more sensitive type of documentation is also available in our Customer Trust Portal for customers who have secured audit rights.

(b) Enhanced Audit: The Enhanced Audit option is for customers with questions about Splunk's audit

documentation, or for customers that need additional or non-standard questionnaires completed outside of the pre-sales assessment process or outside an annual cadence. For this option, customers can engage assistance from Splunk at then-current daily rates. Customers should contact their sales representative if they wish to request Enhanced Audit services from Splunk.

(c) Comprehensive Audit: Comprehensive Audits can be requested only once a year. For this option, customers may engage Splunk for up to three days at the then-current package rate, for live reviews of Splunk's documentation available under the Basic Audit, as well as to review more sensitive documentation that Splunk does not post on our Customer Trust Portal for security or confidentiality reasons. This option is for those customers that require a more formal and comprehensive confirmation of the adequacy of Splunk's security posture and internal policies or procedures (for example, to review internal reports that confirm Splunk completes periodic operations like employment verifications and background checks, or to understand in more depth Splunk's risk management system and how we undertake tracking of risks, risk-scoring, and closing of risk tickets). Comprehensive Audits also allow for standard regulator-required or regulator-involved audits (excluding on-site visits directed by regulators in exigent circumstances). Customers should contact their sales representative if they wish to request Comprehensive Audit services from Splunk.

Unlike pre-sales assessments, Splunk incorporates a post-audit remediation consideration process as part of Enhanced and Comprehensive Audits.

7. Termination; Exit Assistance

Splunk grants financial services customers early termination rights in certain circumstances and our Financial Service Addendum takes into account specific requirements of competent regulatory authorities. To reduce any undue impacts on our customers' operations, Splunk has defined processes to facilitate migration of customer data and to minimize the risk of disruptions to customers' operations. At any time, including for thirty (30) days following the expiry or termination of subscriptions, customers may retrieve, delete, or migrate their data that had been ingested into our cloud-based offerings, in accordance with published Splunk Documentation (for example, for Splunk Cloud and for Splunk Observability Cloud).
Customers requiring assistance with retrieving, deleting, or migrating their ingested data may make requests for assistance from Splunk's professional services team, subject to an agreed Statement of Work, at the then-current professional services rates, and in accordance with the exit assistance arrangements which we make available in jurisdictions where required, for our offerings which support critical or important functions.

8. Recovery and Resolution

Some financial services customers are subject to regulations which are designed to ensure the stability of financial markets and customers, in the event of a failure or potential failure of a financial institution. For customers who are subject to these requirements, Splunk understands that regulators or other appointees may exercise certain powers to ensure the ongoing viability of the institution or to affect an orderly wind down. To address these scenarios, Splunk offers a number of reassurances in our Financial Services Addendum, including: (a) Splunk recognizing the power of resolution authorities, and confirming our willingness to reasonably cooperate with such authorities, and (b) Splunk suspending any termination rights that might otherwise be triggered in such circumstances, provided Splunk continues to be paid for our services.

Disclaimer:

Annex

Regulations applicable to Financial Services Customers based on which Splunk has established our programs

- **European Union** Digital Operational Resilience Act (**DORA**) Regulation (EU) 2022/2554
- European Banking Authority (**EBA**) Outsourcing Guidelines 2019
- **European Union MiFID II** Organisation Regulation (Articles 30 and 31)
- **Bank of England** Prudential Regulation Authority (**PRA**) Supervisory Statements on Outsourcing and third-party risk (**SS2/21**) and Operational Resilience (**SS1/21**)
- **European Union Solvency II Directiv**e
- **European** Insurance and Occupational Pensions Authority (**EIOPA**) Guidelines on Outsourcing to Cloud Service Providers (with respect to insurance and re-insurance undertakings)
- Guidance issued by the **United States** Federal Banking Regulators (OCC, FDIC, and Federal Reserve) and Federal Financial Institutions Examination Council (FFIEC) on outsourcing and third-party risk
- Monetary Authority of **Singapore** (**MAS**) Outsourcing Guidelines 2018
- **Canada** Office of the Superintendent of Financial Institutions (**OFSI**) Third-Party Risk Management Guidelines (revised B-10)
- **Australian** Prudential Regulation Authority (**APRA**) Prudential Standard CPS 231 (outsourcing) and CPS 234 (Information security)
- Financial Services Agency of **Japan** (**JFSA**) Comprehensive Guidelines for the supervision of major banks and other FSIs