Splunk Data Platform – Cloud Software - SaaS

Service Overview

The Splunk Data Platform is a cloud-based software platform that enables organisations to ingest, index, search, analyse, and visualise machine-generated data from across their digital environments. Delivered as licensed cloud software, the platform provides scalable data analytics, observability, and security capabilities without the need for on-premise infrastructure.

The platform supports a wide range of operational, security, and business use cases by enabling users to collect and analyse data from applications, infrastructure, networks, and cloud services through configurable ingestion and processing capabilities.

Platform Capabilities

- Cloud-hosted ingestion of structured and unstructured data from multiple sources
- Indexing and storage of high-volume data streams
- Search, query, and correlation capabilities across datasets
- Real-time and historical analytics
- Configurable dashboards, visualisations, and reports
- Alerting based on defined thresholds and conditions
- Support for observability, security monitoring, operational intelligence use cases and IoT/OT integration with Splunk's Edge Hub

Data Ingestion & Processing

- Support for ingestion of log, metric, event, and trace data
- Configurable data parsing, enrichment, and transformation capabilities
- Support for common data sources, protocols, and integrations
- Management of data routing and indexing through platform configuration
- Controls to manage data volume, retention, and indexing behaviour

User Access & Administration

- Web-based access via standard browsers
- Role-based access control (RBAC) to manage user permissions
- Support for integration with identity providers for authentication
- Administrative controls for managing users, roles, and platform configuration

Security & Compliance

- Encryption of data in transit and at rest
- Logical tenant separation within the cloud platform
- Configurable access controls and audit logging
- Support for UK GDPR-aligned data handling requirements
- Data residency options subject to selected deployment region

Support for Integrations & Extensions

- Support for integration with third-party platforms and tools
- APIs and supported connectors to enable data exchange
- Ability to deploy and use supported apps and extensions from the Splunk ecosystem

Development of bespoke integrations or custom applications is not included as part of the software licence and is delivered separately where required.

What the Software Enables

- Centralised visibility of operational and security data
- Improved detection and investigation of incidents and anomalies
- Scalable analytics without managing underlying infrastructure
- Configurable insights aligned to organisational requirements
- Consistent application of access controls and governance policies

How the Software Is Used

The Splunk Data Platform is used by organisations that require a cloud-based solution to analyse and gain insight from machine-generated data. Users access the platform through a web interface to configure data ingestion, perform searches, build dashboards, and monitor alerts, using licensed functionality appropriate to their operational and analytical needs.