Networkology Ltd

Splunk Enterprise

Splunk Enterprise monitors and analyses machine data from any source to deliver Operational Intelligence to optimise your IT, security and business performance. With intuitive analysis features, machine learning, packaged applications and open APIs, Splunk Enterprise is a flexible platform that scales from focused use cases to an enterprise-wide analytics backbone.

Features

- Collects and indexes log and machine data from any source
- Powerful search, analysis and visualization capabilities empower users
- Fraud and cyber threat detection analysis
- Real time analysis for operational intelligence and business reporting
- Information Assurance and security analysis
- Monitor and ensure compliance issues
- Monitor non heterogeneous networks with unpredictable formats.
- Monitor Logistics RFID and logistics databases machine data (HUMS)
- Monitor and manage internet of things including SCADA data
- Big Data Analytics, machine data from internet/internal network

Benefits

- Monitor performance of network infrastructure against Service level Agreements
- Real-time network intelligence, avoid costly network escalations/downtime
- Eliminate legacy software and application costs
- Provide effective security compliance and reduce costs
- Detect and reduce internal and external cyber threats/abuse
- Proactively monitor clients/users understand and anticipate their needs
- Increase security and network management assets productivity
- Consolidate capabilities, reduce platform and application specific tools
- Splunk Accredited Consultants
- Analyse machine data from systems with varying formats.

Pricing

£1725 per licence per year

- Education pricing available
- Free trial available

Service documents

- pdf document: Pricing document
- pdf document: Skills Framework for the Information Age rate card
- pdf document: Service definition document
- pdf document: Terms and conditions

Framework
G-Cloud 11

Service ID
878241982541150

Contact
Networkology Ltd
Stefan Wallington
01249700084
tenders@networkology.com

Service scope

Service scope

Software add-on or extension	No
Cloud deployment model	Hybrid cloud
Service constraints	None
System requirements	Hardware non Windows> 2 x 6 core 2+GHZ, 12GB RAM Windows> 2 x 6 core 2+GHZ, 12GB RAM Linux, 2.6 and later Mac OS X 10.10 and 10.11 Windows 8, 8.1, 10 Windows Server 2008 R2, 2012, 2012 R2

User support

User support

Email or online ticketing support	Email or online ticketing
Support response times	1 hour first response Mon-Fri 9am-5:30pm excl Bank Holidays
User can manage status and priority of support tickets	No
Phone support	Yes
Phone support availability	9 to 5 (UK time), Monday to Friday
Web chat support	No
Onsite support	Yes, at extra cost
Support levels	We support P1-P4 incidents remotely or on site at a further cost (varies depending on the time required to resolve an issue.) A technical account manager is supplied FOC to any business or organisation acquiring Networkology's software or services. You have access to a cloud support engineer Mon-Fri 9am-5:30pm (not dedicated.)
Support available to third parties	Yes

Onboarding and offboarding

Onboarding and offboarding

Getting started	Splunk can provide free evaluation licences. We will provide Professional Services to help plan and execute your deployment and offer a full catalogue of training services to support the deployment.
Service documentation	Yes

Onboarding and offboarding

Documentation formats	HTML PDF
End-of-contract data extraction	The Splunk tool provides analysis and visualisation of data from various sources. The data rests at its original location and does not reside in Splunk. Therefore there is no need for data extraction at end of contract.
End-of-contract process	If a licence is terminated we can provide Professional Services at extra cost to help the Buyer to migrate their analytics need to another supplier.

Using the service

Using the service

Web browser interface	Yes
Supported browsers	Internet Explorer 10 Internet Explorer 11 Firefox Chrome Safari 9+
Application to install	No
Designed for use on mobile devices	Yes
Differences between the mobile and desktop service	If it is through a web browser the functionality is the same. If it is through the Splunk Mobile App custom visualisations do not work.
Service interface	No
API	Yes
What users can and can't do using the API	The Splunk Enterprise REST API provides methods for accessing every feature in our product. Your program talks to Splunk Enterprise using HTTP or HTTPS, the same protocols that your web browser uses to interact

Using the service

	with web pages, and follows the principles of Representational State Transfer (REST).
API documentation	Yes
API documentation formats	HTML ODF PDF
API sandbox or test environment	Yes
Customisation available	Yes
Description of customisation	Splunk application sits within the buyers' network or within the infrastructure of their chosen Cloud Provider. Splunk consumes data from sources within the network. The user is able to configure dashboards and the target data sources. configuration can be through Splunk Web, Splunk's Command Line Interface (CLI), Splunk's REST API and directly in configuration files.

Scaling

Scaling

Independence of resources	Splunk sits in the buyers network or the infrastructure of their chosen cloud provider and therefore contention is under their control.

Analytics

Analytics

Service usage metrics	No

Resellers

Resellers

Supplier type	Reseller providing extra features and support
Organisation whose services are being resold	Splunk

Staff security

Staff security

Staff security clearance	Conforms to BS7858:2012
Government security clearance	Up to Developed Vetting (DV)

Asset protection

Asset protection

Knowledge of data storage and processing locations	Yes
Data storage and processing locations	United Kingdom
User control over data storage and processing locations	Yes
Datacentre security standards	Managed by a third party
Penetration testing frequency	At least once a year
Penetration testing approach	In-house
Protecting data at rest	Physical access control, complying with another standard Other

Asset protection

Other data at rest protection approach	Splunk's own cloud service uses logical data separation, authenticated user accounts, and industry standard hardening. Data in transit is encrypted with industry standard SSL and data at rest is encrypted with AES 256-bit encryption. This service is acccredited to ISO 270001 standards. We can help the buyer to enable a similar configuration suitable for their data at rest protection.
Data sanitisation process	No
Equipment disposal approach	A third-party destruction service

Data importing and exporting

Data importing and exporting

Data export approach	There are many ways that a user can export data. Splunk provides a REST API to export data. Data can be exported by the Splunk Web facility. Users can use the Command Line Interface, SDK's and data forwarding tools.
Data export formats	CSV Other
Other data export formats	XML JSON Raw data
Data import formats	CSV Other
Other data import formats	XML JSON Raw data

Data-in-transit protection

Data-in-transit protection

Data protection between buyer and supplier networks	Other
Other protection between networks	Splunk sits within the Buyers network or the infrastructure of their chosen cloud provider. Data protection between networks is the responsibility of the buyer or their cloud provider.
Data protection within supplier network	TLS (version 1.2 or above) IPsec or TLS VPN gateway Legacy SSL and TLS (under version 1.2) Other
Other protection within supplier network	Splunk sits within the Buyers network or the infrastructure of their chosen cloud provider. There is no connection between Splunks networks and those of the buyer. Data protection between networks is the responsibility of the buyer or their cloud provider.

Availability and resilience

Availability and resilience

Guaranteed availability	Splunk sits within the Buyers network or the infrastructure of their chosen cloud provider. Availability is controlled by the buyer or their cloud provider.
Approach to resilience	Splunk sits within the Buyers network or the infrastructure of their chosen cloud provider. Resilience is the responsibility of the buyer or their cloud provider.
Outage reporting	Splunk sits within the Buyers network or the infrastructure of their chosen cloud provider. Outage reporting is the responsibility of the buyer or their cloud provider.

Identity and authentication

Identity and authentication

User authentication needed	Yes
User authentication	2-factor authentication Public key authentication (including by TLS client certificate) Dedicated link (for example VPN) Username or password
Access restrictions in management interfaces and support channels	Splunk sits in the buyers infrastructures or their cloud service provider of choice. In both instances the Splunk user authentication system allows the assignment of roles which require custom permissions. Admin, Power and User are roles set by default. The buyer can define other roles using a list of capabilities. Splunk authentication is enabled by default in Splunk Enterprise.
Access restriction testing frequency	At least once a year
Management access authentication	2-factor authentication Public key authentication (including by TLS client certificate) Dedicated link (for example VPN) Username or password

Audit information for users

Audit information for users

Access to user activity audit information	Users have access to real-time audit information
How long user audit data is stored for	User-defined
Access to supplier activity audit information	You control when users can access audit information
How long supplier audit data is stored for	User-defined

Audit information for users

How long system logs are stored for	User-defined

Standards and certifications

Standards and certifications

ISO/IEC 27001 certification	No
ISO 28000:2007 certification	No
CSA STAR certification	No
PCI certification	No
Other security certifications	No

Security governance

Security governance

Named board-level person responsible for service security	Yes
Security governance certified	Yes
Security governance standards	ISO/IEC 27001
Information security policies and processes	This offering is for cloud capable software for the buyer to deploy how they chose either inside their network as a private or hybrid cloud or within the infrastructure of their cloud service provider. Therefore the information security policies and processes will remain the responsibility of the buyer or their service provider. However, we understand the requirements for security policies and processes. Our Cloud based service uses third-party validation of our processes and policies and efforts to safeguard customer

Security governance

	data to industry standards worldwide. Working with our audit partners, ISO 27001 certification is completed for Splunk Cloud customer environments provisioned for data ingestion of over 20GB/day

Operational security

Operational security

Configuration and change management standard	Supplier-defined controls
Configuration and change management approach	Splunk sits in the network of the buyer or the infrastructure of their chosen cloud provider, Configuration and change management is the responsibility of the buyer or their supplier.
Vulnerability management type	Undisclosed
Vulnerability management approach	Splunk sits within the infrastructure of the buyer or their chosen cloud service provider and therefore they control their vulnerability management process. However we have a robust process for threats to the Splunk platform . We maintain a policy of evaluating all potential security vulnerabilities that are discovered internally or externally within two business days of discovery. We use the industry standard CVSSv2 to rate vulnerabilities. In the case of critical risk, high impact vulnerabilities, Splunk will make all reasonable effort to supply patches, assuming that patches are a viable stop-gap for customers who cannot otherwise upgrade Splunk.
Protective monitoring type	Undisclosed
Protective monitoring approach	Splunk sits in the infrastructure of the buyer or their chosen cloud service provider and therefore protective monitoring is the responsibility of the buyer or their supplier.
Incident management type	Undisclosed
Incident management approach	Splunk sits within the infrastructure of the buyer or their chosen cloud service provider and therefore incident

Operational security

	management policy and approach is the responsibility of the buyer or their cloud service provider.

Secure development

Secure development

Approach to secure software development best practice	Independent review of processes (for example CESG CPA Build Standard, ISO/IEC 27034, ISO/IEC 27001 or CSA CCM v3.0)

Public sector networks

Public sector networks

Connection to public sector networks	No

Pricing

Pricing

Price	£1725 per licence per year
Discount for educational organisations	Yes
Free trial available	Yes
Description of free trial	Full capability of a Splunk Enterprise license for 60 days allowing indexing up to 500 megabytes of data per day. This can be converted to a perpetual Free license or the buyer can purchase an Enterprise license to continue using the expanded functionality designed for multi-user deployments.
Link to free trial	https://www.splunk.com/en_us/download/splunk-enterprise.html

Service documents

pdf document: Pricing document pdf document: Skills Framework for the Information Age rate card pdf document: Service definition document pdf document: Terms and conditions

Service documents