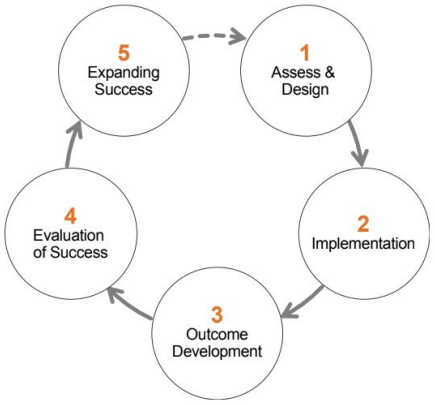
Splunk Cloud Enterprise Security Implementation Success

Accelerate the Time to Value of Your Splunk Cloud Enterprise Security Deployment

Jump start your Splunk Enterprise Security (ES) deployment in the cloud with the Splunk Professional Services Cloud ES Implementation Success Offering. This offering enables you to use our team to help your team quickly get up and running which helps you accelerate your time to value (TTV).

Splunk Success Methodology

Our experts have created this premium offering to support the rapid implementation of Splunk ES in the cloud to help increase your return on investment (ROI). You benefit from our team of Splunk experts who have extensive deployment experience with ES: they will share this experience through best practices to ensure your implementation is quickly optimized to bring your desired results and outcomes for your unique environment.



Offering Highlights

- Solutions Architect designs plan around your needs
- Best-practice based Splunk configuration
- Data onboarding of essential data sources
- Installation of Enterprise Security
- Prescriptive use cases implemented

Prescriptive Outcomes

Splunk recommends certain data sources and use cases to get immediate value from Enterprise Security. All levels of this offering have a set of required data sources and a set of recommended use cases they power, for the desired outcomes. The Base offering contains a slimmed-down list of data sources and use cases for basic security monitoring outcomes. Standard has a full set of recommended data sources and use cases, while Premium goes beyond and can contain custom analysis and development.

Security Use Case Discovery

Splunk provides workshops designed to help you monitor and increase the effectiveness of your security posture. Our experts will help you identify and customize the security queries (use cases) that will provide the greatest added benefit to your security posture and align with your business needs and risk priorities.

ES Health Check

With the Premium offering, Splunk Professional Services will come back twice during the first year of deployment to optimize your environment, validate any changes you have implemented, and work with your staff to increase productivity.

ES Upgrade

During the Health Check, Splunk Professional Services will upgrade you to the most recent version of Splunk ES and review new features and capabilities with your staff.

Three Sizes to Meet Your Needs

Every customer is different, so we have built three different sizes to provide flexibility to your needs. Each of our offerings includes the alignment of our experts and are surrounded by the support of our talented Delivery Managers.

	Splunk Enterprise Cloud Config	On-Prem Forwarder Installation	Data Sources	Splunk ES Configuration	Use Cases	Security Use Case Discovery	Future ES Health Check
Base	✔	✔	7	✔	5-10		
Standard	✔	✔	9	✔	10-20		
Premium	✔	✔	9+	✔	20+	✔	✔

Base Offering

Base is designed for customers with more internal resources dedicated to the Splunk project. Internal Splunk Admins and Users will receive informal training from the Splunk Accredited Consultant and will complete tasks remaining after Splunk Professional Services finishes their work.

Standard Offering

For customers looking for more support during the initial installation but are confident that ongoing maintenance and optimization of Splunk will be handled well by internal resources, build upon the services offered in Base with our Standard offering.

Premium Offering

This is designed for customers who recognize the opportunity for additional business value beyond the set of initial use cases. With the Premium offering, additional services beyond Standard are included, such as ongoing architectural, workshop, and optimization assistance, plus staff augmentation time to meet additional use case and outcome needs.

Included in Every Offering

Planning

- Workshop with a Solutions Architect to develop a plan for implementation

Installation

- Configure Splunk Enterprise in the cloud
- Install On-Premises forwarders to get data to the cloud
- On-board seven or more essential data sources
- Install Splunk Enterprise Security
- Deploy and optimize 5 or more use cases (correlation searches) for your environment
- Optimizing out-of-the-box content

Training

- Providing over-the-shoulder training for your Splunk Admins
- Completing a walk-through of ES functionality for your staff
- Reviewing best practices for onboarding data
- Reviewing best practices for creating correlation searches

Coordination

- A Delivery Manager tracks your path to success

Data Sources

To ensure Splunk ES can provide the insights you need to make faster and smarter security decisions, you need to ensure Splunk is getting data from critical systems throughout your environment. The ES Implementation Success Offering on-boards seven to nine essential data sources:

Base	Standard and Premium
• Active Directory • Exchange • Windows or Linux servers • DNS • Endpoint Anti-Malware • Network Communication (Firewalls) • Web Proxy Request	• Mail • DNS • Authentication • Endpoint Anti-Malware • Web Proxy Request • User Activity • Audit Trail • Network Communication (Firewalls) • Network Intrusion Detection

Setting up Queries

There are certain things you should be looking for that indicate potential threats within your environment. Our team will customize use cases designed to look for indications of malicious activity on your network. These queries are the foundation of a robust security monitoring program and are recommended, based on the data sources implemented in your environment.

Target Customer Attributes

The Splunk Enterprise Implementation Success offering is designed for customers looking to build a production Splunk Enterprise Security installation (without significant on-premises infrastructure) who are seeking a quick time to value for key business initiatives, from requirements gathering through production deployment.

Splunk Professional Services

Our services are backed by Splunk Accredited Consultants, Solutions Architects, and Delivery Managers. They leverage Splunk best practices and experience from thousands of Splunk deployments.

We only exist to get customers to valuable outcomes with their machine data – faster than they could on their own.

Resilience, let's build it together

Splunk Customer Success provides end-to-end success capabilities at every step of your resilience journey to accelerate time to value, optimize your solutions and discover new capabilities. We offer professional services, education and training, success management and technical support, surrounding you with the expertise, guidance and self-service success resources needed to drive the right outcomes for your business. For more information contact us at sales@splunk.com.

Terms and Conditions

This Solution Guide is for informational purposes only. The services described in this datasheet are governed by the applicable fully signed ordering document and any incorporated terms and conditions.