

Splunk Enterprise Security Deployment

rSolutions Professional Services

Overview

This premium service provides complete implementation for the Splunk App for Enterprise Security in production environments already running the Splunk platform. Included in this offering is everything you need to realize a quick time to value in your investment.

Enterprise Security Deployment Includes:

Architectural Review

Our engineers will review the health and configuration of your existing Splunk environment and recommend any remediation prior to deployment. This will ensure that the environment remains supportable, maintainable and operates as expected throughout the project and in the future.

Security Requirements Review

In cooperation with your staff our Splunk engineer(s) will analyze your organization's security requirements and landscape to design a deployment plan tailored to fit your organization's specific security needs.

Forwarder Configurations and Deployments

We will design and deploy forwarders with centralized configuration management via Splunk Deployment Server.

Dedicated Project Manager

Your assigned Project Manager will coordinate everything from data sharing across the project team to tracking project progress and maintaining deadlines throughout the implementation.

Customized Implementation Plan

Our team will design a deployment strategy and software configuration that is grounded in Splunk best practices, while leveraging all the features Splunk App for Enterprise Security has to offer your business.

Deployment Documentation

Our expert team will engage in knowledge transfer with your staff throughout the project and create thorough documentation of the implementation process and ongoing use of Splunk's Enterprise Security App.

Enterprise Security Deployment Benefits:

- > **Expert Guidance and Training:** Be assured that your staff will be taught best practices and be completely familiar with all the app has to offer before we are through.
- > **Optimal Performance of Splunk Enterprise Security App:** Work more efficiently and respond to threats faster.
- > **Content Tailored to Your Specific Security Strategy:** Software configuration will be optimized for your current security processes. Move easily through the program and track the data that matters to your organization most.
- > **Customized Correlation Searches:** Track data across multiple sources and compile it for use by your specific business systems.
- > **Faster Time to Value and Higher Return on Investment:** Our services save time and hassle in deployment and ensure complete use of the software from day one.



Deployment Sizing	Small	Medium	Large
Sizing Description	Single-site with multiple Splunk instances, designed to scale	Single-site architecture with multiple Splunk instances, designed to scale with search redundancy and index clustering.	Multi-site architecture with multiple Splunk instances, designed to scale with search redundancy, index clustering and site-to-site disaster recovery.
Duration	2 Weeks	4 Weeks	8 Weeks
Standard Data Sources Based on use cases supporting certified Security requirements	Up To 5	Up To 10	Up To 20
Custom Data Sources Indexed and normalized into Splunk's CIM	N/A	Up To 2	Up To 2
Standard Reports and Dashboards Leverage built-in dashboards and visualizations	Yes	Yes	Yes
Custom Reports and Dashboards	N/A	2 Views / 4 Searches Each	2 Views / 4 Searches Each
Custom Event-based Correlation Searches and Proactive Alerts	Up To 1	Up To 3	Up To 5

rSolutions Splunk Professional Services

Providing reliable, high-quality and agile service delivery our team of experienced and certified engineers can get you up and running quickly and operating at peak performance going forward. We apply the leading practices tailored to your needs and environment to make sure you get the most out of your investment in Splunk.

rSolutions professional services offer a full suite of Splunk services, including architectural design, configuration, upgrades, migrations and managed services