

Enterprise Security Suite

Security Information Management, Continuous Monitoring and Situational Awareness.



Splunk Enterprise Security Suite (ESS)

Splunk Enterprise Security Suite is a security practitioner’s ‘lens’ for examining the timely security data collected in Splunk. ESS and Splunk act as a single scalable solution that utilizes all your machine-generated data available to isolate security events and perform root cause analysis. With Splunk and ESS, security event investigations don’t have to end with a review of the security data. Forward thinking users know that the business also cares about application and data security. ESS organizes security-relevant data in an easy-to-use security domain format to provide continuous monitoring and situational awareness. Splunk and ESS can be implemented in days instead of weeks or months—giving you the most often used security event management functionality without all the headaches and costs of alternate solutions.

Security issues happen fast and can start anywhere in your enterprise architecture. By collecting and correlating system performance information with security data in real-time, ESS can provide an end-to-end view of data protection and availability. ESS leverages Splunk’s ability to scale across terabytes of data to watch for persistent threats that only reveal themselves as patterns of activity in large amounts of system data over long periods of time. Built for speed, ESS lets you drill-down from time lines and graphical elements into the raw system data. When working with the raw data, built-in workflow actions augment the security investigation process and allow the user to follow the trail of an investigation wherever it leads across hosts and across security domains. ESS provides over 50 of the most common security search-based correlations. Splunk with ESS makes it easy to use these out-of-the-

box correlations as templates for additional customized correlations, dashboards and reports.

Add Business Context to Security Events

Security log data presented to the business without meaningful context gets little attention from business managers. ESS contains a built-in customizable asset database framework that provides context for security incidents. Asset data and security metrics can be reported via ESS by business unit, location, asset criticality and other asset-related information.

Easy Data Collection

Splunk collects and indexes all machine generated data without the need for custom connectors or adapters, even for multi-line custom application logs. ESS leverages Splunk’s ability to index log data, configuration files, events and activities generated by any application, server, network, or security device without complex connectors, collection schemas or expensive database deployments.

Splunk Enterprise Security Suite Overview

Security Posture

Get real-time SOC-like presentation of security events and incidents. From any dashboard or graphic, drill down into specific security events and see notable security events by

location, host, source type and geography. Key performance indicators (KPIs) provide real-time monitoring of your security posture including vulnerabilities, out-of-date or unwanted software, systems with malware and hosts allowing insecure authentication. ESS lets security administrators control and set security policy thresholds.

Access Control

Simplify access control monitoring, exception analysis and audit processes for applications, operating systems and identity management systems across the enterprise. Correlate events from LDAP directories, Microsoft® Active Directory and RSA® Authentication Manager with operating system, application activities and physical access devices. Satisfy compliance and forensics requirements to track user and system access controls and authentication attempts on Windows, Linux and Solaris and the critical applications that run in these environments.

Endpoint Protection

Increase the effectiveness of endpoint security products such as Symantec™ Endpoint Protection, IBM® Proventia Desktop, or McAfee® Endpoint Protection. Prioritize and correlate threats to reduce false positives and see long term trending. Set policies for violations and discover and report on exceptions. ESS Endpoint Protection includes searches, reports and a library of alerts for malware, rare activities, resource utilization and availability.

Incident Review

ESS Incident Review provides a view of a single event or a 'roll-up' of related system events. It provides an incident management workflow for security teams allowing them to verify incidents and move them from an 'unreviewed' to 'reviewed', or 'closed' status while supplying comments about the status changes. These status changes are audited and displayed via dashboards in the audit portion of the ESS tracking team metrics. Escalations can be set up to automate the tracking of notable events and automatically trigger workflows in third-party incident management and trouble ticketing systems.

Network Protection

Integrate event and log data from network and security devices across the enterprise. Define network access policies and discover and report on anomalies across firewalls, routers, DHCP, wireless access points, load balancers, intrusion detection sensors and data loss prevention devices. Correlate events to follow network session activity across network technologies. ESS Network Protection includes correlations, searches, reports and dashboards. They let you monitor, alert and report on intrusion detection, vulnerability management, packet filtering and more.

Asset Center

Understanding where your company assets are located, who owns them and how critical they are relative to your infrastructure will help you to prioritize security events and investigations. ESS leverages Splunk's ability to 'look-up' data

stored in an asset database, spreadsheets or CSV files and use information for additional context for security events in reports and dashboards.

Audit

One of the most important aspects of data governance is the auditing of the security solution itself and the protection of event and log data against tampering and unauthorized access. Splunk ESS provides reports on all Splunk user and system activities for a complete audit trail. The Splunk engine uses data signing to maintain chain-of-custody and detect any alterations to the original log and event data.

Resources

The resources section of ESS contains a wealth of information about how to customize and build search-based correlations and add new data sources to ESS. This section also contains a threat management category with pre-defined links to common security resources for additional research.

Supported Platform Requirements

Splunk ESS 1.1.1 will run on Splunk version 4.1.6 or greater up to and including Splunk version 4.2. For a list of Splunk supported operating systems, please see <http://www.splunk.com/download>.

Features

- Security domain-specific taxonomy supporting dashboards, searches, reports, alerts, and security-relevant event types and correlations
- Award-winning, universal and scalable, real-time log event collection and indexing from any application, server, network or security device
- Robust Splunk Common Information Model (SCIM) to parse, categorize and normalize incoming event data
- Intuitive, easy-to-use interface facilitates communication of status and issues across the organization
- Scalable, distributed architecture and flexible deployment options

Get Started Today !

Website: www.splunk.com
Address: 250 Brannan St, San Francisco, CA, USA, 94107
Email: info@splunk.com | sales@splunk.com
Phone: +1 866-438-7758 | +1 415-848-8400
Free Download: www.splunk.com/download
Community: Splunk Answers | community@splunk.com