

Enterprise Security Suite

Security information management, monitoring and reporting to facilitate situational awareness.



Splunk Enterprise Security Suite (ESS)

The threat landscape is constantly changing. How can you achieve effective security posture awareness, faster incident response and meet stringent compliance reporting requirements with the growing onslaught of IT data spread across your enterprise?

Now, even with limited security resources, you can harness the power of Splunk because all your IT data is security-relevant information.

ESS supports the convergence of security, compliance and operations activities. It enables advanced security reporting, search-based correlation, and incident handling to help detect, respond, and prevent security-related issues. Organizations achieve more comprehensive security and compliance control monitoring and reporting and lower security operations costs.

Splunk indexes log data, configuration files, events and activities generated by any application, server, network, or security device without complex connectors, custom parsers or expensive database deployments.

ESS provides a simpler approach than traditional security information and event management (SIEM) systems with:

- Flexible security information taxonomy
- Easy implementation and management

- Linear, cost-effective scalability on commodity servers
- Support for any data source and data type
- Fast ad-hoc search capabilities
- Cost effective, pay as you grow licensing

What Is It?

The Splunk Enterprise Security Suite is an integrated set of security applications consisting of predefined searches, reports, alerts, dashboards and workflow actions supporting a wide variety of security use cases including:

- Security event monitoring
- Security information management
- Forensics/incident investigations
- Governance controls
- Log management

Splunk Enterprise Security Suite Apps

Splunk ESS is an integrated solution comprised of 6 apps that includes domain-specific dashboards, searches, reports, alerts, and hundreds of security-relevant event types and correlations.

Security Posture

Get immediate presentation and alerts of security events and incidents. Drill down into specific security events from the security posture dashboard. See notable security events by location, host, source type and geography. Key statistics provide real-time monitoring of your security posture including vulnerabilities, out-of-date or unwanted software, systems with malware and hosts allowing insecure authentication. Overall security policy thresholds can be controlled by the administrator.

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. Define user access and resource access policies, and discover and report on exceptions. 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. The Splunk Endpoint Protection App includes searches, reports and a library of alerts for malware, rare activities, resource utilization and availability.

Incident Response

The Splunk Incident Response App adds event actions and dashboards to manage critical events and situations. Escalation actions automate the tracking of notable events and automatically trigger workflows in third-party incident management and trouble ticketing systems such as BMC® Remedy, Cisco® Works, HP® Service Desk and IBM® Tivoli.

Network Protection

Integrate event and logging 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. The Splunk Network Protection App includes correlations, searches, reports and dashboards for monitoring, alerting and reporting on intrusion detection, vulnerability management, packet filtering and more.

Governance

The Splunk Governance App provides a scorecard-based capability to manage the policy and procedure content tracking and report the status of ISO 27002 compliance. ISO controls are linked to supporting searches, reports and alerts in the Splunk Enterprise Security Suite. The Governance dashboard details your current posture directly related to IT security and log management. Security policies can be configured to align with and help meet requirements for data retention, log review, incident detection, audit trail and compliance reporting.

Audit and Data Protection

One of the most important ISO governance requirements is the auditing of the security itself and the protection of event and log data against tampering and unauthorized access. The Splunk Audit and Data Protection App provides reports on all Splunk ESS user and system activities for 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.

Features

- Security domain-specific taxonomy supporting dashboards, searches, reports, alerts, and hundreds of security-relevant event types and correlations
- Leverages Splunk scalable, award-winning universal, real-time log event collection and indexing from any application, server, network or security device
- Uses Splunk Common Information Model (SCIM) to parse, categorize and normalize incoming event data
- An intuitive, easy-to-use interface facilitates communication of status and issues across the organization
- Scalable, distributed architecture and flexible deployment options
- Easy integration with system management, enterprise security and incident management systems
- Software-based solution runs on Windows, Linux, Solaris, AIX, FreeBSD and OSX

Get Started Today!

Website: www.splunk.com | www.splunk.com/goto/ess

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

More Info: sales@splunk.com