Splunk Enterprise Security

Analytics-driven SIEM solution for real-time threat detection, investigation, and automated response across hybrid and multi-cloud environments.

https://www.splunk.com/

Overview

Splunk Enterprise Security (ES) is a leading, analytics-driven Security Information and Event Management (SIEM) solution built as a premium application on the highly scalable Splunk operational intelligence platform. It is designed to help Security Operations Center (SOC) teams detect, investigate, and respond to internal and external attacks by centralizing and aggregating all security-relevant events from diverse sources like network, endpoint, access, malware, vulnerability, and identity systems.

The platform provides a unified work surface and streamlined workflows for threat detection, investigation, and response (TDIR) by natively integrating with Splunk SOAR (Security Orchestration, Automation, and Response). Key capabilities include real-time monitoring and alerting, advanced threat detection utilizing machine learning and analytics, and risk-based alerting to prioritize high-confidence threats. The solution is highly valued for its powerful Search Processing Language (SPL), robust log aggregation, and extensive third-party integration options available through the Splunkbase app ecosystem.

Splunk ES is highly scalable and flexible, supporting deployment across on-premise, cloud, and hybrid environments, and is best suited for large organizations and enterprises with well-staffed IT teams due to its complexity and high cost.

Key Features

- Real-Time Monitoring and Alerting
- Advanced Threat Detection (ML/Analytics)
- Security Orchestration Automation and Response (SOAR) Integration

- Risk-Based Alerting and Prioritization
- Threat Intelligence Integration
- Incident Investigation and Case Management
- Log Aggregation and Correlation
- Customizable Security Posture Dashboards

Pricing

Model: enterprise

Pricing is based on consumption, either by data ingestion volume (GB/day) or workload capacity (Splunk Virtual Compute - SVC units). It is a premium application that requires an Enterprise or Cloud license, and is known to be costly. Public pricing is not disclosed.

Target Company Size: medium, enterprise

Integrations

Splunk SOAR, AWS, Azure, GCP, Firewalls, Endpoint Detection Tools, Identity Providers (e.g., Okta, PingIdentity)

Compliance & Certifications

ISO 27001, SOC 2, PCI DSS, HIPAA