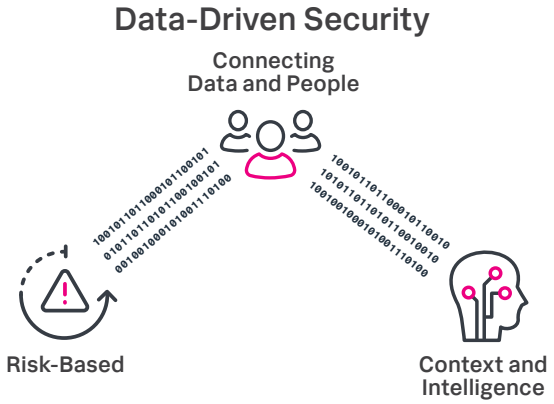
splunk>

PRODUCT BRIEF

Splunk Enterprise Security

Data-driven insights for full breadth visibility, detection and investigation

- **Gain full visibility and improve security posture** across your multi-cloud, hybrid, and on-premises environment
- **Accelerate threat detection and investigation** using risk-based alerting, integrated threat intelligence, and out-of-the-box security content
- **Quickly gather context** from your technology investments with a flexible data platform and integrations across multi-vendor tools and technologies



Your security team faces a dynamic threat landscape, emerging adversary tactics, and evolving business demands. But to meet these challenges, your team needs data-driven capabilities, contextual insights and accurate rapid threat detection techniques. These capabilities can help you reduce mean-time-to-detection and make informed decisions to strengthen business outcomes.

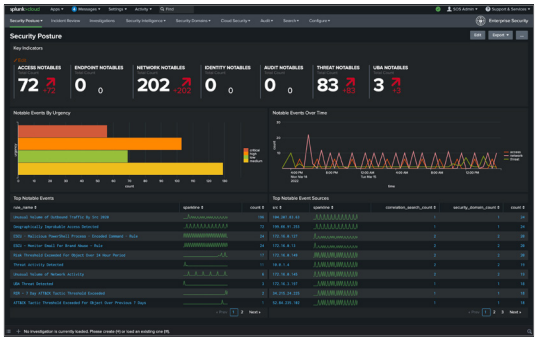
Splunk Enterprise Security (ES) is a data-centric, modern security information and event management (SIEM) solution that delivers data-driven insights for full-breadth visibility into your security posture so you can protect your business and mitigate risk at scale. With unparalleled search and reporting, advanced analytics, integrated intelligence, and pre-packaged security content, Splunk ES accelerates threat detection and investigation, letting you determine the scope of high-priority threats to your environment so you can quickly take action. Splunk ES is built on an open and scalable data platform that allows you to stay agile in the face of evolving threats and business needs.

Splunk ES helps security teams — of all sizes and levels of expertise — to streamline security operations. It provides:

- **1170+ out-of-the-box detections** that align to industry frameworks such as MITRE ATT&CK, NIST, CIS 20, and Kill Chain
- **Actionable intelligence** with associated normalized risk scores and the necessary context from intelligence sources that are required in order to detect, prioritize, and investigate security events
- **Real-time detections** for suspicious and malicious behaviors using cloud-based streaming analytics
- **2700+ security and IT integrations** built by Splunk, partners, and community members to make it easy to introduce your security tools and data sources into Splunk
- **80% reduction in alert volume** to reduce alert fatigue, provide clarity and prioritization for analysts, and close cases in minutes instead of weeks
- **Operationalize the MITRE ATT&CK Framework** with a visualization matrix that highlights the tactics and techniques observed in risk events to save time when investigating events
- **Quickly discover the scope of an incident and respond accurately** with a comprehensive view of the malicious executables and threat actors observed on machines and users
- **Support for every deployment type** through cloud, multi-cloud, on-premises, and hybrid to match business needs and growth

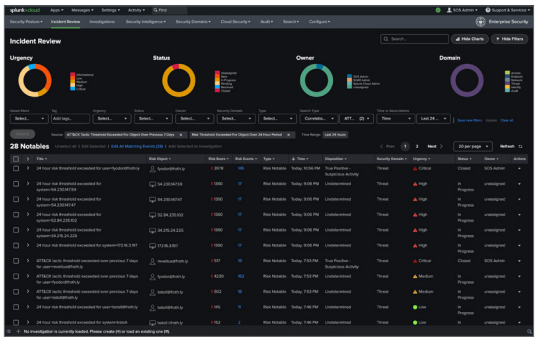
Data-Driven Security

Splunk Enterprise Security provides visibility and insights into data that powers and secures the business, enabling analysts to make critical decisions with speed and accuracy with the objective of seamlessly detecting and defending the enterprise.



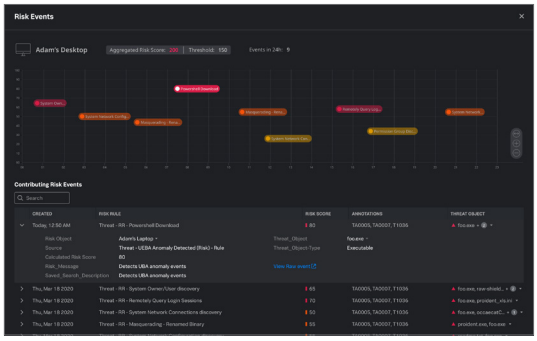
Full Visibility

Break down data silos and gain actionable intelligence into the full breadth of your security posture. Monitor tens of terabytes of data per day — any data from anywhere, structured or unstructured. Backed by an unparalleled data platform, arrive at data-driven decisions that protect your business and reduce risk. Achieve outcomes inside and outside of the security organization (IT, DevSecOp, and more).



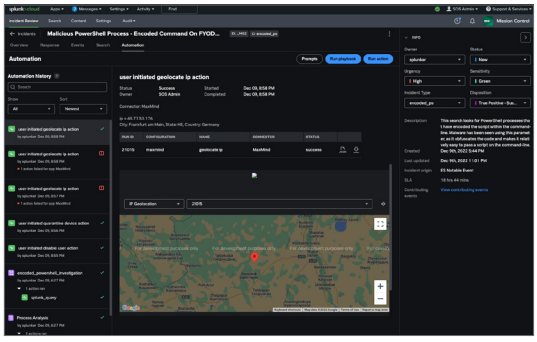
Increased Flexibility and Compatibility

Stay agile in the face of changing threats and business needs with an adaptable data platform regardless of where the organization is on their cloud or hybrid journey. Quickly gather context across your multi-vendor security ecosystem by utilizing technology integrations built by Splunk, partners, and the community on Splunkbase, which houses 2,500+ apps and add-ons.



Accelerated Threat Detection

Increase the speed of security investigations by more than 50% with unsupervised machine learning to detect unknown threats and anomalous behaviors. Accelerate investigations and gain critical context by enriching and prioritizing high-fidelity alerts with integrated threat intelligence to boost SOC productivity and drive down fatigue.



Unify Your Security Operations

Mission Control, an application available to Splunk Enterprise Security users, brings order to the chaos of your security operations. Splunk Mission Control unifies detection, investigation and response capabilities within one common work surface; simplifies security workflows by codifying your processes into easy-to-follow response templates; and empowers your team with automation to reduce analyst grunt work and increase the speed of response.

Ready to supercharge your security operations with a cloud-based data-driven SIEM solution?
Learn how to get started with Splunk.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

23-165055-Splunk-Enterprise Security-PB-104