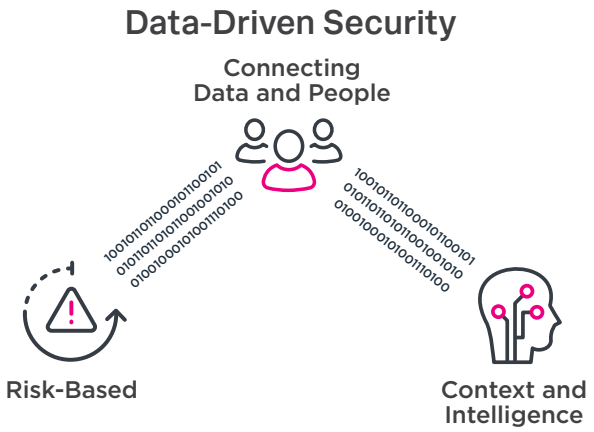
splunk> turn data into doing

PRODUCT BRIEF

Splunk Enterprise Security

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

- **Improve security posture** and gain full visibility across your multi-cloud, hybrid, and on-premises environment
- **Accelerate threat detection and investigation** using risk-based alerting, 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



You're faced with adapting to a dynamic threat landscape, evolving adversary tactics, advanced threats and evolving business demands — and your existing security technologies can't keep up. To meet these new challenges, modern security teams need data-driven capabilities, contextual insights and accurate and rapid threat detection techniques to reduce mean-time-to-detect and make business-centric decisions. Security teams can more quickly detect, investigate, and respond to attacks by centralizing and utilizing all their machine data.

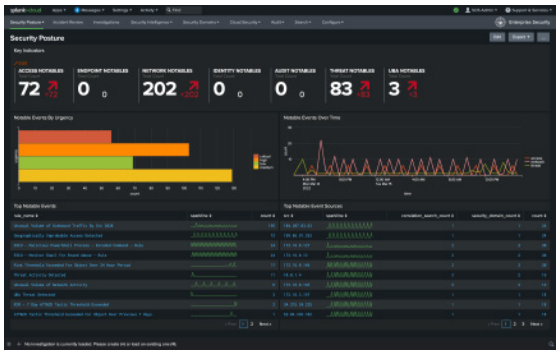
Splunk Enterprise Security (ES) is a data-centric, modern security information and event management (SIEM) solution that delivers data-driven insights for full breadth visibility into your security posture so you can protect your business and mitigate risk at scale. With unparalleled search and reporting, 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. Built on an open and scalable data platform, you can stay agile in the face of evolving threats and business needs. Our extensive ecosystem of Splunk, partner, and community-built integrations as well as flexible deployment options ensure your technology investments are working in tandem with Splunk ES whilst meeting you wherever you are on your cloud, multi-cloud, or hybrid journey.

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

- Insight from data that is automatically retrieved from network, endpoint, access, malware, UBA anomalies, vulnerability and identity technologies, and shared to correlate using pre-defined rules, risk-based alerting, or via ad-hoc searching.
- Out-of-the-box capabilities to manage and prioritize alerts, contextual searches, and the rapid detection and analysis of advanced threats.
- Flexibility to customize correlation searches, risk-based alerts, reports and dashboards to fit specific needs — whether deployed for continuous monitoring, incident investigation and response, a security operations center (SOC), or for executives who need to view business risks.
- Improve operational efficiency using workflow-based context for automated and human-assisted decisions.

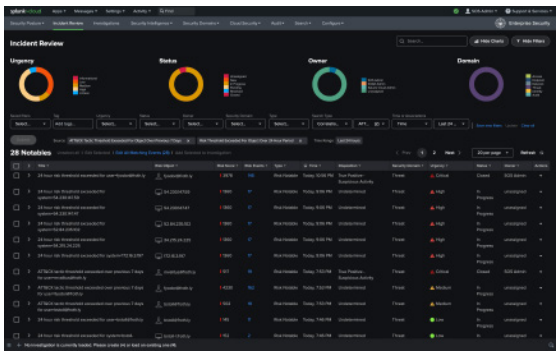
Data-Driven Security Defined

The process of discovering relationships across all security-relevant data, including data from IT infrastructures, point security products and all machine-generated data to rapidly adapt to a changing threat landscape.



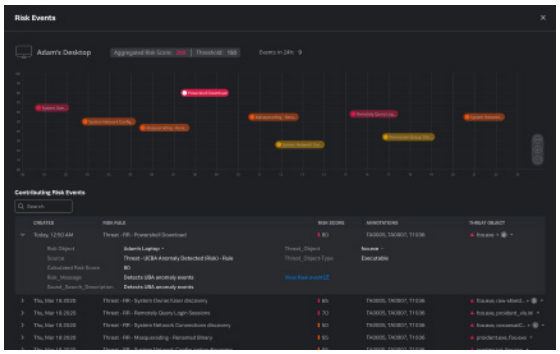
Continuously Monitor Security Posture

Get a clear visual picture of your organization's security posture by using a comprehensive set of pre-defined dashboards, custom views with key security metrics and performance metrics, static and dynamic thresholds, and trending indicators. Reduce organizational risk by using the Use Case Library for faster detection of newly discovered and ongoing threats and accelerating incident response.



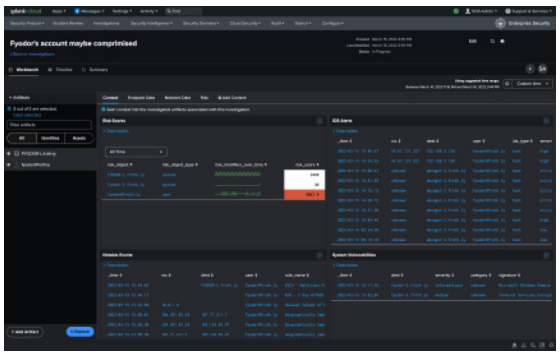
Prioritize and Act on Incidents

Reduce false positives, detect more sophisticated threats, and align security operations to industry frameworks like MITRE ATT&CK with Risk-Based Alerting (RBA). Optimize incident response workflows by using centralized logs, prioritized alerts, UBA anomalies, pre-defined reports and correlations, and incident response workflows with risk scores. Streamline investigations and accelerate incident response using Investigation Workbench to investigate one or more notable events in one view.



Rapidly Investigate & Analyze Threats

Gain full context of the events leading up to a high-priority alert with RBA. Conduct rapid investigations using ad hoc search, as well as static, dynamic and visual correlations to improve response times. Investigate and pivot on any field from any data retrieved automatically from across the security and IT stack to rapidly develop threat context and track attacker steps to verify evidence. Utilize Adaptive Response actions to automate retrieval, sharing, and responses in multi-vendor environments.



Handle Multi-Step Investigations

Conduct breach and investigative analyses to trace the activities associated with compromised systems. Apply the kill chain methodology and investigate the attack lifecycle using ad hoc searches and the out-of-the-box functionality within ES. Enable faster detection and response process by utilizing automatically delivered security detection and investigation content developed by the Splunk Threat Research Team.

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