splunk>

PRODUCT BRIEF

# SPLUNK® ENTERPRISE SECURITY

Analytics-driven security and continuous monitoring for modern threats

- **Optimize security operations** with faster response times using Adaptive Response and Investigation Workbench
- **Improve security posture** with end-to-end visibility across all machine data, in the cloud and on-premises
- **Increase investigation capabilities** using user behavior analytics detected anomalies and threats
- **Make better informed decisions** by leveraging threat intelligence

## Analytics-Driven Security

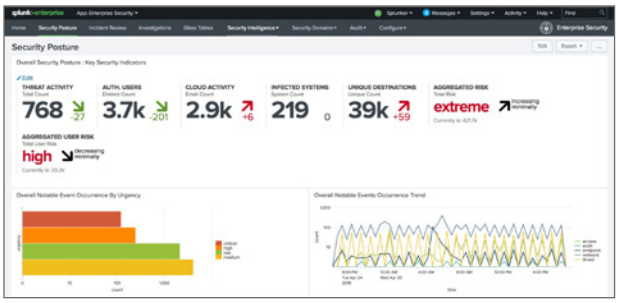

You're faced with adapting to a dynamic threat landscape, evolving adversary tactics, advanced threats and changing business demands—and your existing security technologies can't keep up. To meet these new challenges, modern security teams need analytics capabilities and contextual incident response; and they must be able to rapidly implement new threat detection techniques to reduce time-to-threat-response and make business-centric decisions. Security teams can more quickly detect, respond and disrupt attacks by centralizing and leveraging all machine data.

Splunk Enterprise Security (Splunk ES) is a security information and event management (SIEM) solution that enables security teams to quickly detect and respond to internal and external attacks, to simplify threat management while minimizing risk, and safeguard your business. Splunk ES enables your security teams to use all data to gain organization-wide visibility and security intelligence. Regardless of deployment model—on-premises, in a public or private cloud, SaaS, or any combination of these—Splunk ES can be used for continuous monitoring, incident response, running a security operations center or for providing executives a window into business risk. Splunk ES can be deployed as software together with Splunk Enterprise or as a cloud service together with Splunk Cloud.

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

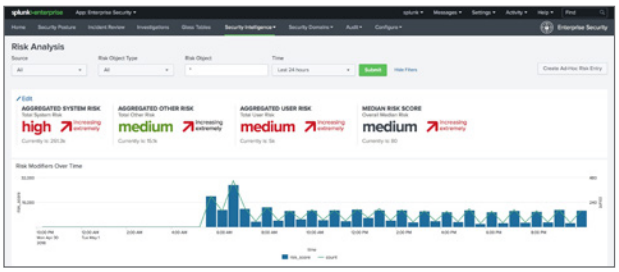
- **Insight from data** that is automatically retrieved from network, endpoint, access, malware, UBA anomalies, vulnerability and identity technologies, and shared to correlate using pre-defined rules or via ad hoc searching
- **Out-of-the-box capabilities to manage alerts** and power dynamic discoveries, contextual searches, and the rapid detection and analysis of advanced threats
- **Flexibility to customize** correlation searches, alerts, reports and dashboards to fit specific needs—whether deployed for continuous monitoring, incident 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

**Analytics-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.



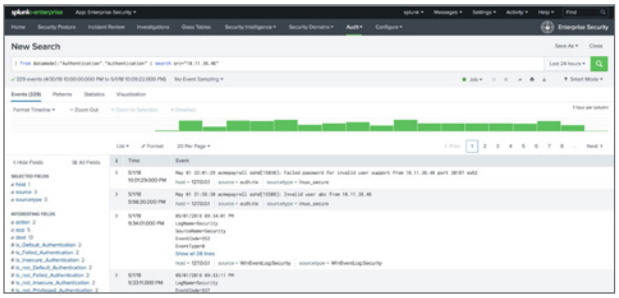

## Continuously Monitor Security Posture

Get a clear visual picture of your organization's security posture by using a comprehensive set of pre-defined dashboards, custom Glass Table views with key security metrics, key performance metrics, static and dynamic thresholds, and trending indicators.



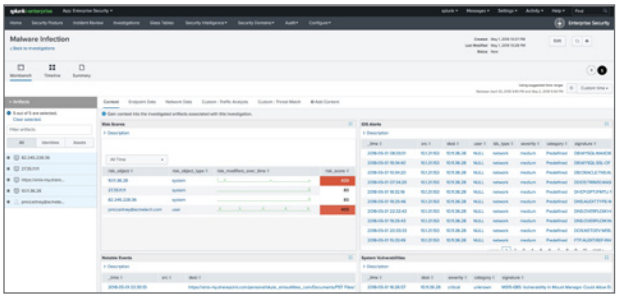

## Prioritize and Act on Incidents

Optimize incident response workflows for individual analysts or investigation teams by using centralized logs, alerts and incidents, UBA anomalies, pre-defined reports and correlations, incident response workflows with risk scores, and correlations for a security-specific view. Streamline investigations and accelerate incident response using Investigation Workbench to investigate one or more notable events in one view.




## Rapidly Investigate Threats

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. Automate and optimize threat detection and remediation using 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 all ES capabilities in combination with the Investigation Timeline and Investigation Workbench. In addition, ES Content Update, a subscription service, enables analysts and investigators to continuously improve and expedite their response to threats, independent of periodic software updates.

**Try Splunk Enterprise Security Now** Experience the power of Splunk Enterprise Security – with no downloads, no hardware set-up and no configuration required. The Splunk Enterprise Security Online Sandbox is a 7-day evaluation environment with pre-populated data, provisioned in the cloud, enabling you to search, visualize and analyze data, and thoroughly investigate incidents across a wide range of security use cases. You can also follow a step-by-step tutorial that will guide you through the powerful visualizations and analysis enabled by Splunk software. **Learn More.**

splunk>

**Learn more:** www.splunk.com/asksales

www.splunk.com