Splunk Enterprise Security

Detect what matters, investigate holistically and respond rapidly

Product Benefits

Realize comprehensive visibility to make sense of data noise and enable fast action.

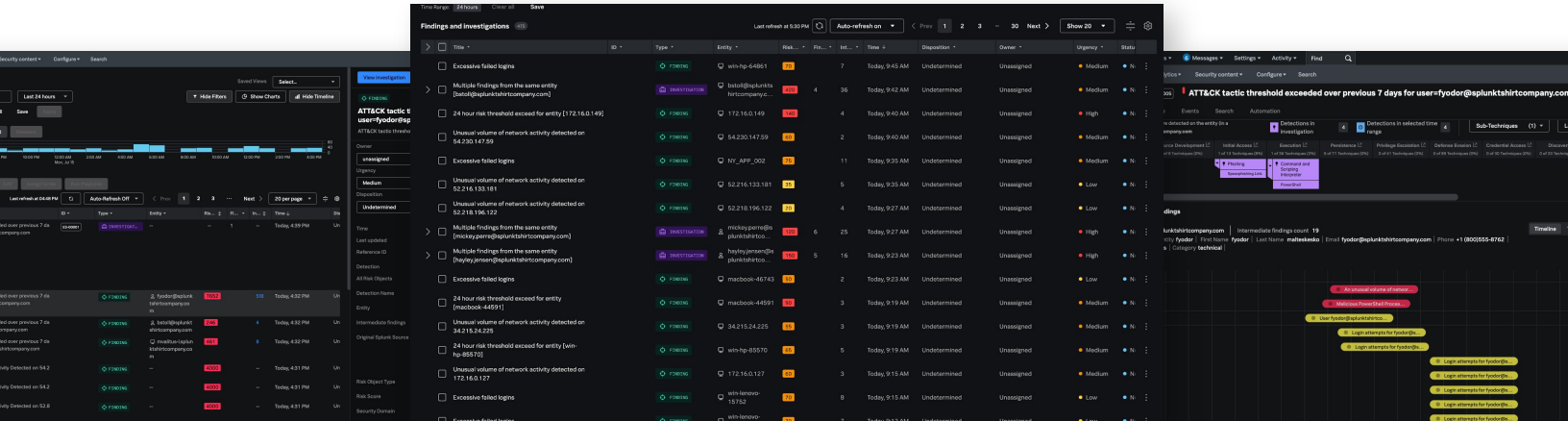
Empower accurate detection with context to streamline investigations and increase productivity.

Fuel operational efficiency by unifying threat detection, investigation and response workflows.

Your security team faces significant challenges in today's threat landscape. They grapple with analyzing data noise, trying to gain visibility across hybrid, cloud and on-prem environments, while being inundated with vast amounts of data from various security and IT sources. It's a struggle to address every minor security issue and prioritize major vulnerabilities before they escalate. Solving for this requires the ability to turn volumes of raw data into actionable insights.

Threat detection is made even harder by a pervasive lack of context related to security events. Amidst security noise and an overwhelming number of alerts that require action, analysts struggle to discern high-priority threats from low-priority threats without sufficient context. To make matters worse, defending the organization from a wide range of risks now includes detecting sophisticated, AI-driven threat campaigns. Plus, security teams are burdened with managing an average of 25+ different security tools, across detection, investigation and response.

As the market-leading security information and event management (SIEM) and security analytics solution, Splunk® Enterprise Security is the trusted choice for security operations centers (SOCs) around the globe. Splunk has paved the way in advancing SIEM and security analytics by being at the forefront of innovation in security to help thousands of customers outpace adversaries. Its powerful capabilities enable you to realize comprehensive visibility, empower accurate detection with context and fuel operational efficiency. Built on the Splunk platform powered by AI capabilities, Splunk Enterprise Security delivers analytics at scale for continuous security monitoring with cost-effective data optimization. With Splunk, you can detect what matters, investigate holistically and respond rapidly.



Gain comprehensive visibility

Unmatched, comprehensive visibility by seamlessly ingesting, normalizing and analyzing data from any source at scale enabled by Splunk's data-powered platform with assistive AI capabilities.

Make sense of alerts

Be enabled for fast action when an alert is triggered with the custom alert actions feature. Custom alerts can be set to varying levels of granularity based on conditions such as data thresholds, trend-based conditions and behavioral pattern recognition like brute force attacks and fraud scenarios.

Prioritize focus with context

Drastically reduce alert volumes by up to 90% with risk-based alerting (RBA). RBA uses the Splunk Enterprise Security correlation search framework to collect risk events into a single risk index. Collected events create a single risk notable when they meet a specific criterion, so you can stay focused on imminent threats that traditional SIEM solutions might miss.

Utilize curated detections

Tap into 1,700+ out-of-the-box detections based on Splunk Threat Research deep dives into detection engineering to find and remediate threats faster. These detections also align to industry frameworks like MITRE ATT&CK, NIST CSF 2.0 and Cyber Kill Chain®.

Build high-confidence aggregated alerts

Enhanced detection capabilities help analysts understand and implement a risk-based alerting detection strategy with turnkey flexibility to build high-confidence aggregated alerts for investigation.

Complete threat detection, investigation and response

Native integration with Splunk® SOAR* automation playbooks and actions with the case management and investigation features of Splunk Enterprise Security and Mission Control delivers a single unified work surface. Optimize mean time to detect (MTTD) and mean time to respond (MTTR) for an incident.

Execute response workflows

Response Plans directly in Splunk Enterprise Security allow users to collaborate and execute incident response workflows for common security use cases easily.

Simplified terminology

The taxonomy in Splunk Enterprise Security aligns to the Open Cybersecurity Schema Framework (OCSF), making it easy for your security team to understand exactly what they are working on across detection, findings, and investigations workflows.

Build what you need

Access Splunk's network of 2,200+ partners and Splunkbase's 2,800+ partner and community-built apps that seamlessly integrate with your existing tools. Collect, search, monitor and analyze data using a centralized, vendor neutral solution to help you meet increasingly complex compliance requirements.

Read more >

Take a tour >

Latest releases >

*Splunk SOAR subscription required

splunk>

Contact us: splunk.com/asksales

splunk.com