

Splunk for Security

Because Splunk collects and analyzes data from every part of the organization, Splunk acts as the security nerve center for small and big companies. Splunk's security platform gives organizations the ability to detect, respond and remediate threats faster. This helps analysts sitting inside of the Security Operations Center (SOC) automate their security and threat hunting processes, giving them more time back to focus on setting a proactive security strategy. The cyber-threat landscape grows more dangerous and complicated by the day, and only a data-driven approach enables security teams to quickly detect, respond to and remediate attacks.

Top 5 things you need to know about Splunk's Security Solutions:

- 1** Splunk Enterprise Security (ES) streamlines all aspects of security operations and is suitable for organizations of all sizes and expertise
- 2** Customers will use Machine Learning to detect anomalies, events or circumstances that do not fit normal patterns
- 3** Splunk Insights for Ransomware is a new offering that delivers organizations a complete analytics solution to manage ransomware threats
- 4** Splunk User Behavior Analytics (UBA) is an out-of-the-box solution that helps organizations find known, unknown and hidden threats with machine learning. This helps analysts automate their security processes, giving them more time back to focus on strategy and threat hunting
- 5** The Adaptive Response Initiative, which now has more than 20 leading security vendors, was built to help integrate technologies such as next-generation firewall, endpoint security and threat intelligence, among others