splunk>

PRODUCT BRIEF

SPLUNK® USER BEHAVIOR ANALYTICS

Detect cyberattacks and insider threats

- **Improve detection** of known, unknown and hidden cyberattacks and insider threats
- **Increase security analyst effectiveness** by prioritizing threats and avoiding false positives
- **Easy to use** for SOC analysts, incident responders and SIEM administrators

Advanced Security Analytics

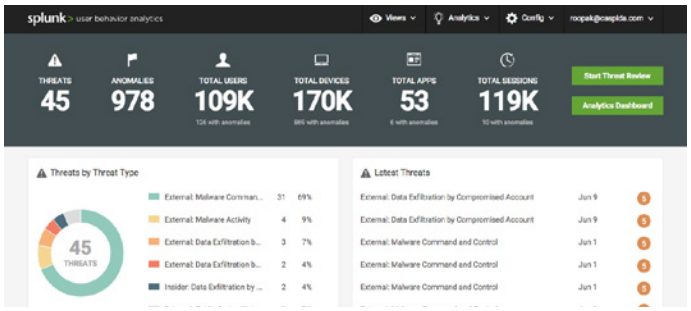
Sophisticated cyberattacks can be hidden and difficult to find, yet addressing these threats is critical to protecting confidential data. That means today's security teams are tasked with finding and responding to the threats hidden in their environments regardless of organizational size or skillset.

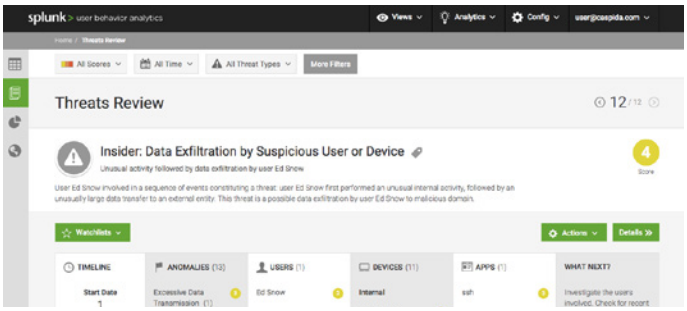
Splunk User Behavior Analytics (Splunk UBA) helps organizations find known, unknown and hidden threats using machine learning, behavior baselines, peer group analytics and advanced correlation to find lurking APTs, malware infections and insider threats. Splunk UBA addresses security analyst and hunter workflows, requires minimal administration and integrates with existing infrastructure to locate hidden threats.

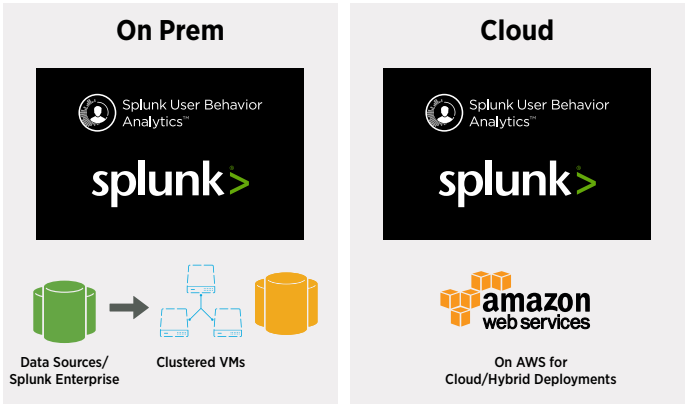
What Is Behavior-Based Threat Detection? Behavior-based threat detection is based on machine learning methodologies that require no signatures or human analysis, enabling multi-entity behavior profiling and peer group analytics – for users, devices, service accounts and applications. The result is automated, accurate threat and anomaly detection.

The entire lifecycle of security operations—prevention, detection, response, mitigation, to the ongoing feedback loop—must be unified by continuous monitoring and advanced analytics to provide context-aware intelligence. Splunk Enterprise, Splunk Enterprise Security (ES) and Splunk UBA work together to:

- Extend the search/pattern/expression (rule) based approaches in Splunk Enterprise and Splunk Enterprise Security (Splunk ES) with threat detection techniques to detect threats with sophisticated kill chain visualizations
- Provide security teams with machine learning, statistical profiling and other anomaly detection techniques that leverage the readily available data at massive scale in Splunk Enterprise
- Combine machine learning methods and advanced analytics capabilities to enable organizations to monitor, alert, analyze, investigate, respond, share and detect known and unknown threats regardless of organizational size or skillset







Streamlined Threat Workflow

Reduce billions of raw events to thousands of anomalies, then to tens of threats for quick review and resolution. Leverage security-semantics-aware machine learning algorithms, dynamic statistical methods and correlations to identify hidden threats without human analysis. Context, location and container awareness minimize false positives.

Threat Review and Exploration

Visually sequence threats and highlight abnormal and suspicious paths and frequencies. Identify critical threats using advanced correlations across models, leveraging self-learning and adaptive algorithms—machine learning and statistical. Interactively investigate threats and supporting evidence.

Kill Chain Detection and Attack Vector Discovery

Identify abnormal APT and breach activity (e.g. CnC, lateral communication) and kill chain attacks (e.g. pass-the-hash). Detect lateral patterns of malware or malicious insider proliferation. Respond to real-time flagging of anomalous activity (e.g. suspicious URL or land-speed login violations). Detect behavior-based irregularities (e.g., VM or AWS container threat activity). Pinpoint botnet or CnC activity (e.g., Trojans or polymorphic malware).

Platform Architecture & Deployment Options

Splunk UBA includes the Hadoop ecosystem for scalable, cost-efficient and open data persistence. It's designed for real-time and large-scale event analysis, and includes time-series and graph databases for processing and representing security connections within the network. RESTful APIs automate data ingestion with third party products, helping to drive remediation and prevention. Splunk UBA is proven to scale to over hundreds of terabytes and billions of events, and is deployable on-premises as software, on a virtual machine, or as a customer-managed public cloud instance (AWS and vCloud Air).

Download Splunk Free or explore the online sandbox. Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs. **Learn more** about Splunk User Behavioral Analytics by contacting **ubainfo@splunk.com**.

splunk> sales@splunk.com www.splunk.com