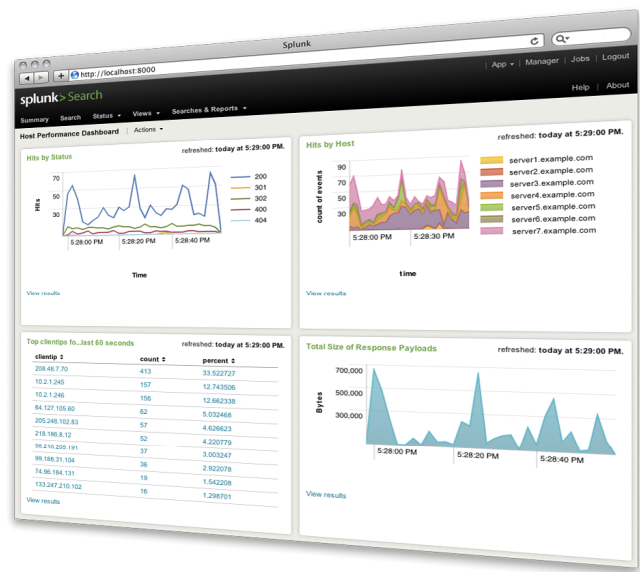
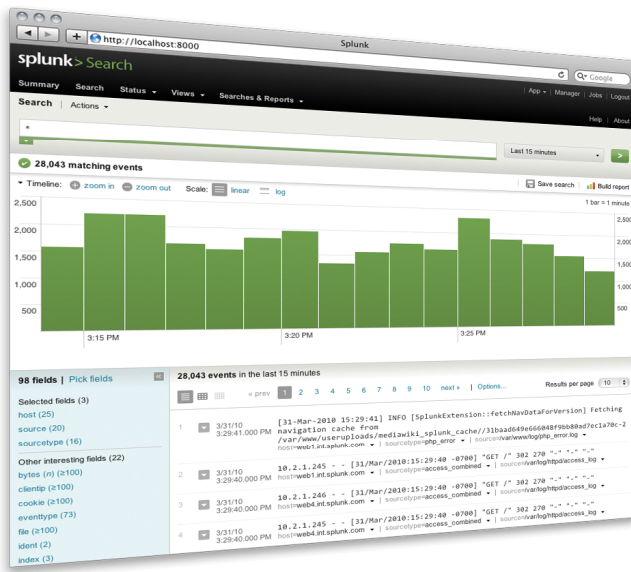


Splunk for Security

Analysis of all machine-generated data is required for security, risk management and operational intelligence.



All Data is Security-relevant

The role of IT security is expanding, driven by new and evolving security use cases with risk implications for the business. Gone are the days when security investigations started and ended with firewall, anti-virus and intrusion-detection from a rule-based security event management system. Today's security professionals instead face a far more complex set of challenges, which can be summarized by the following trends:

- **Rule-based systems are reactive not proactive.** Traditional software and appliance-based security products that depend on vendor updates can't react fast enough to detect the malicious code within zero-day vulnerabilities.
- **Hacker motivations have changed.** Cyber espionage and financial gain are the primary motivations behind today's malicious activities. Meanwhile, persistent and hard to detect malware can be easily created using readily available Internet resources.
- **Data protection, system availability and risk management are all security priorities.** Security-savvy organizations realize that all machine-generated data has security relevance. The first indication there is a security event doesn't always come from security data sources. Application data alone can contain the subtle signals or patterns that indicate the start of a security incident.

Security teams need access to machine data from enterprise security systems, plus the operating systems and applications they protect, wherever they are—physical, virtual or in the cloud. Much larger datasets must be reviewed over longer periods of time to discover anomalous patterns of activity that can indicate the start of a security event.

Using Splunk for Security

Flexible, Scalable Security Investigation

Splunk is scalable and flexible enough to search across terabytes of data from any machine data source such as traditional security sources, custom applications, and databases. Splunk automatically provides a timeline view of all collected data. This timeline can be used to focus on the precise time that a security event occurred. Any search result can be turned into a

report for distribution. This is especially useful for ad-hoc queries in support of compliance initiatives such as PCI, SOX, or HIPAA.

Real-time Forensics

Once a forensic investigation is complete, Splunk searches can be saved and monitored in real time. Real-time alerts can be routed to the appropriate security team members for follow-up. Correlation across system data by vendor or data type is supported in Splunk's easy-to-use search language.

Splunk supports a common information model giving you control over how data is represented in Splunk, expressing security events in clear, meaningful terms. Splunk's search language supports correlations that can generate alerts based on a combination of specific conditions, patterns in system data or when a specific threshold is reached.

Splunk lets you see real-time information from security and network devices, operating systems, databases and applications on one timeline, enabling your security teams to quickly detect and understand the end-to-end implications of a security event. Splunk watches for hard-to-detect patterns of malicious activity in machine data that traditional security systems may not register. This approach can also provide the building blocks for a variety of supported fraud and theft detection use cases.

Metrics and Operational Visibility

Understanding business risk requires a metrics-based approach to measure effectiveness over time. Splunk's built-in search language contains the commands needed to express search results as tables, graphics, and timelines on security dashboards. Key performance indicators (KPIs) can be monitored by business unit, compliance type, location, and much more.

Real-time Business Insights

Splunk can provide the needed context for security events by collecting and displaying data from your financial systems or asset management databases in reports and dashboards. Helping you understand the cost of a system outage or network degradation is as simple as having Splunk monitor the average total hourly or daily sales from financial data and then calculating the value of lost orders due to lack of availability and display it on the Splunk dashboard.

Splunk Provides Operational Intelligence

Your machine-generated data contains a record all human-to-machine and machine-to-machine interactions. The value of this data to the security team to solve problems, proactively monitor for threats, and provide business insight is huge. The key to extracting value from this data is having a single, easy-to-use solution that can scale, collect system or application data regardless of format and turn it into meaningful information supporting business decisions.

Splunk becomes the enterprise-wide system of record where you monitor, search, and report on real-time data from any user, network, system, or application activity. Correlation across this data is key to solving fraud, data security, insider threat and network security problems before they happen. This increases team performance resulting in a reduced risk to the business.

Splunk and SIEM

Splunk can complement an existing security information and event management system (SIEM). Traditional SIEM deployments help reduce the amount data security teams need to review while correlating different data sources using a rule-based approach to reduce false positives. This data reduction model forces users to decide what data will be included in a security investigation before a security event actually occurs. This artificially limits incident investigations and may lead to false conclusions, often times away from the root-cause.

In contrast, Splunk's scalability and schema-less approach expands the amount and types of data collected and analyzed. Splunk augments the SIEM "rules-based" approach with its pattern-based analysis capabilities. Additional alerts can be created based on application error rates or other thresholds.

This approach breaks down silos between operations and security teams. Splunk includes real-time APIs that can stream data to a SIEM correlation engine, allowing you to drill-down from the SIEM into Splunk while preserving legacy processes, workflows and technology investments.

Splunk for Security Use Cases

Pattern-based Malware Detection

In one quarter of 2010 McAfee reported over 10 million new, never-before-seen pieces of malware. Rule-based systems such as anti-virus or intrusion detection systems, depend on vendor updates to detect malware already seen in the wild and are easily defeated. Monitoring for anomalous patterns of machine behavior in system data is a better approach for detecting new types of persistent, stealthy malware-based attacks.

"Rules-based SIEMs aren't designed to detect polymorphic attacks or patterns from advanced persistent threats."



Fraud Detection

Splunk can discover evolving fraud patterns with real-time search across all of your web access and transaction logs. Complex, suspicious patterns can be found with correlations and transaction searches, these can also be scheduled to generate proactive alerts. Audit trail and data signing preserves chain-of-evidence for audits or if you need to prosecute or take civil action.

"Our Security team detects and investigates fraudulent activity as it happens."



Insider Threat

Malicious insiders are often the source of the most damaging security incidents. Detecting logic bombs and data thefts that circumvent application controls and malicious scripts is reactive at best with cumbersome manual analysis. Specialized monitoring tools don't cover many of the data sources where insiders leave trails.

Splunk lets you monitor user behavior before malicious activity can impact your business.

"Splunk helps us find what we are looking for—and it discourages criminal behavior. Would-be fraudulent users know they will be found now."



Network Security

The volume of IDS, IPS and other security events and alerts can overwhelm security teams. Meanwhile, traditional SIEM tools are expensive, don't scale well and involve the installation and maintenance of complex and costly adapters for every data format and source. In addition, significant storage overhead is required to retain this data. The result of this scale and complexity is that many potential intrusions go unchecked increasing exposure and risk. Splunk helps you with immediate assessment and containment of events and alerts. With Splunk you can Search, in seconds, across all your network elements and security components from one place. Index IDS, IPS, vulnerability data, firewall scans and network device logs—from any vendor technology. Long-term data can be retained with chain-of-evidence and data signing for audits or formal investigations.

"Splunk allows us to quickly consolidate and correlate disparate log sources, enabling previously impractical monitoring and response scenarios."



Real-time Correlation and Alerting

Correlation of information from different data sets can reduce false-positives and provide additional insight and context. For long-term correlations, Splunk can write individual system events to internal files also monitored by Splunk and aged out over time. If the right group of events writes to the file, before it is aged out, the correlation is completed and an alert is issued.

"Splunk real-time alerts help us to see abuse and fraud activities as they happen."



Splunk for Security – Features

- Index any type of machine data from any source
- Search and report on any combination of real-time streaming and historical data
- Set real-time alerts that track correlated events with built-in notification throttling and thresholds
- Powerful search language enables sophisticated correlation without hard-to-write rules
- Monitor patterns of activity for anomalies and outliers
- Report on incidents and risk across multiple security products
- Keep up with change—no models or rules to maintain
- Automatic knowledge capture through event tagging, field naming and extraction
- Real-time APIs allow Splunk to either compliment or replace a SIEM implementation

Get Started Today !

Website: www.splunk.com

Address: 250 Brannan St, San Francisco, CA, USA, 94107

Email: info@splunk.com | sales@splunk.com

Phone: +1 866-438-7758 | +1 415-848-8400

Download: www.splunk.com/download