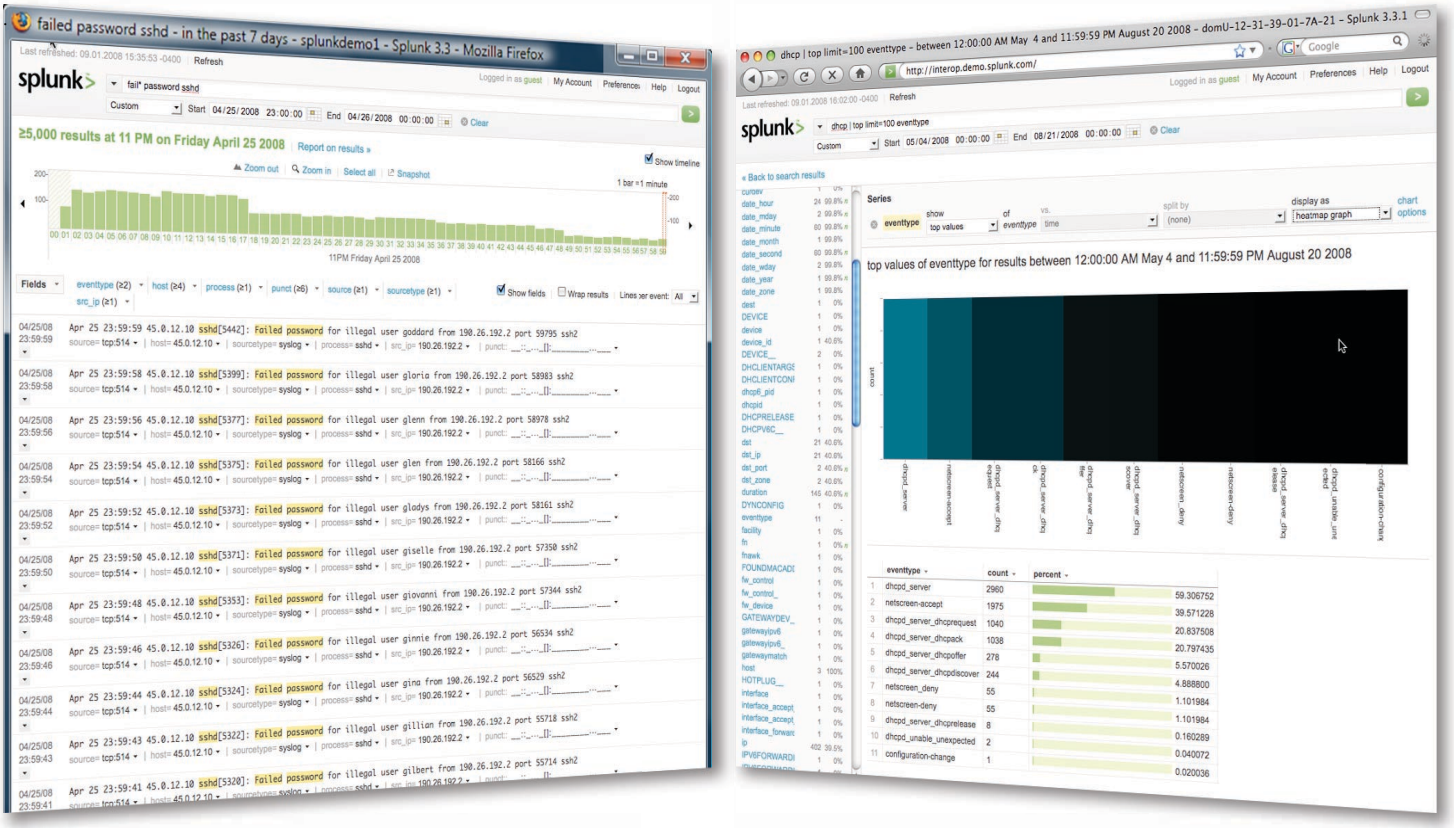
Splunk for Security

A new approach to enterprise security. IT Search makes all your IT data security-relevant.
Gain situational awareness across technology silos and speed incident response.



Situational Awareness

Splunk IT Search is the scalable, flexible way to embrace the onslaught of security events and information from across your entire application stack. Achieve situational awareness by integrating real-time information from security and network devices, operating systems, databases, and applications. Use ad-hoc search across all your technologies and data to trace misuse, data leaks, attackers, or malicious insiders. Spot troublesome trends before they result in successful compromises.

- Data Leakage and Security
- Fraud Detection
- Insider Threat
- Misuse
- Network Security

Faster, more comprehensive incident response and forensic analysis means lower exposure and risk, as well as reduced cost. Splunk provides a comprehensive view across silos - from IDS, firewalls, proxies, access control systems and SIEMs to applications, configurations and system specific attributes. Rich visualization and reporting provides quickly understandable views into your security posture. Through a more comprehensive picture into the changing threat landscape you can more quickly assess and resolve security incidents.

The old way

Silos of data hinder incident response.

You've deployed a wide variety of technologies, but still can't get to the bottom of your security incidents. The volume of false-positives from your security technologies are overwhelming and you are dealing with too much inaccurate data to complete the full picture. Your security issues are not detected by your security technologies but through other sources, such as customer complaints. Fraud and misuse investigations lack the necessary data, even though you are collecting a huge amount of security events. External attacks are too hard to investigate due to slow and cumbersome ad-hoc investigations. Change and configuration monitoring isn't integrated as part of your security posture.

The new way

Splunk provides situational awareness.

Gather all the data necessary to monitor the threats posed to your organization. Use Splunk as your central repository where you can search, alert, and report in real time on any user, network, system, or application activity. You can correlate data from across your application stack to solve fraud, misuse, data security, insider threat, and network security problems. Detect misuse early and assess the impact to quickly mitigate the exposure, resulting in reduced risk.

Splunk for Security Use Cases

Data Leakage and Security

Information silos in today's IT infrastructures mask suspect data flows. Security teams are inundated by events and alerting data from: SIEMs, content monitoring and filtering devices, data-at-rest and encryption technologies, client security suites, and network access controls. And security information management tools lack easy support for ever changing data formats.

"We investigated reports of data leakage in seconds by searching activity for a specific user or URL. Integrating new data sources was easy. We got the complete picture."
David Hazekamp, Former Security Architect, Motorola

Splunk pinpoints leaks quickly. Search across silos and follow the winding paths of data leakage attempts. Search content monitoring logs, firewall activity, and logs from email, IM, Web proxies and client security to understand any scenario. Transaction searches find complex suspicious patterns that are hard to identify. Integrate with SIEM and security monitoring tools for one-click investigations.

Fraud Detection

Phishers and scammers are continuously thinking of new ways to compromise customer accounts and try to take advantage of any loopholes in transaction and system architectures. Rigid and narrow monitoring and analysis tools are no match against constantly evolving threats and can't help with zero-day scenarios.

"Splunk's ability to collate and report on any log file or data stream helps us detect and investigate fraudulent activity quickly."
Peter Bassill, CISSP, Gala Coral Group

Splunk discovers evolving fraud patterns. Search across all of your Web access and transaction logs in real time. 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 features preserve chain-of-evidence for audits or if you need to prosecute or take civil action against perpetrators.

Insider Threat

Malicious insiders are the source of the most damaging security incidents. Detecting logic bombs, 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 us monitor privileged user activity on sensitive systems to proactively detect insider threats and reduce our exposure and risk."
Trevis Edgeworth, Senior Director Network Architecture, Epsilon Data Management

Splunk threads together insider steps. Search across every place a malicious insider may have passed through to steal information or plant something dangerous. Alert on patterns of badge access, administrative logons, access to given files and script or configuration change through application logs, database access, file system changes, and authentication system events.

Misuse

Misuse of Web surfing, network access and other resources drives up IT costs and exposure. But there is no way to alert on many policy violations without maintaining homegrown scripts. Wasted resources, HR and legal exposure go unchecked as cumbersome approaches allow misuse to continue.

" Splunk's made the job of tracing user steps a lot easier. We have more information at our fingertips than ever before."
Allen Hecker, Senior Security Engineer, Weill Cornell Medical College

Splunk reveals policy violations. Search across the complete datacenter stack of technologies to monitor user activity. Index logs from Web proxies, firewalls, servers and applications. Discover complex instances of suspicious patterns with transaction searches and turn them into alerts for proactive monitoring.

Network Security

The volume of IDS, IPS and other security events and alerts are overwhelming to security teams. SIEM tools are very 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 allows us to quickly consolidate and correlate disparate log sources, enabling previously impractical monitoring and response scenarios."
Gavin Reid, CSIRT Manager, Cisco Systems

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 and traps. Retain long-term data with chain-of-evidence and data signing for audits or formal investigations. A wide variety of pre-programmed searches, alerts and reports will improve your security monitoring coverage right away.

Ad-hoc Investigations

It's what you don't know that can hurt you. Flexible IT Search injects new power into your investigations. There are no schemas or databases to slow you down, or canned reports to limit your findings. You will find "the needle in the haystack" and get visibility into the impact of zero-day attacks using Splunk.

Features

- Index any type of IT data from every source
- Search your entire infrastructure from one place
- Powerful search language enables sophisticated correlation without hard-to-write rules
- Distributed search across silos to enable holistic analysis
- Turn any search into a proactive alert
- Report on incidents and risk across multiple security products
- Keep up with change - no models or rules to maintain
- Powerful knowledge capture through event tagging, field naming and extraction
- Share alerts and data with service providers and other tools
- Secure, policy-based access to IT data enables production controls
- Launch searches contextually from any existing console

Get Started Today !

- Download your own free copy of Splunk today at www.splunk.com/download.
- Visit www.splunk.com/security for tips, tricks and apps to help get off the ground with Splunk for Security.