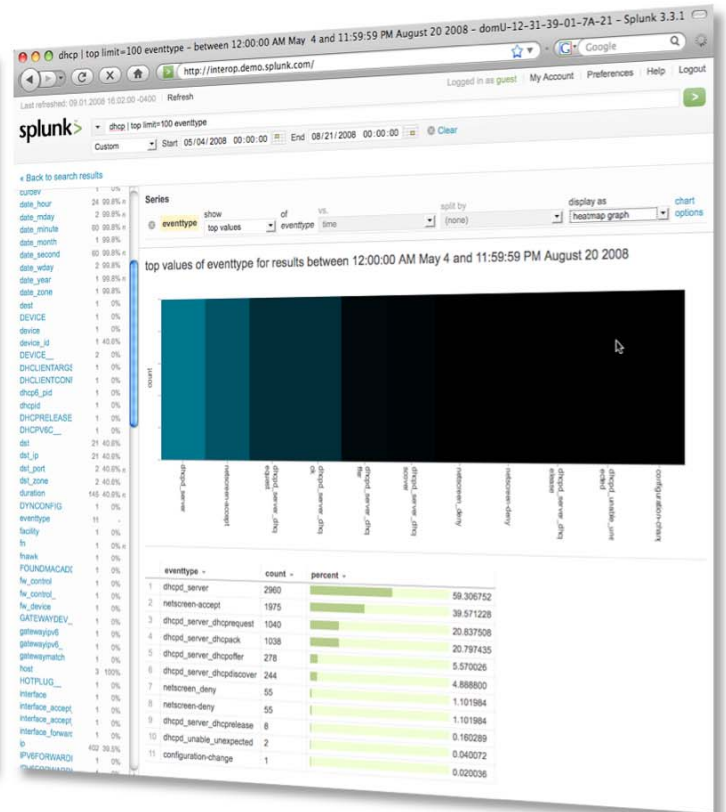


# Splunk for Security

IDS, firewalls, proxies, access control systems, and SIEMs generate huge amounts of security data. Unify diverse sets of data and consoles and speed security incident response.



## Situational Awareness

Splunk IT Search is the scalable, flexible way to embrace the onslaught of security events and information in your environment. Achieve situational awareness by integrating real time, ad-hoc search across all your security technologies and data. Trace the trail of an attacker in minutes and spot troublesome trends, events and incidents before attacks succeed and your infrastructure is compromised.

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

Faster, more comprehensive incident response means lower exposure and risk. Splunk provides a consolidated deep dive repository of all your heterogeneous security data in one place. Search, alert and report in real time across all your security technologies. .

Rich visualization and reporting provides quickly understandable views of your security posture so you can identify unanticipated threats before vulnerabilities occur and continuously observe the complete changing threat landscape.

## The old way

Data overload hinders incident response.

You've deployed a wide variety of security technologies but still can't respond quickly to security incidents. Overwhelming numbers of alerts mean you can't easily decide which require response. To effectively track the trail of an attacker you have to use multiple consoles – one window to look at outgoing web traffic, another for authentications and still another for DHCP leases. Analysis of a serious incident can take days. Ad-hoc investigations are slow and cumbersome and you don't have the fast access to all your data sources in real time that you need.

## The new way

Splunk provides situational awareness.

Search all your security data for fast incident response. Merge in other intelligence like trouble tickets and cyber threat data. With Splunk you can search, alert and report in real time on any user, network, system or application activity. Eliminate the need for multiple consoles and follow the trail of an attacker from one place. Now you can perform more in-depth analysis and respond to incidents faster and more thoroughly, lowering your exposure and risk.

# Splunk for Security Applications

## 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, data-at-rest encryption, client security suites, network access controls. Volume of data overwhelms existing technologies. And security information management tools lack easy support for every changing data formats



**"We investigate reports of data leakage in seconds by searching activity for a specific user or URL. Integrating new data sources is easy. We get the complete picture."**

Dave Hazecamp, 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 legitimate customers' accounts and take advantage of loopholes in transaction and system architectures. Diverse, constantly evolving threats defeat rigid and narrow monitoring and analysis tools and don't help with zero day scenarios.



**"Splunk's ability to collate and report on and log 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 transaction searches and scheduled to generate proactive alerts. Audit trail and data signing features preserve chain-of-evidence 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."**

Travis 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, physical badge access systems 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 data center stack of technologies to see what users do. Index logs from web proxies, firewalls, servers and applications. Find instances of complex suspicious patterns with transaction searches and turn them into alerts for proactive monitoring.

## Network Security

Volume of IDS, IPS and other security events and alerts overwhelm security teams. SIEM tools are expensive and don't scale well involving the installation and maintenance of multiple adapters for every data format and significant storage overhead to retain data. As a result 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's real time search helps you with immediate assessment and containment of events and alerts. Search in just seconds across all your network elements and security components from on 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 potential prosecution. A wide variety of pre-programmed searches, alerts and reports will improve your security monitoring coverage right away.

## 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
- Everyday use capture and sharing knowledge
- 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](http://www.splunk.com/download).
- Visit [www.splunk.com/security](http://www.splunk.com/security) for tips, tricks and applications to help get off the ground with Splunk for Security.