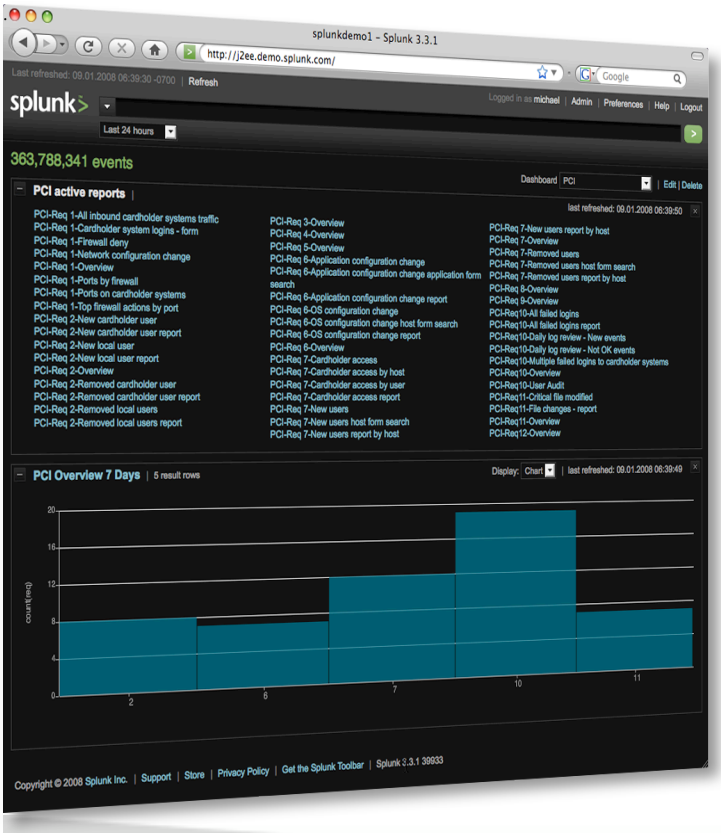
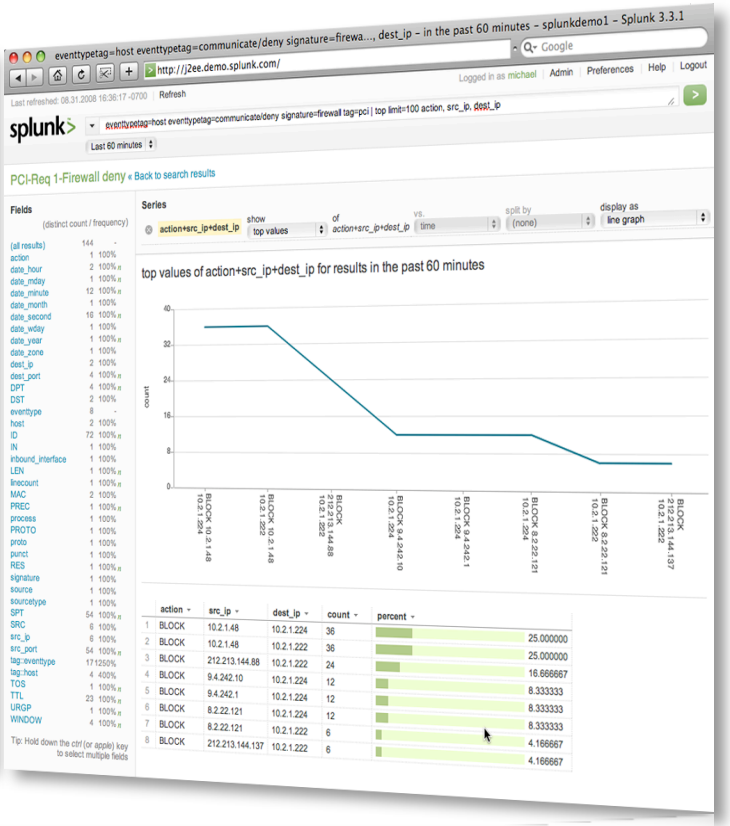
splunk>

Splunk for Compliance

Compliance drives new requirements to monitor, alert and report on logs and IT data. But the data is scattered everywhere and it's difficult to access, analyze and manage.





Cost effective, sustainable compliance.

Splunk IT Search is the cost effective and flexible way to meet your compliance requirements from audit trail collection and reporting, to file integrity monitoring with a single solution.

Meet requirements to collect, retain, search, alert and report on logs and IT data scattered about the data center. Generate any report in seconds and automate reporting to compliance analysts and auditors with scheduled searches and reports.

- **e-Discovery** - Search every data source required for e-Discovery from one place. Get instantaneous results across large data sets.
- **FISMA** - Securely collect, index and store all your log and IT data along with audit trails to meet NIST requirements.
- **HIPAA** - Search all your IT data to instantly assess reports of EPHI leakage and meet HIPAA's explicit log requirements.
- **PCI** - Rapid compliance with PCI requirements for log retention, review and change monitoring, comprehensive reporting on all PCI controls such as passwords and firewall policy.
- **SOX** - Make the ambiguous chore of compliance-mandated routine log review easy and straightforward.

Demonstrate "due-care" and increase operational efficiency by eliminating compliance friction.

The old way

Complex, deficient log management.

Reporting on firewall, access control and application logs and IT data to demonstrate compliance controls is difficult and costly. Each of these systems generate logs in different formats and locations. Each auditor request involves a different, manual procedure. But the requirement to limit access to production systems has an even bigger impact. System administrators and developers are denied access to production systems to analyze logs and configurations, limiting their ability to respond to operations and security incidents.

The new way

Efficient, low maintenance compliance.

Bring powerful tools to the challenges of change management. With Splunk you can search, alert and report on any type of IT data from all your sources. Meet compliance requirements from audit trail collection and reporting, to file integrity monitoring with a single solution. Generate any compliance report in seconds. Give developers and application support secure, read-only remote access to the IT data they need to diagnose application and service problems via Splunk, without taking the operational hit imposed by demands to restrict login access to production systems.

Copyright© Splunk Inc. 2008 All rights reserved.

Using Splunk for Compliance

Secure data retention

Splunk provides the most efficient and secure solution for capturing and retaining all of your IT data for extended periods. Securely capture all your data in real time including syslog and even complex application logs. Hardened deployments and comprehensive auditing and security ensure integrity. Archive or retire data based on age or storage limits.

Controlled data access

Splunk eliminates the compliance barriers that get in the way of operations. Provide developers and application administrators real-time access to all of the logs, configurations and status commands they need in order to analyze and resolve production problems. Role-based access controls let you adhere to strict compliance with production server access restrictions.

Compliance reporting

Meet explicit requirements to monitor, review and retain logs, configurations and other IT data. Demonstrate compliance quickly and easily across all other types of controls. Report on firewall activity to show that firewall policy is in place and functioning correctly. Report on access control events to show that account deactivation procedures are being followed. Generate ad-hoc reports to answer any auditor question in seconds and automate reports with scheduled searches.

Security monitoring

Splunk lets you meet requirements to automate monitoring of security events. Index audit trails across firewalls, applications, access control, IDS and any other component, then simply save, schedule and set alerting rules for any search. Alerts can send notifications via email, RSS, SMS or trigger scripts for easy integration with your existing monitoring consoles. As new mandates create new monitoring requirements, simply add new data sources and searches.

Compliance investigations

Minimize the distraction of compliance investigations and discovery requests. Stop using a different tool for each of your systems - web proxies, email servers, and more. Splunk's fast and simple search across all your data will get you the information in seconds.

Audit trail review

Splunk makes the ambiguous chore of compliance-mandated routine log review easy and straightforward. Search Splunk daily for all activity from the previous day on in-scope servers. Use Splunk's time histogram and filters to understand patterns. Classify and tag innocuous events as "ok". Search for events not tagged "ok" the next day so that you're only looking at new or suspicious events each day. Best of all, Splunk tracks your review history for auditors.

Splunk for Compliance Applications

e-Discovery

Escalating legal requests to investigate online activity are distracting IT staff at educational institutions and large enterprises. Servicing requests is distracting and time consuming and the inability to respond effectively opens organizations to legal risk.

"When the FBI is asking for intelligence under a tight timeline, you need to be able to search your IT data and generate any material findings quickly."

Anonymous

Splunk makes e-Discovery fast and easy. You can search every data source required for e-Discovery from one place. Instantaneous results across large data sets slash the time to respond to requests. Set up simple searches for HR personnel to lift the burden from IT staff. Data signing and audit trails demonstrate the integrity of your results.

FISMA

FISMA and NIST standards require Federal Government Agencies have the ability to effectively respond to incidents by analyzing massive amounts of data from large network and IT infrastructures. Splunk scales to provide visibility into every security technology in large network infrastructures. Powerful search and reporting of results and flexible ways to organize and tag systems with inventory information enable the creation of status views for any security control or location.

"Federal agencies should implement Splunk because it can bring all the security information together, correlate and bring a coherent picture of your security posture."

Bill Hornish, Federal Business Development, Splunk

HIPAA

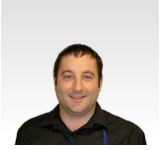
HIPAA and EPHI security and privacy rules include explicit requirements for audit trail collection, review, automated monitoring and incident investigation. But providers and insurance carriers lack the ability to rapidly search IT data in support of incident investigation requirements. Slow, manual investigation processes raise the level of exposure and risk of violations. Splunk closes HIPAA compliance gaps. Search all your IT data to instantly assess reports of EPHI leakage and meet HIPAA's explicit log collection and monitoring requirements.

"Splunk is the CHW standard for event logging for HIPAA. It's a critical tool for monitoring access to information to our business, and the privacy of our patients."

Steve Hight, Director Strategic Technology, CHW

PCI DSS

Credit card merchants find collecting and retaining audit trails for at least one year is the most daunting PCI compliance requirement. It's difficult to access, analyze and manage all the data from card processing systems. Existing PCI solutions are expensive, clumsy and difficult to maintain. Splunk for PCI Compliance is a pre-packed application that provides rapid compliance with PCI requirements for audit trail collection, retention and review.



"Failure to comply with PCI equates to failure for our business. Splunk enables us to demonstrate compliance across all PCI DSS requirements."

Peter Bassill, CISSP, Gala Coral Croup

SOX

Demonstrating IT controls based on ITIL, COBiT, COSO, ISO 17799, BS-7799 and other IT operations frameworks has become an immense burden for IT. Ad-hoc requests to report on everything from firewall to wireless access point activities distract from regular duties. Splunk provides comprehensive visibility for SOX IT controls. Search all the data generated by SOX control tools and technologies from one place for instantaneous retrieval of any information requested by IT auditors.

"Splunk automated our evidence gathering for SOX compliance, saving engineering from working on compliance related tasks."

"David Jones, IT Ops Manager, Alexza Pharmaceutical

Get Started Today !

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

Copyright© Splunk Inc. 2008 All rights reserved.