splunk> listen to your data™

Splunk for Compliance

Meet Compliance Requirements by Monitoring, Alerting and Reporting on Machine Data

Cost effective, Sustainable Compliance

Splunk Enterprise is a massively scalable data engine for machine-generated data. It collects, indexes and harnesses machine data across your infrastructure in real time. Splunk offers a 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 machine data throughout your IT infrastructure. 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 Machine Data along with audit trails to meet NIST requirements.
- HIPAA - Search all your machine data to instantly assess reports of EPHI leakage and meet HIPAA's explicit log requirements.
- PCI - Rapid compliance with explicit PCI requirements for log retention/review and change monitoring, comprehensive reporting on all PCI controls such as passwords and firewall policy.
- SOX - Splunk makes the ambiguous chore of compliance-mandated routine log review easy and straightforward.

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

The Compliance Challenge

Reporting on firewall, access control and application logs and machine 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.

Enter Splunk

Bring powerful indexing, search, alerting and reporting to the challenges of change management. With Splunk you can search, alert and report on machine data from virtually any source. Meet compliance requirements from audit trail collection and reporting, to file integrity monitoring with a single solution. Generate any compliance report in seconds. And you'll overcome the operational impact of demands to restrict production system access by giving developers and application support secure, read-only access to the machine data they need without touching production systems.

Secure data retention

Splunk provides a highly efficient and secure solution for capturing and retaining your machine data for extended periods. Securely capture all your data in real-time including syslog and even complex application logs. Integrity is ensured via hardened deployments and comprehensive auditing and security. Archive or retire data based on age or storage limits.

Controlled data access

Splunk helps eliminate the compliance barriers that get in the way of operations. Provide developers and application administrators with real-time access to 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 machine data. Demonstrate compliance quickly and easily across 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 auditor questions 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 other components, then simply save, schedule and set alerting rules for a 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 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 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 law enforcement requests to investigate suspected criminal activity online are distracting IT at education institutions and large enterprises that provide Internet access. Servicing requests is a 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 the security technologies in large network infrastructures. Powerful search and reporting of results and flexible ways to organize and tag systems with inventory information and enable the creation of status views for different security controls or locations.

> **"Federal agencies should implement Splunk because it's 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 machine data in support of incident investigation requirements. Slow, manual investigation process raises level of exposure and risk of violations. Splunk closes HIPAA compliance gaps. Search your machine 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 patient privacy."**
>
> **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. The Splunk App 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

Sarbanes-Oxley IT compliance has driven public companies and their vendors to adopt stringent IT controls based on ITIL, COBiT, COSO, ISO 17799, BS-7799 and other best-practice frameworks for IT operations and security. Demonstrating these controls has become a huge burden for IT operations, Splunk provides comprehensive visibility for SOX IT controls. Search the data generated by SOX control tools and technologies from one place. Instantaneous retrieve the 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

Free Download

Download Splunk for free. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.

splunk> listen to your data™