splunk>

Splunk for PCI Compliance

The old way:

Complex, deficient PCI log management.

Collecting and retaining audit trails for at least a year is among the most daunting requirements for PCI compliance. It's difficult to access, analyze and manage all the data. Legacy solutions demand constant maintenance and are open to question by auditors. Implementing adequate integrity controls is a significant technical challenge.

Demonstrating compliance involves generating ad hoc reports on administrative logs generated by other compliance-mandated technologies such as firewalls, access control systems and applications. Each of these systems generate logs in different formats and locations. Each auditor request involves a different, manual procedure.

Point log management appliances are heavyweight yet limited solutions for collecting and reporting on logs and audit trails. They don't work with custom applications, require constant maintenance to keep up with constantly changing data sources, and offer little operational benefit apart from compliance.

Beyond the explicit PCI requirements for log monitoring and retention, the requirement to limit access to production systems has an even bigger, though often misunderstood, impact. When developers and application administrators are denied access to production systems to analyze logs and configurations, they are thwarted in finding and fixing problems with revenue-generating applications and services.

The new way:

Simple, complete PCI log management.

With Splunk you can Search, alert and report on any type of IT data to address the complete range of PCI related IT data issues and requirements.

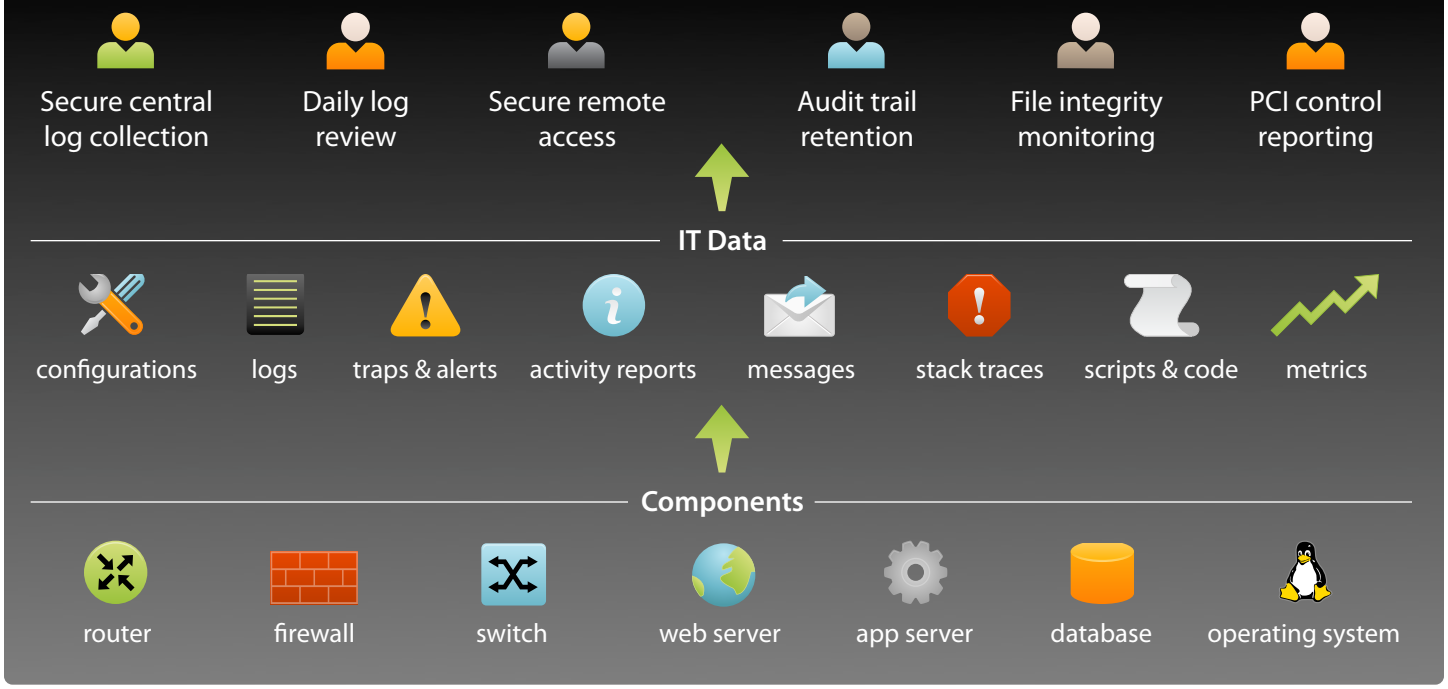
Generate reports in seconds to prove compliance with any PCI control, from password policy to firewall configuration. Comply with PCI's explicit log collection, review and retention requirements across all of your infrastructure including file integrity monitoring.

Best of all, Splunk lets you overcome the barriers introduced by PCI-mandated access restrictions - so you don't have to impact operations for compliance.

Benefits

- Rapid compliance with PCI requirements for audit trail collection, retention and review
- Meet requirements for file integrity monitoring
- Prove compliance with all PCI controls
- Answer any auditor data request in seconds
- Increase availability by overcoming PCI-mandated access restrictions
- Control access to sensitive data

Solution at a Glance



Using Splunk for PCI

Secure central log collection *(Requirement 10.5)*

Splunk provides the most comprehensive solution for PCI's explicit requirement for secure log collection. Just configure all your network devices and servers to direct syslog-NG at Splunk over an encrypted tunnel. Deploy Splunk to application hosts to capture file-based logs in real-time and forward them securely to your central Splunk index. Real-time centralization is critical to avoid an attacker covering their tracks by compromising the audit trail prior to it being forwarded to the log host. Because Splunk signs your data at point of capture, a single click in Splunk search results checks the integrity of your data anytime.

Daily log review *(Requirement 10.6)*

Splunk makes the chore of daily log review light work with fast search, visualization and tagging. 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". Then, search for events not tagged "ok" the next day so that you're looking only at new or suspicious events each day. Best of all, Splunk tracks your daily review history for your auditors.

Secure remote access *(Requirement 7.1)*

Splunk eliminates the hidden toll PCI takes on availability by providing secure, remote access to all IT data despite strict production controls. PCI mandates that you limit access to servers that store or transmit cardholder data. In practice, this means developers and administrators who keep your revenue-generating systems running don't have access to the production systems. With Splunk, you can keep your business running AND keep the auditors happy. Use Splunk as a real-time window into application logs, system status, configurations, and anything else developers or administrators need to know to keep things running.

Audit trail retention *(Requirement 10.7)*

Splunk keeps the cost and hassle of retaining logs for PCI under control. Splunk stores your data in an efficient, compressed format and lets you control data retention by age. Want to keep things simple? Set Splunk to retire data after exactly one year. Want to save on storage? Set Splunk to archive compressed raw data only nearline after a few weeks and restore the archive on demand. The choice is yours.

File integrity monitoring *(Requirements 10.2.2, 11.5, 10.5.5)*

With Splunk, you don't need to buy one tool for configuration auditing and another for log management. Capture and index changed files for audit trails and administrative actions. Since few systems are configured to log every command issued by root users, Splunk creates an audit trail by watching relevant files and directories. Alerts can send notifications via email, RSS, SMS or trigger scripts for easy integration with your existing monitoring consoles. Alerts can also trigger automated actions to immediately react to certain conditions.

Features

- Indexes every type of IT data from every source
- Monitors configuration file changes
- Automates compliance reporting across all components
- Flexible and fast search lets you meet any auditor data request in seconds
- Accelerates mandated daily audit trail review with event classification, visualization and tagging
- Flexible alerting and reporting across all IT data
- Secure, policy-based remote access to IT data mitigates the impact and violations of access restrictions
- Lets you share alerts and data with service providers and other tools
- Over 40 reports to accelerate reporting across PCI compliance mandated controls, from firewall configuration to password management
- Over 85 saved searches to facilitate ad-hoc investigations of incidents involving cardholder data
- Over 15 alerts to automate policy compliance monitoring

PCI control reporting *(All requirements)*

Splunk not only gives you compliance with key PCI requirements, but it lets you demonstrate compliance quickly and easily across all PCI-mandated controls. Report on firewall logs to show that firewall policy is in place and functioning correctly. Report on access control administrative logs to show that account deactivation procedures are being followed. Automate reporting by scheduling any search for delivery via email and RSS. Put key charts on dashboards for compliance and security managers to oversee compliance activities. Generate ad hoc reports to answer any auditor question in seconds.

Get Started Today !

Download your own free copy of Splunk today at www.splunk.com/download.

Visit www.splunk.com/PCI for tips, tricks and applications to help get off the ground with Splunk for PCI Compliance.