

# Splunk for PCI Compliance

## Address the Complete Range of PCI DSS Log and Data Issues and Requirements

### Easy PCI Compliance

The Splunk for PCI application is built on the Splunk engine for machine-generated data. Use this powerful combination to search, alert and report on any type of machine-generated data to address the complete range of PCI requirements.

- Meet key PCI DSS requirements for log collection, audit trail collection, file integrity, monitoring, retention and review
- View your current compliance posture with the PCI DSS scorecard
- Use PCI dashboards to monitor log information requirements related to:
  - Access Control
  - Cardholder Data
  - Network Security
  - Endpoint Security
  - Monitoring and Testing
- Investigate cardholder data issues with Splunk search in real-time
- Accelerate reporting across PCI controls, from firewall configuration to password management, with pre-defined views
- Create custom alerts to automate policy monitoring

### The Old Way

#### Complex, deficient PCI log management.

Collecting and retaining audit trails is daunting and implementing integrity controls is a significant technical challenge. Demonstrating compliance involves creating ad-hoc reports from administrative logs generated by other compliance-mandated technologies like firewalls, access control systems and applications. Each of these systems generate logs in a different format and location and every auditor request involves a different manual procedure. Appliances are heavyweight and limited solutions for collecting and reporting on logs and audit trails that don't work with custom applications, require constant maintenance and offer little operational benefit.

### The Splunk Way

#### Simple, complete PCI log management.

Splunk can address all your PCI requirement needs—use it to generate reports in seconds to prove compliance with any PCI control, from password policy to firewall configuration. Comply with the explicit log collection, review and retention requirements across your entire infrastructure, even for file integrity monitoring.

Use dashboards to quickly view compliance status and identify gaps. Best of all, Splunk lets you overcome the barriers introduced by PCI-mandated access restrictions so you don't have to impact operations for the sake of compliance.

### Using Splunk for PCI Compliance

#### Secure Central Log Collection (Requirement 10.5)

Splunk is the most comprehensive solution for the secure log collection mandated by PCI. Just configure all your network devices and servers to direct a syslog-ng stream at Splunk over an encrypted tunnel. Because Splunk signs your data at the point of capture, a single click into a Splunk search result will check the integrity of your data.

#### Daily Log Review (Requirement 10.6)

Splunk makes the chore of daily log review light work with its fast search, visualization and tagging capabilities. You can classify and tag innocuous events as “OK”, then search for outliers from day-to-day so that you're only looking at new or suspicious events. Splunk always tracks your daily review history, satisfying auditor conditions for data access logging.

### Supported Platform Requirements

Splunk ESS 1.1.1 will run on Splunk version 4.1.6 or greater up to and including Splunk version 4.2. For a list of Splunk supported operating systems, please see <http://www.splunk.com/download>.

### Splunk for PCI Reporting & Monitoring

#### File Integrity Monitoring (Requirements 10.2.2, 10.5.5, 11.5)

Splunk captures and indexes changed files for audit trails and administrative actions so you don't need to buy one tool for configuration auditing and another for log management.

Relevant files and directories are monitored to create an audit trail, and alerts can send notifications via email, RSS or SMS. Splunk alerts can even trigger scripts to easily integrate with your existing monitoring consoles.

### Audit Trail Retention (Requirement 10.7)

Splunk keeps the cost and hassle of retaining logs for PCI under control by storing your data in an efficient, compressed format and allowing you to control data retention by age.

### Secure Remote Access (Requirement 7.1)

Splunk provides secure, remote access to all machine generated data despite strict production controls, eliminating the hidden toll PCI takes on availability. 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.

Splunk lets you demonstrate compliance quickly and easily across all PCI-mandated controls by monitoring and reporting on compliance status across all requirements.

### Network Security (Requirements 1 and 2)

Splunk automates the monitoring and reporting of network security with views, look-ups and searches that summarize the activity of default accounts still in use, changes to firewalls and routers, non-approved services, ports and protocols and restricted network connections that may impact cardholder data.

### Cardholder Data (Requirements 3 and 4)

Splunk ensures cardholder data is properly protected with on-demand search capabilities that identify credit card numbers stored in clear text, enabling you to verify that connections are restricted between untrusted network and system components in the cardholder data environment.

### Endpoint Security (Requirements 5 and 6)

The Splunk for PCI Malware Center monitors the current state of your malware protection with key statistics and the ability to configure and monitor thresholds. Use the System Update Center to report on systems that have and have not been updated and see which systems have been up for the longest time.

### Access Control (Requirements 7, 8 and 9)

Splunk's Access Control Dashboard summarizes the current state of authentication events so you can quickly identify gaps in access control requirements. Included are over fifty on-demand searches that provide successful and failed authentication events in multiple combinations.

### Monitoring & Testing (Requirements 10 & 11)

Splunk for PCI automates and simplifies monitoring and testing with capabilities to correlate application, OS and identity management systems. You can define access policies and then quickly discover, report and alert on violations, exceptions and anomalies. Use the Ad-hoc search capabilities, user and

system access tracking and correlations to facilitate forensics investigations.

Using Splunk, you'll be able to answer any auditor data request in seconds, increase availability by overcoming PCI-mandated access restrictions and control access to sensitive data by user or role.

## Features

- Indexes all machine-generated data from any source
- Monitors configuration file changes
- Automates compliance reporting across all components
- Meets any auditor data request in seconds
- Accelerates mandated daily audit trail review with event classification, visualization and tagging
- Provides flexible alerting and reporting across all machine-generated data
- Mitigates the impact and violations of access restrictions with secure, policy-based remote access to all relevant data
- Shares alerts and data with service providers & other tools
- Triggers automated actions with alerts to immediately react to certain conditions
- Accelerates reporting from firewall configuration to password management

## 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](mailto:sales@splunk.com).