Simplified PCI Compliance

The Splunk® App for PCI Compliance is built on top of the Splunk Enterprise® indexing and analytics engine for machine-generated data and events. The Splunk App for PCI Compliance is used to meet PCI requirements around log retention and review; to measure the effectiveness and status of PCI compliance technical controls; to identify and prioritize any control areas that may need to be addressed; and also to quickly answer any auditor report or data request. The app features:

- Continuous, real-time monitoring of PCI DSS compliance
- Scorecards and reports to measure compliance against key PCI requirements trackable in machine data
- Pre-built, real-time searches and visualizations to quickly identify and prioritize areas of PCI non-compliance
- Awareness and prioritization of in-scope assets and employees via integration with asset and employee directories
- Incident review and workflow capabilities to quickly investigate and remediate areas of non-compliance
- Audit trail for log review and report accesses
- Flexible search capabilities to quickly answer any auditor data request

Together, the Splunk App for PCI Compliance and Splunk Enterprise combine to create an automated and highly scalable solution to help measure and ensure PCI compliance.

Current PCI Compliance Pains

Collecting and retaining data for audits is daunting and implementing integrity controls is a significant technical challenge. For most PCI solutions, ingesting the wide variety of operational and security data types with a myriad of formats requires pre-collection data normalization. This activity can require constant maintenance and can quickly become someone's full-time job. This is particularly problematic when custom applications are in-scope for PCI compliance. Splunk software's ability to index any machine-generated data lets you focus more on analysis and less on data collection.

Some available solutions support an organization's PCI compliance needs with so-called “report-packs or modules” that are add-on components to a SIEM. Yet simply having canned reports alone will not help you become PCI compliant. The PCI DSS standard has been a requirement for merchants who accept credit cards since 2004. While it has undergone significant changes since its inception, PCI DSS is now considered a mature standard. As such, a PCI auditor may request that you demonstrate proficiency in data analysis and investigation of a potential PCI issue—clearly beyond the scope of canned reports. Splunk Enterprise makes this a simple exercise. Many solutions don’t provide an easy way to get from high-level dashboards to raw data. Others don’t provide an easy way to separate in-scope systems from those that aren’t, creating the possibility of inaccurate reporting.

Simple, Complete PCI Log Management, Reporting and Incident Tracking With Splunk

The Splunk App for PCI compliance and Splunk Enterprise can address your key PCI requirement auditing and reporting needs. Use it to easily ingest any data source, view compliance in high level reports, scorecards and dashboards and automate the log review process. As compliance issues are discovered, built-in workflows allow the right person to be notified with a detailed view of the issue to be addressed and corrected. Most importantly, your PCI posture is continuously monitored—so there will be no more end-of-the-quarter fire drills.

The Splunk App for PCI Compliance is a stand-alone application that organizes and presents visualizations to help you identify and address PCI compliance gaps while providing fast triage, drill-down and root cause analysis drill-down that Splunk Enterprise offers.

Splunk and OperationalizingPCI Compliance

Splunk directly helps with PCI DSS Requirement 10, which calls for the logging, monitoring and retention of all access to network resources and cardholder data. Splunk is able to support requirement 10 by indexing authentication-related event data and log files. In addition, Splunk software can also measure compliance against PCI DSS requirements 1-8 and 11 by indexing machine data and events from the cardholder environment relevant to these requirements, which includes data sources such as firewalls, anti-malware, data loss prevention, vulnerability scanners and intrusion detection systems.
The Splunk App for PCI Compliance then runs pre-built Splunk searches against this machine data to identify and highlight areas of PCI non-compliance. Examples of non-compliance on a PCI network include default user accounts being used, endpoint protection not running, or credit card numbers being transmitted unencrypted. More detail on the PCI DSS requirements tracked and measured in the Splunk App for PCI Compliance are below. For each requirement, the Splunk App for PCI Compliance has pre-built scorecards, reports and correlation searches.

**Requirement 1. Install and maintain a firewall configuration to protect cardholder data.** Grab the logs from your internal and external firewalls and store them centrally in Splunk Enterprise. Use Splunk software to monitor traffic patterns to and from cardholder systems to the internal network and other networks and/or systems that are considered untrusted. Track and report on firewall changes and rule usage to ensure that the firewalls are protecting the cardholder environment as expected.

**Requirement 2. Do not use vendor-supplied defaults for system passwords and other security parameters.** The security configurations of the systems within the cardholder data environment are the first line of defense against malicious attacks. Malicious individuals will often use the default configurations and other default settings, user accounts and passwords to compromise systems. These settings are well known in the hacker communities. Applying thorough and meaningful hardening standards makes it more difficult for people to access your systems.

**Requirement 3. Protect stored cardholder data.** PCI requires that you protect the data at rest on the cardholder systems. Have a policy for credit card retention, encryption, truncation, masking and hashing as necessary to ensure that the data is protected in the right places. This includes all aspects of the data life cycle from initial storage to disposal. Ensure that credit card data does not find its way into the log data. Splunk can also ingest storage data loss prevention events indicating exposed cardholder data.

**Requirement 4. Encrypt transmission of cardholder data across open, public networks.** Use Splunk software to verify the building and tear down of IPSec transmissions and that trusted legitimate certificates not are used—not self-signed. Make sure the correct version of TLS or SSL is used to encrypt data in transit. Don’t use WEP for wireless or you’ll pay for it at audit time. Splunk can also ingest storage data loss prevention events indicating exposed cardholder data.

**Requirement 5. Protect all systems against malware and regularly update anti-virus software or programs.** Use Splunk to index events from anti-malware products, including anti-virus, host-based intrusion prevention, or endpoint threat detection and response software. Then use Splunk to monitor the agents to ensure they are running periodic scans, are of the latest version, and also are receiving the latest signature updates. You can also use the free Splunk universal forwarder to directly monitor critical systems to look for OS events that could indicate malware that is not signature-based. These events could include things like changes to key configuration files, rarely seen services or registry keys, or software running in abnormal directories.

**Requirement 6. Develop and maintain secure systems and applications.** Use Splunk to index operating system or patch/endpoint management systems to identify systems that have insecure configurations or haven’t rebooted. Patch trending is handled easily by putting all the vulnerability data into Splunk and monitoring patch metrics. Splunk software can also help to prioritize hosts based on CVSS score if included in the patch management product.

**Requirement 7. Restrict access to cardholder data by business need to know.** All access attempts to applications and hosts in scope for PCI can be monitored and reported on by Splunk. Splunk can also automatically take this indexed data and cross-check it in real-time against employee directories to identify when someone trying to log into the PCI environment should not be doing this based on their role or department. The data in this environment paints a complete picture of the user and access record: where the user is accessing the data from, the access time of day, what system is being used to access the data and what system is accessed.

**Requirement 8. Identify and authenticate access to system components.** Use Splunk to monitor for account sharing by monitoring same account password accesses from different locations/IP addresses inside your company. Monitoring the account creation/deletion lifecycle is possible with Splunk. This can bring to light processes that may not have been followed to delete accounts as part of employee separation processes. Monitoring user accounts for clear text authentication, auditing password resets, and generating a list of inactive user accounts is also possible with Splunk software.

**Requirement 10. Track and monitor all access to network resources and cardholder data.** Accounting for access to all network, systems, applications and cardholder data requires the collection of data and log management. Splunk Enterprise can act as the log storage solution for log data—the definitive record of all human-to-machine and machine-to-machine interactions. Splunk can also retain this access data for three months or more to meet PCI requirements, and its search interface and visualizations make it simple to perform critical log reviews daily.

**Requirement 11. Regularly test security systems and processes.** Splunk can index data from vulnerability scans conducted (by an ASV) from inside or outside the perimeter, the results of a penetration test (XML file, CSV, other format) or other test data collected. Dashboards can easily be created to trend the number of vulnerabilities by CVSS number (4 or greater).

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