sumologic

SOLUTIONS BRIEF

PCI DSS Compliance with Sumo Logic

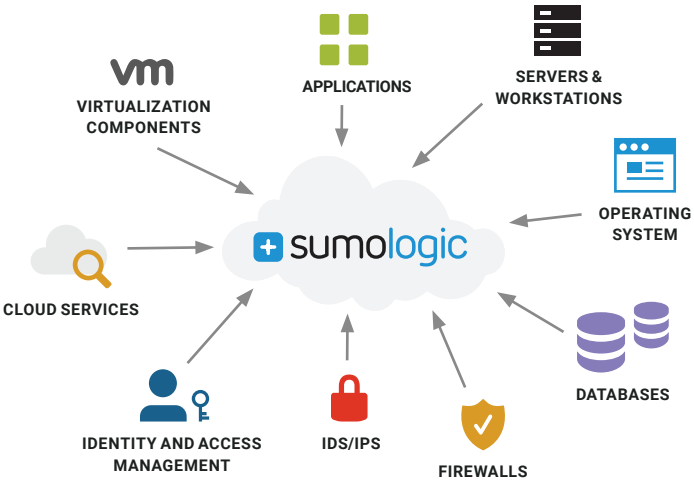
Sumo Logic is a cloud-native, data-analytics service that helps address log management, monitoring and data retention as prescribed by PCI DSS Requirement 10.

The complex and evolving requirements of PCI DSS compliance create a myriad of challenges for InfoSec teams in organizations that process, store or transmit credit and debit card information.

The PCI Challenge

As the systems that fall within the scope of PCI generate data at an exponential rate, the task of maintaining compliance requirements and protecting critical data is becoming overwhelming – the Verizon 2015 PCI Compliance Report found that 80% of organizations failed their 2014 interim compliance assessment.[1] When combined with the increasing sophistication of attacks, it's no wonder that IT struggles to reconcile these growing needs with existing solutions that don't work. According to Mandiant M-Trends report2, companies have no idea they have been hacked, and the median number of days before breach detection is 205 – that is over 6 months! The end result is an expensive yet incomplete infrastructure that requires more manpower to manage and simply adds to the chaos and ongoing security risks.

Over the years, the PCI compliance standard has undergone substantial changes, and the unpredictable nature of compliance audits where auditors can request precise information related to an organization's operations makes meeting all requirements an arduous.



"Demonstrating continuous adherence with PCI and other regulatory compliance standards is a priority for CloudPassage. Sumo Logic helps us address compliance with a unified view of our infrastructure, strengthens real-time security monitoring and meets log review and retention requirements which shortens audit cycles."

Bart Westerink, Sr. Director, Security & Compliance, CloudPassage

task. According to a recent survey by the PCI Security Standards Council (SSC) Daily Log Monitoring Special Interest Group (SIG)[3], addressing requirement 10 (Track and monitor all access to network resources and cardholder data) and 10.6 (Review logs and security events for all system components to identify anomalies or suspicious activity) were particularly challenging for the majority of respondents. The reasons given were as follows:

- Identifying appropriate and/or relevant log sources
- Differentiating between "normal" activity and a "security event"
- Handling large volumes of log data
- Meeting the stated frequency of manual log reviews
- Correlating log data from disparate systems

Lessons Learned from Payment Breaches and its Applicability to Requirement 10

The Verizon 2015 PCI Compliance Report also found that none of the companies that had suffered a breach in 2014 complied with requirement 10 for logging and monitoring – 0%!

Monitoring key systems is critical for achieving sustainable security and companies that exhibit poor logging and monitoring are likely to take longer to spot breaches, giving criminals more time to do more damage. The report's authors say that fulfilling this requirement is likely to give you the "biggest bang for your compliance buck." Failure to comply with them is more closely associated with having a breach than the other requirements.

How Sumo Logic Helps You Comply with PCI DSS Requirement 10

Sumo Logic helps organizations of any size meet the stringent and challenging logging, monitoring and data retention requirements spelled out in PCI DSS Requirement 10.

PCI Req.	Description	Guidance
10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	Promptly backing up the logs to a centralized log server or media that is difficult to alter keeps the logs protected even if the system generating the logs becomes compromised
10.5.4	Write logs for external facing technologies onto a secure, centralized internal log server or media device.	By writing logs from external-facing technologies such as wireless, firewalls, DNS, and mail servers, the risk of those logs being lost or altered is lowered, as they are more secure within the centralized environment.
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity.	Many breaches occur over days or months before being detected. Regular log reviews by personnel or automated means can identify and proactively address unauthorized access to the cardholder data environment.
10.6.1	Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	Checking logs daily minimizes the amount of time and exposure of a potential breach. Daily review of security events—for example, notifications or alerts that identify suspicious or anomalous activities—as well as logs from critical system components, and logs from systems that perform security functions, such as firewalls, IDS/IPS, file-integrity monitoring (FIM) systems, etc. is necessary to identify potential issues. Note that the determination of "security event" will vary for each organization and may include consideration for the type of technology, location, and function of the device. Organizations may also wish to maintain a baseline of "normal" traffic to help identify anomalous behavior.
10.6.2	Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	Logs for all other system components should also be periodically reviewed to identify indications of potential issues or attempts to gain access to sensitive systems via less-sensitive systems. The frequency of the reviews should be determined by an entity's annual risk assessment.
10.6.3	Follow up exceptions and anomalies identified during the review process.	If exceptions and anomalies identified during the log-review process are not investigated, the entity may be unaware of unauthorized and potentially malicious activities that are occurring within their own network.
10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	Retaining logs for at least a year allows for the fact that it often takes a while to notice that a compromise has occurred or is occurring, and allows investigators sufficient log history to better determine the length of time of a potential breach and potential system(s) impacted. By having three months of logs immediately available, an entity can quickly identify and minimize impact of a data breach. Storing logs in off-line locations could prevent them from being readily available, resulting in longer time frames to restore log data, perform analysis, and identify impacted systems or data.

The Sumo Logic Advantage for PCI Compliance

- Automate and demonstrate compliance with PCI DSS Requirement 10
- Visibility across all systems
- Simplify compliance and shorten audit cycles
- Secure by Design: Platform is PCI DSS 3.0 Service Provider Level 1 Certified
- Deployed in minutes, not days
- Reduced cost of ownership with a cloud-native, highly-scalable service
- Segmented, unalterable, and centralized repository for all your log data

"Our distributed, high-availability environment requires predictive real-time security event monitoring to meet stringent PCI requirements. Sumo Logic plays a critical role in making that happen and provides in-depth diagnosis that helps us improve our overall security posture for business success."

Rama Notowidigdo, CTO, Kartuku

About Sumo Logic

Sumo Logic is a secure, cloud-native, data analytics service, delivering real-time, continuous intelligence across an organization's entire infrastructure and application stack. More than 700 customers around the globe experience real-time operational, business and customer insights using Sumo Logic for their DevOps, IT ops and security and compliance use cases. With Sumo Logic, customers gain a service-model advantage to accelerate their shift to continuous innovation, increasing competitive advantage, business value and growth. Founded in 2010, Sumo Logic is a privately held company based in Redwood City, CA and is backed by Greylock Partners, DFJ, IVP, Sutter Hill Ventures, Accel Partners and Sequoia Capital. For more information, visit www.sumologic.com.

Sources:

1. Verizon 2015 PCI Compliance Report
2. Mandiant M-Trends Report (2012 -2015)
3. Effective Daily Log Monitoring SIG https://www.pcisecuritystandards.org/get_involved/special_interest_groups.php

sumologic

Toll-Free: 1.855.LOG.SUMO | **Int'l:** 1.650.810.8700
305 Main Street, Redwood City, CA 9460

www.sumologic.com