sumo logic

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.

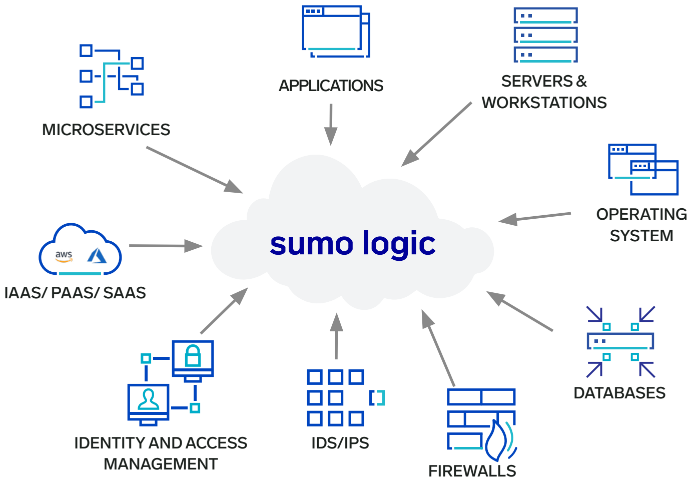
The complex and evolving requirements of PCI DSS compliance create a myriad of challenges for InfoSec teams in organizations that process, store or transmit credit and debit card information.

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 – Almost 50% of the organizations are still not compliant with PCI as per Verizon's PCI compliance report. 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 reports, 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 task.

> **"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**



According to a recent survey by the PCI Security Standards Council (SSC) Daily Log Monitoring Special Interest Group (SIG), 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 Reqirement 10

Organizations are required not only to achieve 100% compliance with the PCI DSS, but also to maintain it. This means having all applicable security controls continuously in place. 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
10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
10.5.4	Write logs for external facing technologies onto a secure, centralized internal log server or media device.
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity.
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.).
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.
10.6.3	Follow up exceptions and anomalies identified during the review process.
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).

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 3.2 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

About Sumo Logic

Sumo Logic is a secure, cloud-native, machine data analytics service, delivering real-time, continuous intelligence from structured, semi-structured and unstructured data across the entire application lifecycle and stack. Nearly 2,000 customers around the globe rely on Sumo Logic for the analytics and insights to build, run and secure their modern applications and cloud infrastructures. With Sumo Logic, customers gain a multi-tenant, 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, Calif. and is backed by Accel Partners, Battery Ventures, DFJ, Franklin Templeton, Greylock Partners, IVP, Sapphire Ventures, Sequoia Capital, Sutter Hill Ventures and Tiger Global Management. For more information, visit www.sumologic.com