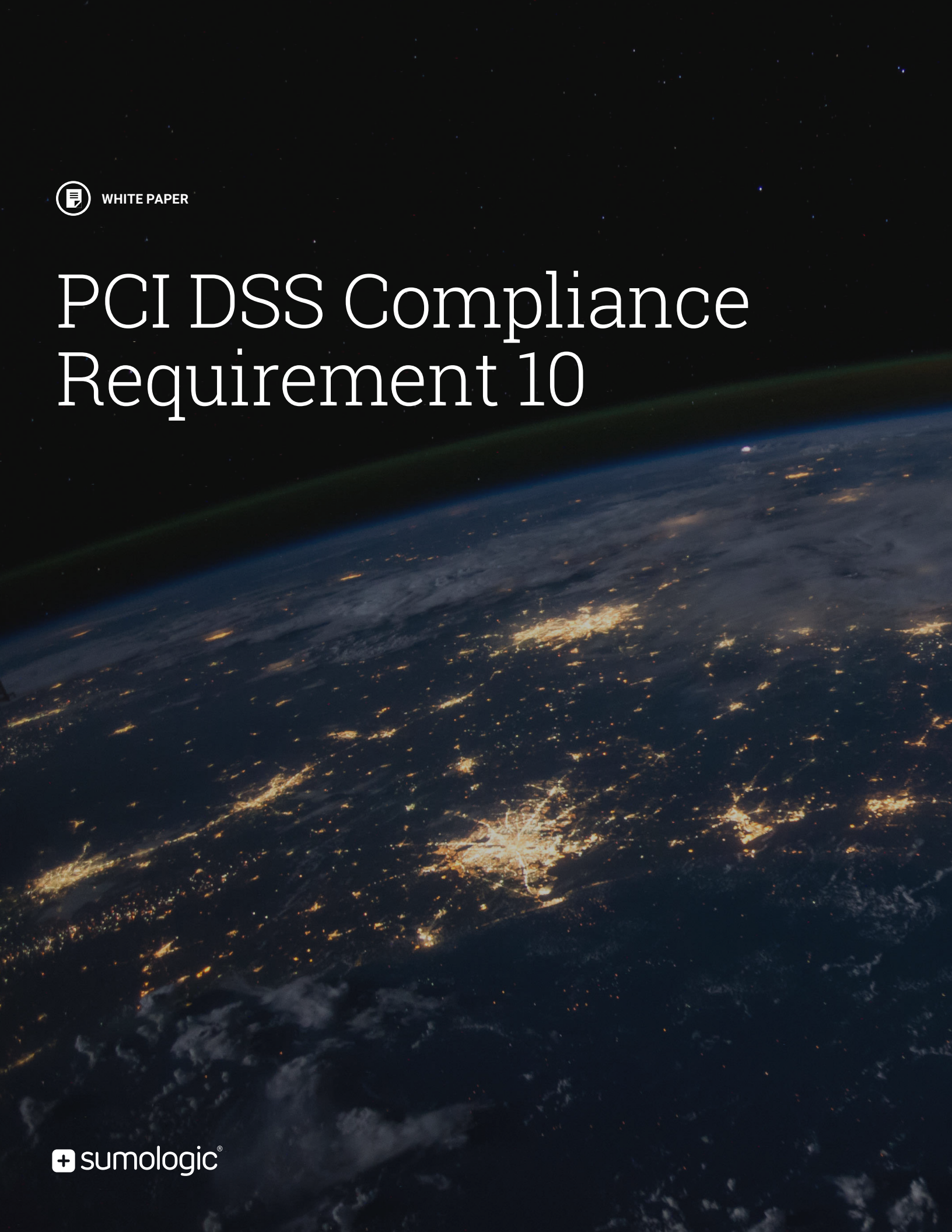
WHITE PAPER

PCI DSS Compliance Requirement 10



sumologic®

The Payment Card Industry Digital Security Standard (PCI DSS) is the benchmark by which network safety and auditing is measured. Developed and modified by the PCI Security Standards Council, a global consortium of experts devoted to account data protection, PCI DSS Requirement 10 mandates that merchants must "establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user."

How to Ensure You Comply with Requirement 10

Requirement 10 strives to ensure safe and reliable transfer of major credit and payment card data via the monitoring and analysis of PCI system activity logs.

To remain compliant with the standard, your organization faces an uphill battle protecting customer data against a multitude of threats, the list of which grows daily. Below we'll take a look at the varying angles from which PCI DSS 10 must be studied to build good IT security policy. These include:

- A four-point approach to security and compliance
- How recent changes to compliance standards will affect you
- Planning for flexibility in your compliance approach

With new development processes such as DevOps and agile and new architectures including IaaS, PaaS and containerization, achieving compliance is an order of magnitude more complex, so it's important to work with a qualified security assessor as you build your plan.

A Four-Point Approach to Security and Compliance

The challenges of maintaining a secure and compliant network vary by organization. An on-premise data center comes with the advantage of complete control over all its pieces and services, but the exposure of relying on internal resources and technology to to govern all aspects of security.

A **cloud** or **hybrid** network design inverts these challenges; by outsourcing many aspects of compliance and security responsibility, control is replaced with dependence on third parties.

Whatever the network architecture, IT analysts and compliance experts around the world face common pain points.Whatever the network architecture, IT analysts and compliance experts around the world face four common pain points:

- Centralized logging
- Proof of immutability
- Daily reviews
- Data retention

Strong, sound policies for your compliance team will address these four areas.

1. Centralized Logging

Somewhere out there on the web, a customer at your site types credit card info onto his smart phone. The phone connects to a wireless access point, which passes the data through a router or switch, and so on, until the credit card data bounces through wires and equipment and ends up with you.

Throughout this process, PCI DSS compliance makes you responsible for everything that happens to that data, both when the customer sends it and afterwards, as the data lives in your records.

Keeping track of all that data is tricky, especially with so many network devices keeping their own logs. All of those logs must be thoroughly scanned until a vulnerability is isolated and can be reported, and logging into each device remotely and gathering logs probably isn't an option when dozens of devices are in play.

Compliance requires gathering all of this disparate log data into one central location for review and root-cause analysis and audit queries should a vulnerability be found. A variety of approaches exist for this centralized logging, ranging from raw data dumps to real-time log aggregation supported by easy to use, machine-learning technologies that ingest large volumes of data, automatically analyze anomalies and deploy pre-designated actions when compliance-threatening events strike your network.

Machine learning can quickly surface outliers and detect exceptions to patterns in log data, thereby minimizing the impact of falling out of compliance. One particularly useful capability is the ability to compare

what has changed across two different time periods or two different devices in order to isolate potential vulnerabilities.

Understanding the data that must be gathered, the method used to gather it, and a system for auditing your centralized logs is essential to good compliance policy.

2. Proving Immutability

Achieving centralized logging is just the start of a battle. PCI DSS 10 compliance requires not just a "black box" where all transaction activity can be stored and guarded, but an auditing system for who went near the data, when, and why, with full reporting accountability that proves your centralized logs have not been and cannot be altered without leaving evidence.

Why? Cyber criminals are endlessly resourceful, and the most skilled of them likely understand logging and security better than your IT team. One common technique criminals use to disguise their trails is log disabling; it's the cybercrime equivalent of turning off security cameras so perpetrators can't be tracked. Another great way to cover up a digital crime like data theft is to break into the storage vault where the logs outlining the activity are stored and delete evidence of the crime.

Stay compliant by staying on top of your centralized logging data with a plan for proving at any moment that your logs are immutable and even the cleverest cybercriminals can't get to them without getting caught.

3. Daily reviews of infrastructure

Requirement 10 calls for self-audits, so be sure to audit your security infrastructure. Firewalls, routers, and other internal equipment must be reviewed on a regular basis. Regulations call for daily reviews of activity and logs for this equipment so that anomalies or threats are proactively addressed and don't have time to fester in your environment.

If you are using a public cloud provider, they are responsible for the daily review of the infrastructure and you are responsible for the application security, plus any edge devices within your network. Work with your engineers and compliance team to ensure that logs from any device can be accessed and analyzed both on a regular basis and at a moment's notice.

4. Rigid Data Retention Policies and Practice

Though organizations often can define their own data retention policies, nobody wants to be caught in an audit situation where logs that might contain suspect activity have been purged or overwritten. For this reason it is imperative that clear and strict policies for retaining your logging data are in place and well-understood by everyone in your organization.

Data retention ranges are generally three months of hot storage, plus nine months of cold storage. This combination of hot and cold storage is designed to lower overall costs. In most cases, you will be able to purge the data once a successful audit report is completed and rely on the audit report to address any compliance questions that arise. In an audit, this kind of consistency is the difference between passing and failing.

Treat your native, cloud, or hybrid network environment as a living and vulnerable entity in an increasingly hostile global web environment. Approaching your IT architecture, security, and compliance planning along these four points will help you keep your network healthy and safe.

How Recent Changes to PCI Standards Affect You

As threats evolve, so too must defenses. The PCI Security Standards Council's most recent changes are outlined in PCI DSS v3.2, in which some previous 'best practice' recommendations have been made mandatory. Though the details of all the changes are important, key highlights include:

Multi-factor authentication.

Formerly a best practice, standard compliance now mandates multi-factor authentication for secure transactions. Where formerly as initial password validation was enough to perform transactions, now at least one secondary method – commonly a security token or a form of biometric authentication – is required for Requirement 10 compliance.

Deep penetration testing at least biannually.

In addition to the daily audits outlined above, new guidelines require that qualified external third-parties probe your network for vulnerability at least every six months and report results. Numerous IT security companies provide services to help organizations stay compliant by performing deep penetration testing testing on their networks and summarizing their risk posture and compliance threats.

The goal of this requirement is to simulate as nearly as possible a sustained professional intrusion and find out where and how crooks might exploit your network weaknesses so you can shore up defenses in advance.

Migration deadline for Secure Socket Layer(SSL) and early

Transport Layer Security (TLS). Perhaps one of the most significant security changes involves SSL/TLS security. SSL has been the industry standard for security encrypted transactions for almost 20 years, even though malware programs have found and exploited vulnerabilities in both SSL and TLS v.1.0-1.2. New changes in DSS 10 v3.2 stipulate that organizations must migrate away from these older security technologies, which have a sunset deadline of June 2018.

As many organizations continue to rely heavily on SSL/TLS, a solid plan for migrating to more secure technology like TLS v.1.3 now will immediately make your network safer and spare you a mad rush to compliance as the sunset deadline approaches.

Planning for flexibility in your compliance approach

The PCI Security Standards Council uses a term called Evolving Requirements, defining it as "changes to ensure that standards are up to date with emerging threats and changes in the market." In this market, the only constant may be changes and the emergence of new threats.

In 2015 CNN reported that more than a million new viruses were launched every day, along with nearly 320 million new pieces of malware catalogued that year. With the forces of digital darkness coming at your network infrastructure that hard, your plan for compliance must be as broad and flexible as the threats you face.

Knowing latest changes and requirements is critical, but so is actively studying threat matrices and evolving your compliance strategy to being prepared to defend against the most dangerous known problems of the day.

No compliance plan (or general IT strategy) today can be complete without addressing user owned devices. The old days of enforcing hard separation between the 'internal' network and external devices are gone in an age of hybrid cloud infrastructures, smart phones,

and tablets, when the CEO may well want to stream the PowerPoint presentation on his cloud drive to a portable projector via Bluetooth.

Each these devices come with powerful capabilities—and serious compliance implications. Revise your policies or adapt new ones to address the reality, not the possibility, of user owned devices operating within your secure network space.

Immediate Next Steps for Ensuring Compliance

Now that you know the main pitfalls and perils of the path to compliance, what's next? Start by running through this brief checklist.

Begin with a full audit.
Establish your operating baselines and do an initial security assessment. As your policy develops, look back at starting points and compare them to lessons learned and emerging threats. The gap will frighten you, but that fear can be turned into strong security.

Include your people.
Involve the people who will depend on these policies in their development and adoption. Few business process interruptions are as frustrating as IT policy changes that take users off guard and leave them scrambling to perform previously basic tasks. So if your production database access must move to multi-factor authentication, make sure people accessing it can give input on the processes, and that they know when the change will impact them.

Write for humans.
The average user doesn't know what PCI DSS 10 v3.2 is, and that's okay. But when it comes to explaining the importance and implementation of good policy, don't leave the writing up to your CIO or lead engineer. Involve experienced tech policy writers who know to use simple phrases and explanatory analogies to make it as simple and accessible to the end-user as possible.

Plan for digital Darwinism.
The compliance policy you commit to paper will likely have new wrinkles to consider before the printer ink is dry. The race between technology and business, known as digital Darwinism, sees many companies fail to adapt to the ever-evolving state digital advances. Dedicate resources to studying payment card industry trends, threats, and best practices on a regular basis, not just during mandatory audits.

The nature of compliance calls for doomsaying and worst-case scenarios, so you effective IT architects can plan and prepare for all of them. But look at the upside: emerging technologies give us ways to intimately connect with customers and even chart their shopping and buying activity in real-time as they interact with modern applications. With the right technology partners, companies can leverage PCI DSS compliance protocols to their advantage strengthening their efforts to spot compliance breaches and security threats and defend against them in ways never before possible.

The right tools are the secret to adding the compliance power you need to dominate the modern digital marketplace and win out over internal and external threats.

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. More than 1,000 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, CA and is backed by Accel Partners, DFJ, Greylock Partners, IVP, Sequoia Capital and Sutter Hill Ventures. For more information, visit www.sumologic.com.

sumologic®

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

www.sumologic.com