ALERT LOGIC™

COMPLIANCE

6 Steps to Overcoming PCI DSS Compliance Challenges

In Multi-Cloud Environments and Hybrid Environments

No more fire drills

A Payment Card Industry Data Security Standard (PCI DSS) audit can be passed by complying with the bare minimum requirements, but that falls short of the purpose of it: to secure and protect cardholder data.

Meeting compliance is about passing an audit at a specific point in time and also maintaining it after the audit. The real challenge is sustaining continuous compliance to avoid costly breaches at the hands of motivated and skilled adversaries.

Indeed, as detailed in Verizon's "2019 Payment Security Report," nearly two-thirds (63.3%) of the organizations assessed did not maintain all PCI DSS controls. But this failure to sustain PCI DSS compliance isn't due to a lack of security tools; most organizations have lots of them. What they're missing is PCI expertise or the dedicated staff required to keep pace—a problem that is only compounded by the growing use of cloud services. Organizations are rapidly moving to highly scalable, multi-cloud, and hybrid environments, which adds layers of compliance complexity and blurs the lines of responsibility.

This eBook examines the challenges inherent in achieving continuous PCI DSS compliance across multi-cloud and hybrid landscapes and what to look for in evaluating solutions and service providers that can address those complexities.

63.3% of the organizations assessed did not maintain all PCI DSS controls.

"2019 Payment Security Report," Verizon

Meeting PCI DSS compliance requirements in the cloud is a shared responsibility between cloud service providers and their customers.

Why PCI matters and who must comply

Failure to maintain PCI DSS compliance can have significant consequences. Most obvious are the fines and higher processing fees, but there's also unwanted publicity and brand damage if your organization suffers a breach. In some instances, maintaining relationships with certain business partners may require you to comply with PCI DSS.

It's a simple matter of security. If you routinely stay in full compliance, it usually means that you have a robust security posture and significantly lower chances of experiencing a breach.

Organizations with a strong security posture understand that being compliant does not necessarily mean you are secure.

However, being secure means being compliant and in order to be secure you need to do more than the minimum. Unfortunately, according to the 2019 Verizon Report only 18% of organizations do more than the minimum when it comes to PCI compliance.

In order to sustain a strong security posture, you must start with establishing a process to assess your organization's compliance responsibilities and establish metrics. Metrics will hold people accountable whether they are directly involved with payment systems and cardholder data or tangentially connected on the network.

Clouding the PCI picture

Although your network may be PCI DSS compliant, signing on for cloud services potentially expands the scope of your environment subject to PCI compliance.

Cloud service providers might address some of the PCI DSS requirements—such as physical access or ensuring that the underlying OS is patched and up to date—but customers are ultimately responsible for achieving and sustaining PCI DSS compliance, including addressing vulnerabilities in web applications and ensuring that cloud services are properly configured. For example, one PCI requirement is a daily review of system logs. Although Amazon Web Services (AWS) can send you CloudTrail logs, that doesn't satisfy the PCI DSS requirement of regular log review analysis required to identify and proactively address suspicious activity related to potential unauthorized access to the cardholder data environment.

That's just one example of the tasks involved in achieving and sustaining PCI DSS compliance in cloud environments. Others include:

- Doing vulnerability scanning of new workloads and web applications within minutes of deployment
- Monitoring and investigating risky configuration changes to various cloud services
- Ensuring that web applications are automatically protected by scalable web application firewalls (WAFs)
- Centralizing massive amounts of log data from cloud services and deployed applications to support audits that require up to a year's worth of raw log file data

There's no sugarcoating it: Sustaining continuous PCI DSS compliance is complicated and easy to get wrong without the proper tools and expertise.

Deploying and managing these security compliance controls can strain even the largest organizations' technical, human, and financial resources.

Six compliance solution considerations

Not all options are created equal, of course. Look for a solution that can help you address the following six issues.

1 LOG CHALLENGES

With respect to system logs, PCI DSS requires you to:

- Identify any systems that are in scope with respect to PCI DSS
- Continuously collect log data for those systems
- Review log events and suspicious activity daily to identify any security risks

2 AUTOMATION

Automating various tasks is crucial to reducing manual processes and procedures as well as reducing errors. Your compliance solution should automate the collection of log files for daily analysis. It should also detect, scan, and monitor new workloads—as soon as they are deployed—for software vulnerabilities and configuration issues such as those found in the OWASP Top 10. Automation should also extend to WAFs, to ensure that they can scale with applications without degrading performance.

3 EASY TO USE

The goal is to find an effective security solution that seamlessly and simultaneously addresses PCI compliance by protecting customer data—including cardholder data—from unauthorized access. Managed services, where a provider does the heavy lifting, will generally deliver more-effective security and immediate outcomes than alternatives managed by internal IT staff members who are already spread too thin.

4 AVOIDING THE QUICK FIX

Avoid any solution that looks too good to be true, and make sure the solution is PCI ASV certified. Be wary of vendors offering fast PCI compliance with no mention of improving security controls and technologies. It just doesn't work that way.

5 SUPPORT FOR MULTIPLE ENVIRONMENTS

An ideal PCI solution will handle the different sorts of environments in which payment data lives, including on-premises office buildings, retail locations, private data centers, public clouds, and hybrid clouds.

6 EASY TO USE

Look for services that include daily review and analysis of your log data, incidents, and compliance reports—by security and compliance experts who can deliver analysis and recommendations. The service provider should also have live staff members who interact with customers when needed, such as to discuss PCI DSS scan results.

On the next page, discover how Rent-A-Center put all these considerations into action to efficiently and effectively meet PCI compliance requirements.

Rent-A-Center's cloud-first approach on AWS

Rent-A-Center offers brand-name rent-to-own furniture in more than 3,000 stores across the United States, Canada, and Mexico. No-cost repairs and a no-credit path to ownership deliver a unique customer experience.

"AWS and Alert Logic synergies has allowed me to avoid costly CapEx purchases year in and year out on maintenance and support."

— Mike Santimaw, VP of Information Security, Innovation Labs & Corporate Solutions, Rent-A-Center

THE CHALLENGE

Technology underpins virtually all of Rent-A-Center's operations, from point-of-sale terminals to in-store displays and e-commerce, yet the company strives to maintain a lean IT team. These issues made cloud services an attractive option. "We don't have a huge IT staff, and we needed ways to speed up delivery and improve service in our stores," says Gary Sprague, director of information security at Rent-A-Center. "Using the cloud had the potential to increase our efficiency and enable us to continue growing without opening our own physical data centers across the country." However, Rent-A-Center couldn't afford to ignore security when adopting cloud services. As a public company, it is governed by strict Sarbanes-Oxley security and privacy requirements. And, because it takes credit card payments, it must adhere to the PCI DSS.

WHY ALERT LOGIC

Prior to adopting a cloud-first approach, Rent-A-Center partnered with Alert Logic for its fully managed 24/7 security as a service. The company wanted to continue getting this high level of security assurance after moving to the cloud. Rent-A-Center discovered that Alert Logic was available through the AWS Marketplace, an online store that helps organizations find, buy, and use software and services. The company decided to adopt Alert Logic in the cloud, based on past positive experiences. Alert Logic on AWS has empowered Rent-A-Center with advanced threat analytics, detection, and alerting across its applications and services. Using full-packet inspection within the AWS environment, it uniquely protects against threats that proliferate inside an organization's cloud environment as well as attacks coming from the outside.

The results

The increased visibility from Alert Logic and AWS cloud management tools gives Rent-A-Center's IT staff peace of mind. "You might think you're safer on-premises managing things yourself, but it can actually be harder to know what's going on," says Sprague. "When you're in the cloud and the tools are designed to show you what's most important, you can be more proactive." Using AWS and Alert Logic has enabled Rent-A-Center to transition to a cloud-first approach. "When we upgrade applications, we migrate them to the cloud," says Sprague. "If that's not possible, we shift to a different solution that works in AWS. "Using Alert Logic on AWS provides cost-effective, 24/7 security coverage of our entire environment, the equivalent of six full-time security employees," says Sprague. "Those resources can now be used to create better services and experiences."

Achieve Security Compliance and Improve Audit Preparation

To help our customers overcome PCI compliance challenges, we advise Alert Logic. Their Managed Detection and Response (MDR) capabilities enable customers to achieve compliance across multiple requirements and improve their preparations for audits, supplying on-demand dashboards and 24/7 platform support.

To learn more, visit https://www.alertlogic.com/solutions/security-compliance/