softwerx

ALIEN VAULT
An AT&T Company

EXECUTIVE SUMMARY

How to Simplify PCI DSS Compliance with a Unified Approach to Security

- PCI DSS is a technical regulation that focuses on credit cardholder data security.
- Organizations struggle to comply, even though fines and other costs can be severe.
- Businesses face implementation challenges in an ever-changing threat landscape.
- Best practices help organizations overcome PCI DSS challenges.
- AlienVault USM Anywhere simplifies and reduces the cost of compliance.

SEPTEMBER 20, 2018

Sanjay Ramnath, VP Product Marketing, AlienVault

EXECUTIVE SUMMARY

How to Simplify PCI DSS Compliance with a Unified Approach to Security

Overview

In 2004, major credit card vendors—Visa, MasterCard, American Express, Discover, and Japan's JCB—mandated that any organization handling credit cards for payment or processing must comply with PCI DSS. Today, companies still face challenges implementing and maintaining the security controls necessary to follow this regulation, which can lead to costly fines and data breaches.

Managed service providers (MSPs) can help businesses challenged by PCI DSS compliance. MSPs can offer both the expertise to comply with the regulation and solutions that provide a unified approach to security, such as AlienVault Unified Security Management (USM) Anywhere.

Context

Sanjay Ramnath discussed challenges that businesses often face in complying with PCI DSS, and how MSPs can help these organizations with compliance and a unified approach to security.

Key Takeaways

PCI DSS is a technical regulation that focuses on credit cardholder data security.

PCI DSS is designed to encourage and enhance cardholder data security and reduce credit card fraud. While this technical regulation focuses on protecting cardholder data, the main concepts can be extended to protect any type of sensitive data stored by an organization.

PCI DSS 3.2.1 Control Objectives and Requirements	
Build and maintain a secure network and systems	• Install and maintain a firewall configuration to protect cardholders • Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	• Protect stored cardholder data • Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	• Protect all systems against malware and regularly update anti-virus software or programs • Develop and maintain secure systems and applications
Implement strong access control measures	• Restrict access to cardholder data by business need to know • Identify and authenticate access to system components • Restrict physical access to cardholder data
Regularly monitor and test networks	• Track and monitor all access to network resources and cardholder data • Regularly test security systems and processes
Maintain an information security policy	• Maintain a policy that addresses information security for all personnel

PCI DSS could be a good set of guidelines for a company that's looking to strengthen or implement security processes.

Sanjay Ramnath

softwerx
ALIEN VAULT
An AT&T Company

How to Simplify PCI DSS Compliance with a Unified Approach to Security

Organizations struggle to comply, even though fines and other costs can be severe.

Banks and credit card institutions can levy fines ranging from $5,000 to $200,000 when an organization is found not to be in compliance with PCI DSS. Despite the hefty costs, organizations are still struggling with compliance, leading to even more costly breaches.

Cost of Non-compliance and Data Breaches	
Non-compliance	Fines range from $5,000 to $200,000
Cardholder data breaches	• $50-$90 fine for each cardholder whose data is breached • $141 cost per stolen record • Potential suspension of credit card acceptance • Erosion of brand and reputation • Legal issues

The Verizon 2017 Payment Security Report found that 100% of breached organizations failed PCI DSS compliance. Among those that were in compliance, 45% still had security gaps that required some form of remediation.

Businesses face implementation challenges in an ever-changing threat landscape.

PCI DSS is complicated to implement because the modern threat landscape is constantly changing. To stay in compliance, businesses cannot just implement technologies and processes and move on; they need to continue to maintain and update systems to keep new threats at bay.

Organizations face three key challenges when implementing and complying with PCI DSS:

1. **Compliance is a moving target.** Modern attacks are designed to evade perimeter defenses. Meanwhile, network and application architecture within the business is changing with cloud, mobile, infrastructure as a service (IaaS), platform as a service (PaaS), and other new technologies. Security configurations drift and shift as environments evolve.
2. **Compliance is never "done."** It needs to be part of ongoing security hygiene; not just updated to pass audits. Even when a PCI DSS audit is completed successfully, it does not mean the organization is secure.
3. **Resources are scarce.** Scarce resources make the cost of compliance prohibitive for some small businesses. Because of costs and a lack of expertise, organizations struggle to integrate PCI DSS-related technologies, struggle with data overload from disjointed services, and cannot scale security teams to review all of the events, alarms, and logs that can identify a problem.

These challenges provide MSPs with opportunities to help IT-constrained organizations comply with PCI DSS and improve security on an ongoing basis. MSPs and partners can also help organizations avoid common PCI DSS pitfalls.

Top 10 PCI DSS pitfalls include:

1. Improper scoping
2. Failing to patch systems regularly
3. Failing to audit access to cardholder data

How to Simplify PCI DSS Compliance with a Unified Approach to Security

4. Failing to review and monitor audit logs daily
5. Addressing PCI DSS compliance only during an annual audit
6. Failing to shut down third-party vendor remote access after use
7. Failing to change vendor default configurations, such as passwords
8. Obsession on putting things out of scope
9. Failing to track where cardholder data is stored
10. Storing sensitive authentication data after authorization

Sanjay Ramnath shared some best practices learned from AlienVault partners. These best practices can help MSPs and organizations overcome challenges and avoid the pitfalls of PCI DSS.

Best Practices to Help Organizations Overcome PCI DSS Challenges

- **Start with a PCI DSS readiness assessment.** Before solving the problems, first step back and articulate the problem. Understand the environment, including applications, attack vectors, vulnerabilities, and risks. Identify gaps and determine whether the resources exist within the organization to solve these problems, or if outside help is needed.
- **Make PCI DSS part of security hygiene** using continuous monitoring and response.
- **Ensure visibility across all relevant assets**, whether they are on-premise or in the cloud. Collecting and reviewing data from all of these assets provides a holistic view of the environment.
- **Integrate and simplify** by using solutions that bring multiple required controls into one platform, such as with AlienVault USM Anywhere.
- **Ensure the confidentiality, integrity, and availability of security data** is maintained.

How to Simplify PCI DSS Compliance with a Unified Approach to Security

AlienVault USM Anywhere simplifies and reduces the cost of compliance.

AlienVault USM Anywhere is a unified security management system that helps MSPs simplify PCI DSS compliance at clients, as well as reduce overall costs. The solution provides an integrated platform that combines five essential security monitoring capabilities—intrusion detection, asset discovery, vulnerability assessment, behavioral monitoring, and security information and event management (SIEM) —to support continual compliance in the business environment.

Biography

Sanjay Ramnath
VP Product Marketing, AlienVault

Sanjay Ramnath aims to make cybersecurity accessible to organizations of all sizes. He currently leads strategic product marketing for AlienVault, a leader in Unified Security Management. He has also held product leadership roles at Barracuda Networks where he designed, built and launched security and data protection solutions spanning hardware/software, SaaS and public cloud platforms.