Solution Brief

PCI Compliance

5 Common Struggles maintaining a PCI DSS compliant environment

Maintaining a compliant PCI DSS network environment is an everyday battle. While compliance is assessed and attested to on an annual basis, there are daily, weekly, monthly and quarterly acts that must also be carried out in order to meet specific requirements. With these tasks come common pitfalls, whether technical or procedural that can affect an entities ability to maintain a complaint in-scope network.

Dell SecureWorks offers a full suite of PCI Compliance Security consulting and remediation solutions to help businesses of all sizes address PCI DSS compliance. Our expert consultants are knowledgeable on all PCI DSS requirements, and can help you navigate the changes, identify the processes you need to implement, as well as assess and maintain your unique environment to ensure you are compliant.

The following lists typical pitfalls complying with PCI DSS experienced by Dell SecureWorks consultants, with brief guidance on how to mitigate each item.

1 Patching systems

The description that defines the scope of the network is confusing. According to the definition, it includes system components which store, process, or transmit cardholder data and all the systems connected to those systems. Deciding which devices are in the network and need to be patched on a regular basis adds stress to the networking and systems administration teams.

How do organizations address this?

If it is in-scope, it needs to be patched on a regular basis.

- The only exception to this rule is third-party applications which the entity does not manage, examples include payment or web applications like Java or Silverlight which are not owned nor maintained by the entity

2 PCI DSS Requirement 10: Meeting each logging requirement

Logging and auditing system components is an everyday process that can bring daily struggles. Common issues arise from requirements that require a daily security review of audible events that must be offloaded to either a centralized logging server or to media which is secured and difficult to alter. Whether through technical (not having appropriate configurations) or business (not having enough team member) restrictions, maintaining compliant logging solutions can bring down an entities compliance percentage, and cause additional stress on teams who manage systems that must be logged. *The guidelines are:*

- Any system which stores, transmits or processes cardholder data must send its system and application logs to a centralized logging server
- Individual cardholder data access (this applies to multiple systems) must also be logged and retained for one year, with three months of logs available for immediate analysis

Expert Testing, Analysis and Assessments

- Highly **Credentialed Experts** passionate about security
- Focused on security **Best Practices** for your industry
- Deep understanding of **Compliance, Regulations and Security Frameworks**
- Latest **threat intelligence** from Dell SecureWorks Counter Threat Unit™ research team
- Risk based approach

3 Securing and hardening management interfaces

Web servers are integral to an organization's online presence. If there are web based management interfaces, they now (for the time being) must only communicate over secure channels such as HTTPs with TLS1.2. With the recent SSLv3 vulnerability:
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566
browsers utilizing that protocol will be considered non-compliant, and fail a PCI DSS vulnerability scan performed by an ASV. *The solution recommended is (as there is not a technical fix at the time for the vulnerability)*:

- Subscribe to the National Vulnerability database to stay apprised of vulnerabilities which affect in-scope system components, especially those which are web and public facing

4 Understanding and implementing Compensating Controls

Sometimes business or technical restraints may hinder the appropriate measures so a requirement is fully met. To address these, there are Compensating Controls that allow entities to go above and beyond the requirement with technology and processes to meet the intent of the requirement.

However, knowing which requirements allow a Compensating Control, and how to securely and compliantly implement them is a common struggle that the technology team will face.

We suggest verifying that the following are met to ensure a compliant Compensating Control:

- The controls meet the intent and rigor of the original PCI DSS requirement.
- The controls provide a similar level of defense as the original PCI DSS requirement, such that the compensating controls sufficiently offset the risk that the original PCI DSS requirement was designed to defend against. (See Navigating PCI DSS for the intent of each PCI DSS requirement.)
- The controls are "above and beyond" other PCI DSS requirements.

5 Seeking answers from different sources yields different results

If an organization is not actively engaged with a Qualified Security Assessor (QSA) company, the first place they seek guidance is the Internet. While the Internet is a great resource for a lot of things, it is also an open forum and advice and guidance on something as specific as a PCI DSS requirement should be taken with caution. *The only way to get honest, unbiased advice on how to meet or exceed a PCI DSS requirement is to meet with a validated QSA. A list of certified QSA's can be found here:* https://www.pcisecuritystandards.org/approved_companies_providers/qualified_security_assessors.php

- Regular consulting with a QSA company gives an organization a subject matter expert that is apprised of active changes to the PCI DSS standards and requirements
- QSAs can offer guidance, analyze issues, and provide remediation guidance to identified gaps
- QSAs can also perform an array of security consulting and services which help entities meet the intent of the requirements which they must meet to submit their Attestation of Compliance

PCI compliance is a daily struggle, and knowing how to manage these key items will benefit an organization during this journey on its road to compliance.

Dell SecureWorks is a: PCI Security Standards Council®

- Qualified Security Assessor (QSA)
- PCI Forensic Investigator
- PCI Approved Scanning Vendor (ASV)

About Dell SecureWorks

Dell SecureWorks uses cyber threat intelligence to provide predictive, continuous and responsive protection for thousands of organizations worldwide. Enriched by intelligence from our Counter Threat Unit research team, Dell SecureWorks' Information Security Services help organizations proactively fortify defenses, continuously detect and stop cyberattacks, and recover faster from security breaches.

For more information, call 877-838-7947 to speak to a Dell SecureWorks security specialist.
www.secureworks.com

Availability varies by country. © 2015 Dell Inc. All rights reserved.