REDSEAL

EFFICIENT COMPLIANCE WITH PCI DSS

THE MEASURE OF RESILIENCE

Version 3.0/3.2 of the Payment Card Industry Data Security Standard (PCI DSS) contains a number of challenging new requirements. Organizations must take ownership of the definition of the scope of their cardholder data environment (CDE); retest segmentation after any significant change; and be able to demonstrate "Business as Usual" continuous compliance. RedSeal is an ideal choice for meeting these new challenges. It is currently delivering this set of controls and more in dozens of organizations—in a unique, operationally efficient manner.

PCI Security Standards Council™

PCI DSS 3.0

Among the PCI DSS changes that took effect in 2015 are the following key requirements:

"Business as Usual"

Unfortunately, many organizations have been treating PCI compliance as an annual project, rather than as a continuous process. They strive for compliance in the weeks leading up to the annual audit and don't worry about the quality of their controls the rest of the year. It shouldn't surprise us that most breached organizations weren't fully PCI compliant at the time of the breach. The "Business As Usual" guideline requires that controls be merged into an organization's standard operational process, making continuous compliance "business as usual."

Scope and Segmentation

Prior to PCI 3.0, the definition of acceptable CDE segmentation was vague, which led to insecure implementations. In 3.0 the Council defined segmentation much more strictly—something closer to isolation. This puts more pressure on organizations to define a truly secure segmentation strategy and be able to enforce it.

Expanded Penetration Testing

In PCI 2.0, penetration tests were only required once a year and when "significant changes" occurred. Unfortunately, in order to reduce their testing effort, many organizations were not defining "significant" rigorously enough. Segmentation was not being tested at all. So in PCI 3.0, the definition of what triggers penetration testing is much broader, and the CDE segmentation perimeter must be re-tested "after any changes to segmentation controls/methods".

HIGHLIGHTS

PCI DSS now includes requirements for continuous controls, enhanced network segmentation and penetration testing. To help meet these challenges, RedSeal:

- Provides comprehensive PCI controls to test segmentation, firewalling and DMZ architecture with extremely low operational overhead
- Lowers the cost of PCI penetration testing by reducing the need for manual tests
- Implements all controls consistent with the Business as Usual guidelines added in PCI 3.0.

EFFICIENT COMPLIANCE WITH PCI DSS

PCI DSS 3.1 SPECIAL UPDATE

PCI 3.1 was released in April 2015 in response to vulnerabilities in SSL and "early" versions of TLS, as identified by NIST. All existing implementations of SSL (any version) and early versions of TLS needed to be upgraded to "newer" versions of TLS by June 30, 2016. Any new implementations must immediately use newer versions of TLS and may not use SSL. Exceptions are cases where POS and POI terminals and associated termination points can be demonstrated to not be vulnerable to these exploits. Early versions of TLS are defined to be TLS v1.0, but NIST strongly encourages TLS v1.1 to also be avoided also—i.e. newer versions of TLS should use TLS v1.2 (or higher when available). These requirements are relevant to PCI 3.1 sections 2.2.3, 2.3, and 4.1. PCI 3.1 contains other changes, but these are Clarifications and Additional Guidance updates to 3.0.

PCI DSS 3.2 was released in April 2016, with updates primarily for service providers.

THE REDSEAL ADVANTAGE

RedSeal is a powerful solution for validating network controls and prioritizing vulnerabilities. By analyzing the configuration of Layer 3 network devices, it is able to accurately and continuously determine the efficacy of network segmentation and identify any policy deviations for immediate remediation. No other solution is able to provide this level of clarity of network access policy—across as many as tens of thousands of devices.

RedSeal also combines its network intelligence with scan data from the industry's leading vulnerability scanning vendors to prioritize remediation. In any complex network, internal and external scanning uncovers a huge number of vulnerabilities. The challenge becomes one of priorities: deciding which issues should be fixed first in order to minimize risk. By analyzing the potential impact if any of the discovered vulnerabilities was exploited, RedSeal provides security teams with a prioritized action plan for risk management.

Other important RedSeal capabilities include the ability to create and maintain a validated network architecture map and device inventory, and to apply best practice configuration hardening checks to a wide variety of network devices.

[1] PCI DSS 3.0, page 10

[2] 11.3.4a

EFFICIENT COMPLIANCE WITH PCI DSS

EFFICIENT PCI DSS COMPLIANCE WITH REDSEAL

RedSeal's unique set of capabilities are ideal for meeting audit and compliance control mandates, especially in the areas of network and firewall isolation and penetration testing and remediation. RedSeal supports 37 PCI controls in the following DSS requirement sections:

Requirement 1: Firewall Configuration

Requirement 2: Vendor Defaults

Requirement 6: Secure Systems

Requirement 11: Regular Testing

In addition, RedSeal supports the Business as Usual guideline for continuous controls, providing network segmentation analysis and validation on a daily basis. RedSeal also supports one sampling guideline that can reduce the size and scope of a PCI audit. The individual controls and support are listed at the end of the document.

PCI CONTROL TYPE	REDSEAL SUPPORT
Network diagram and device inventory	√
Firewall policy validation	√
Segmentation validation	√
Network device configuration hardening	√
Penetration testing risk prioritization	√
Business As Usual continuous controls	√
Sampling reduction – Centralized operational processes and controls	√

RedSeal is the only vendor that can implement the continuous network isolation controls required by the PCI DSS in an operationally efficient manner.

EFFICIENT COMPLIANCE WITH PCI DSS

REDSEAL PCI DSS CONTROL SUPPORT DETAILS

REQUIREMENT SECTION	SUB-REQUIREMENTS SUPPORTED	REDSEAL CAPABILITIES USED
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	1.1.1, 1.1.2, 1.1.4, 1.1.6, 1.1.7, 1.2.1, 1.2.2, 1.2.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8, 1.5	Automated network diagram; access path analysis; PCI network architecture policy validation; Network device configuration hardening and best practices validation.
Requirement 2: Do not use vendorsupplied defaults	2.1, 2.2, 2.2.2, 2.2.3, 2.2.4, 2.3, 2.4, 2.5	Network device configuration hardening and best practices validation.
Requirement 6: Develop and maintain secure systems and applications	6.1, 6.2, 6.4, 6.6, 6.7	Risk mapping and prioritization (threat reference library and network connectivity risk assessment); access policy checks; automated policy validation.
Requirement 11: Regularly test security systems and processes.	11.3, 11.3.1, 11.3.2, 11.3.3, 11.3.4, 11.6	Automated network segmentation change detection; risk mapping and prioritization.
Best Practices/BAU (DSS Page 13)	Monitoring of security controls to ensure they are operating effectively and as intended. Ensuring that all failures in security controls are detected and responded to in a timely manner.	RedSeal supports continuous monitoring of the network architecture and daily verification of segmentation policy. It also supports continuous prioritization of vulnerabilities to identify highest risks.
Sampling (DSS Page 15)	If there are standardized, centralized PCI DSS security and operational processes and controls in place that ensure consistency and that each business facility/system component must follow, the sample can be smaller than if there are no standard processes/controls in place.	RedSeal centralizes and automates the processes of configuration hardening and network segmentation validation.