REDSEAL

PCI DSS ASSESSMENT

Making PCI DSS Compliance a Continuous Process

PCI DSS 3.2 moved from compliance as an annual project to making it "business as usual"—part of your standard operational process. The upcoming release, PCI DSS 4.0 takes it further, asking for security to be a continuous process.

RedSeal's PCI DSS Assessment helps you ensure that your network uses and maintains network segmentation and industry best practices for segmentation requirements involved with PCI DSS compliance. The PCI DSS strongly recommends segmenting your network to reduce the scope and cost of a PCI DSS audit, as well as to simplify PCI DSS maintenance and reduce risk. RedSeal tests and monitors your segmentation to ensure that unauthorized access is not allowed into your cardholder data environment (CDE).

RedSeal's PCI DSS Assessment lets you define and monitor the segmentation your company needs to keep your PCI DSS cardholder data secure. It includes the following action and outcomes:

1. Review Deployment Goals

A RedSeal Professional Services Engineer (PSE) will consult with you and your internal stakeholders, to understand your objectives and the setup of your RedSeal platform, as well as to review the PCI segmentation goals and zones.

2. Assess Network Inventory

We'll review your list of network devices and identify the network devices that are in scope for PCI DSS.

3. Assess Network Devices for Secure Configurations

We'll review the configurations of your network devices, checking whether they adhere to organizational and industry best practices as well as those required for PCI DSS compliance.

4. Review PCI Segmentation

To ensure that your devices are correctly segmented for PCI DSS, we'll review your network map inside the RedSeal platform. You'll see how RedSeal displays interconnectivity between devices—including access paths to/from PCI DSS related security infrastructure devices (e.g. firewalls and routers).

5. Present Findings

When the PCI DSS Assessment is complete, we'll create and review a report that includes remediation advice for non-compliant device configurations (as necessary).

For current customers who need to confirm that they're in compliance with PCI DSS.

- Understand current network segmentation of your network and recommend new segmentation if applicable regarding PCI DSS
    - Receive expert assistance defining and populating your segmentation zones (General, Cardholder, DMZ, Out of Scope, etc.)
- Map data flows—be aware of any access paths between your PCI segments and the rest of your network or vice versa.
- Review security devices for secure, compliant configurations
- Document versions of RedSeal-supported devices, identifying any inconsistencies in software