REDSEAL
CYBER THREAT ASSESSMENT

Identifying attack paths before outsiders do by live scanning or penetration testing is central to determine the effectiveness of your organization's cybersecurity defenses, but can easily disrupt your network. What's more, it's a time-consuming process requiring coordination with multiple departments, including legal, IT, security and network. The RedSeal Cyber Threat Assessment is a virtual penetration test that can be used to prepare for Red Team exercises without further burdening your resource-constrained security teams. It will detect any weaknesses in network device configurations, determine exposure of critical data, and provide recommendations to reduce your risk. RedSeal will both identify and analyze potential attack paths—virtually—and train your personnel to do the same. Our experienced engineers will demonstrate how you can use RedSeal to run tabletop exercises as required by National Institute of Standards and Technology (NIST), Cybersecurity Maturity Model Certification (CMMC), Payment Card Industry Data Security Standard (PCI DSS), and North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) compliance.

1. Review Deployment Goals
A RedSeal Professional Services Engineer (PSE) will consult with you and your internal stakeholders to review your security goals, network environment, and the network subnets that will be targeted in the threat assessment.

2. Assess Network Devices for Secure Configurations
We'll remotely perform a multi-point evaluation of your RedSeal deployment to determine the health of your RedSeal platform, and how well it's aligned with your business goals. Then, we'll assess your devices to make sure they're securely configured.

3. Conduct Threat Assessment
When the diagnostics are complete, we'll meet with you to discuss our findings. We'll provide any needed remediation advice to secure the critical subnets that host sensitive data such as confidential information, intellectual property or financial data.

4. Present Findings
When the Threat Assessment is complete, we'll create a report and meet with you to discuss our findings. We'll make sure that you're aware of any threats opening up your internal designated subnets to attack and provide remediation advice.

The RedSeal Cyber Threat Assessment is for existing customers who want to:

- Identify open access into a network from the internet
- Review security device configurations for industry best standards
- Document versions of RedSeal-supported devices, exposing possible software inconsistencies
- Find access to vulnerabilities from untrusted areas of a network
- Enumerate legitimate access into sensitive areas of your network

Remote assessment of 1-4 subnets with similar profiles