

# REDSEAL

## HEALTH CHECK SERVICE

### HEALTH CHECK OVERVIEW

In response to work at home/shelter in place requirements, our business networks have had to change rapidly. We need to ensure that our current network infrastructures can accommodate increased numbers of remote workers—and continue to be secure.

So that you have your business outcomes continually met and what you need to drive your cyber visibility, compliance, and risk vulnerability efforts forward, RedSeal offers this complementary Health Check Service. It includes the following actions and outcomes:

#### 1. Review Deployment Goals

A RedSeal Professional Services Engineer will consult with you and your internal stakeholders to review the objectives for your RedSeal deployment, expected business outcomes, and explain the Health Check Service process.

#### 2. Multi-Point Evaluation

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.

#### 3. Present Findings

When the diagnostics are complete, we'll meet with you to discuss our findings. We'll provide any needed remediation advice to ensure the RedSeal deployment is working to deliver your expected business outcomes.

This complimentary Health Check Service includes a review of your RedSeal deployment and prioritized recommendations. It is highly recommended for:

- Existing RedSeal customers who haven't had resources to manage their RedSeal deployment
- New RedSeal administrators looking to understand their current RedSeal platform setup and get a quick review of features, and recommended actions to operationalize the platform
- Management teams looking to confirm business outcomes from their RedSeal deployment

# REDSEAL

## HEALTH CHECK SERVICE

### RedSeal Risk Management Methodology

Our three-step Risk Management Methodology advocates the continuous use of the RedSeal platform's capabilities to maintain and enhance your organization's cybersecurity posture. The steps are:

**1. Discover** Network (on-premise, cloud, hybrid cloud, and SDN) and endpoint inventories, connections, and associated risk.

**2. Investigate** the information and focus on high risk areas to lower overall risk to an acceptable level across supported cloud infrastructure and physical environments.

**3. Act** to make informed remediation decisions to protect the organization from cybersecurity attacks.

### REDSEAL RISK MANAGEMENT METHODOLOGY

**DISCOVER** YOUR ASSETS  
AND CONNECTIONS; IMPORT  
VULNERABILITY SCANS



**INVESTIGATE** SECURITY  
AND SCAN COVERAGE GAPS;  
PRIORITIZE RISK

**ACT** TO MITIGATE RISKS