REDSEAL
MANAGED SERVICE PACKAGES

REDSEAL MANAGED SERVICE PACKAGES

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 your business outcomes are continually delivered, and you have what you need to drive your cyber visibility, compliance, and risk vulnerability efforts forward, we offer three annual managed service packages.

Depth of Engagement from RedSeal

Cyber Visibility Package
- Network and endpoint Inventory assessments
- Secure configuration assessments
- Ongoing platform updates and management
- Knowledge transfer

Cyber Compliance Package
- Network segmentation and compliance monitoring
- Security change review

Includes Cyber Visibility Package

Cyber Risk Management Package
- Security posture monitoring
- Incident investigation
- Vulnerability risk prioritization

Includes both Cyber Visibility and Cyber Compliance Packages

Value to Customer

MANAGED SERVICE PACKAGES: OVERVIEW

To support your RedSeal deployment, RedSeal's annual managed service packages provide ongoing remote assessments and prioritized recommendations so your teams can address the issues that are most critical to maintaining your organization's security posture.

Cyber Visibility Package Benefits

- Ongoing visibility into what assets you have and how they're connected
- Monitoring your established set of baseline security controls and network best practices
- A roadmap for your security team—developed and executed
- Prioritized recommendation for controls
- Maintenance of basic security and operational hygiene
- Ongoing platform updates and management

Cyber Compliance Package Benefits

- Compliance with regulatory, internal network segmentation requirements
- Accelerated security change reviews

Cyber Risk Management Package Benefits

- Focused remediation—move from "patch everything" to "patch what matters the most" based on asset criticality and reachability from untrusted connections
- Critical systems kept up to date to protect against compromise from cyberattacks
- Quantitative risk data used for decision making