



DELIVER WINNING SECURITY SERVICES

Harnessing RedSeal Security Risk Manager to Strengthen Your Offerings

REDSEAL OFFERS A POWERFUL TOOL THAT STRENGTHENS YOUR CONSULTING PRACTICE. THIS INFORMATION IS PROVIDED TO DEFINE SOME OF THE ADDITIONAL SERVICES YOU CAN OFFER, USING REDSEAL™ SECURITY RISK MANAGER™ (SRM). RED SEAL SRM OFFERS YOU A WAY TO BOOST THE IT SECURITY OF YOUR CLIENT'S NETWORKS— ELIMINATING SECURITY EXPOSURES THAT CAN LEAD TO A BREACH.

Provide New Services that Win Sales and Deepen Account Penetration

RedSeal SRM offers a fast, effective way to add new services to your portfolio:

- Firewall and router audits
- Security remediation planning
- Remediation execution

Instantly Audit Firewalls and Routers

RedSeal automatically collects router and firewall configuration information to create a comprehensive model of the network's components and their interconnectivity.

- Each time data is imported, RedSeal SRM checks every firewall and router configuration as well as the security policy rules for those devices to verify that they have been properly configured.
- RedSeal SRM can spot a range of potential issues, including default passwords, lack of security on administrator access, redundant Access Control Lists (ACLs), and more.
- The RedSeal network configuration check (NCC) function occurs both during import and after analysis is run. Each check failure represents either a violation of best-practices policy or a symptom of a configuration error.
- RedSeal SRM provides guidance on possible remediation steps and visibility as to where in the configuration or security policy the violation was found.

- The results are summarized within the graphical topology and inventory rendering as well as in a set of pre-defined reports which can serve as a security task list or audit result.

Security Remediation Planning

RedSeal SRM plots a graphical network model to group critical assets, such as SOX-associated servers, CRM applications, and others.

- During analysis, RedSeal SRM computes all possible attack vectors to those critical servers, factoring in the applications they are running as well as the access rules that control associated traffic flow.
- The analysis also takes into account the value of these assets relative to others in the network.
- For each server in the critical asset group RedSeal SRM shows the vulnerability count, the severity of those vulnerabilities, the amount of network exposure that they allow, as well as the potential for downstream attacks.
- These results can be filtered and exported to a file, making it easy for you to list the most critical vulnerabilities, and prioritize remediation.
- Further, these reports can provide the basis of historical trend documentation that can be used to fulfill internal and third party audit requirements.



Instant Visibility. Threats Averted.

About RedSeal Systems

RedSeal Inc. provides security risk management solutions that give instant visibility into the threats that leave an open door to valuable company resources.

Evaluate in Your Environment

It only takes 30 minutes to go through an introductory evaluation. Using data from your systems you can see for yourself how RedSeal SRM can help your IT security team identify the most critical vulnerabilities.

E-mail eval@redseal.net
Call 1-888-845-8169
or visit www.redseal.net