RedSeal Network Exposure Management Platform

Don't wait until you've experienced a breach or failed an audit to learn what's on—and off about—your hybrid network. The RedSeal platform helps you take a proactive, continuous approach to cybersecurity and compliance, resulting in greater productivity for your teams, maximum protection for your network, and reduced risk for your organization.

The single source of truth for your hybrid network

RedSeal is a network exposure management platform that helps you close the gaps in your hybrid network security controls. It finds the subnets, access paths, and devices on your network you don't know are there. And if you don't know about them, you don't know what else is connected to them—directly or indirectly, several hops away.

It's those unknowns that put security and compliance at risk. RedSeal helps you manage that risk efficiently by providing a single source of truth that all teams can trust.

Powering continuous threat exposure management (CTEM)

RedSeal is foundational to continuous threat exposure management (CTEM) as a strategic and proactive approach to cybersecurity. RedSeal simplifies and accelerates the CTEM process by delivering a powerful combination of capabilities in a single platform:

- **Network visualization**, bringing all assets and connections into a cohesive, interactive model
- **Attack path analysis**, surfacing all the ways threats can spread laterally through the network
- **Risk prioritization**, ranking all vulnerabilities and other exposures according to true business impact
- **Continuous compliance**, monitoring adherence to external requirements, internal policies, and best practices.

RedSeal integrates with 125+ common (and not-so-common) networking and security products from 65+ vendors to model your hybrid network.
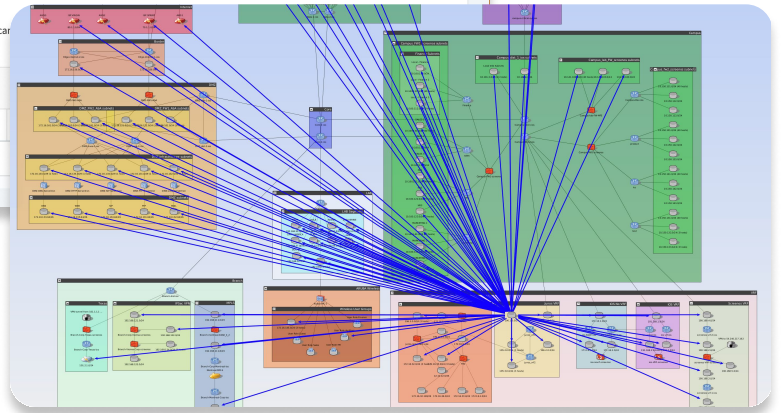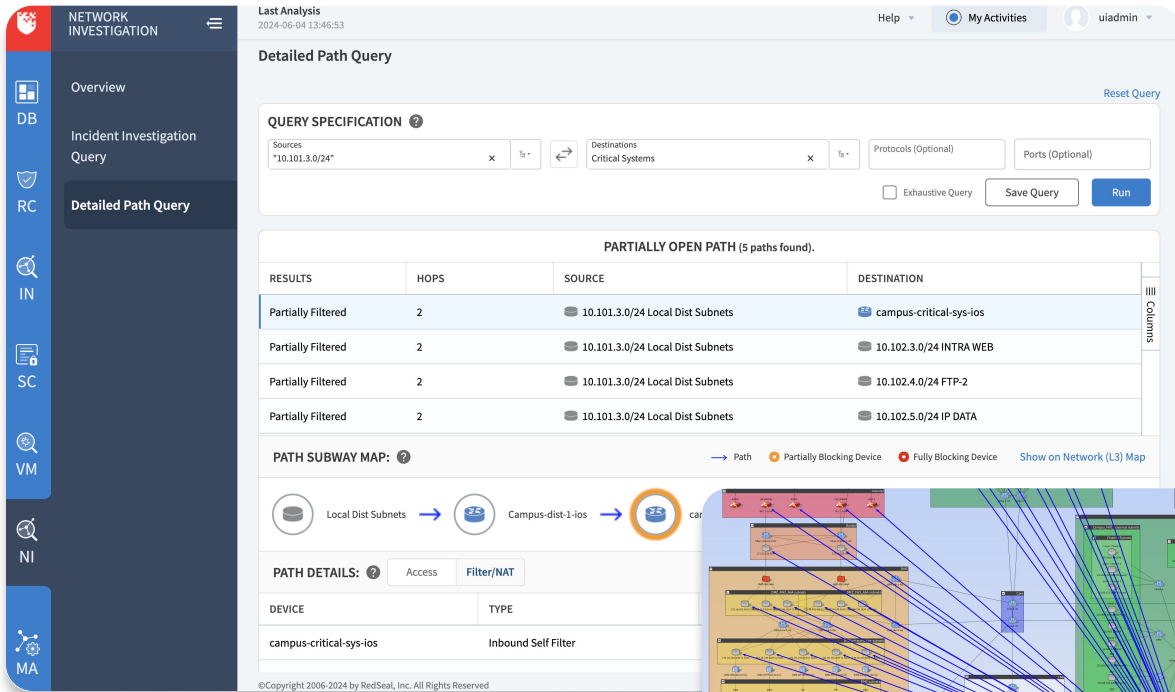
Reduce risk by uncovering unintended connections that lead to high-value assets.

Gain comprehensive network visibility

RedSeal integrates with your existing security and infrastructure investments to build an accurate, interactive model of your entire hybrid network. That model serves as your network's digital twin, ready to answer any questions about devices, resources, configurations, and access, in just a few clicks.

- Bring private cloud, public cloud, and physical resources into a single view, without agents that impact your production environment
- Discover and inventory all networked assets, including those previously unknown or unaccounted for
- See all connectivity among assets, subnets, and internet exposure points, whether traffic is present or not

See every possible attack path

RedSeal thinks like an adversary—at the network level—and finds hidden connectivity that NetOps and SecOps teams don't know about or never intended to create. It shows you all the ways threats can enter and spread laterally through your network, and the exact controls to change to block them.

- Identify and visualize all access paths, traffic flows, and threat vectors, including those that circumvent firewalls or segmentation policies
- Get a hop-by-hop mapping of access from source(s) to destination(s)
- Run a virtual pen test on your entire network at once, revealing vulnerabilities that are, in fact, exploitable
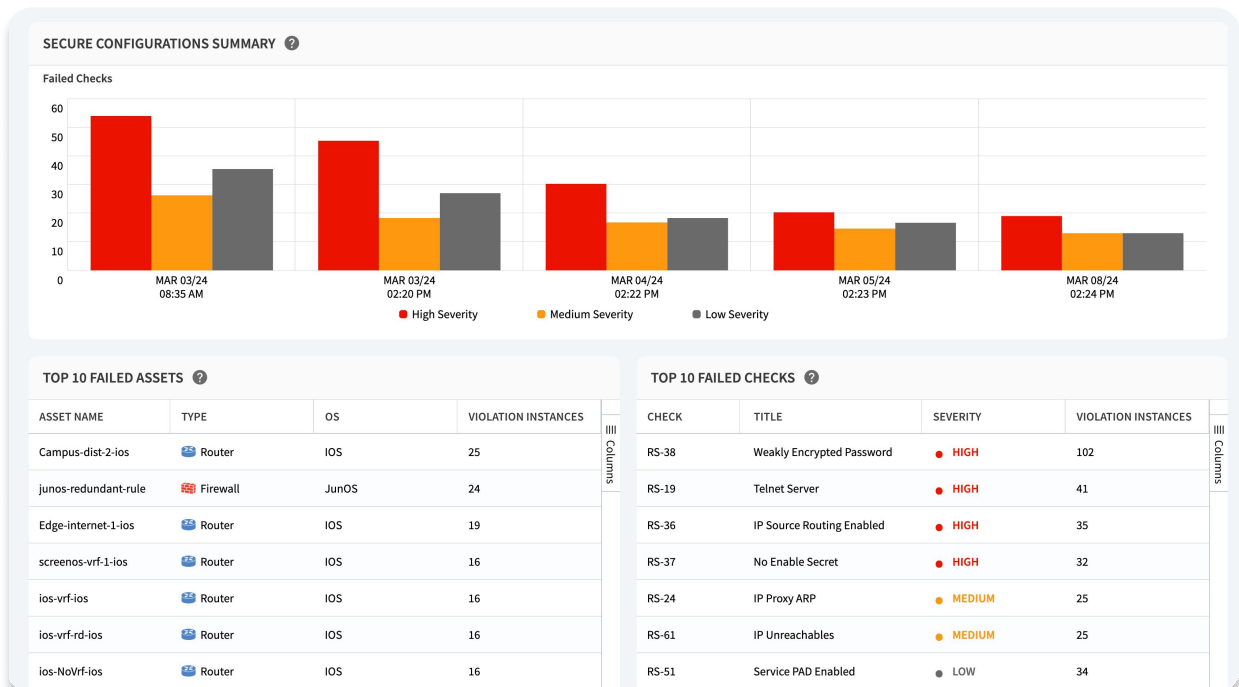
Prioritize the risks that really matter

RedSeal prioritizes all vulnerabilities and exposures according to their risk (or "blast") radius, and delivers detailed validation and guidance to accelerate remediation. Risk radius is based on insights from vulnerability scanners and other security tools enhanced with network context—a breadth and depth of understanding only RedSeal can deliver—to reflect the true business impact.

- Accelerate risk reduction by focusing teams on fixing the most business-critical vulnerabilities first
- Improve the accuracy of vulnerability scanners by identifying optimal placement and missed or blocked coverage areas
- Don't waste cycles on false positives or vulnerabilities that aren't actually exploitable
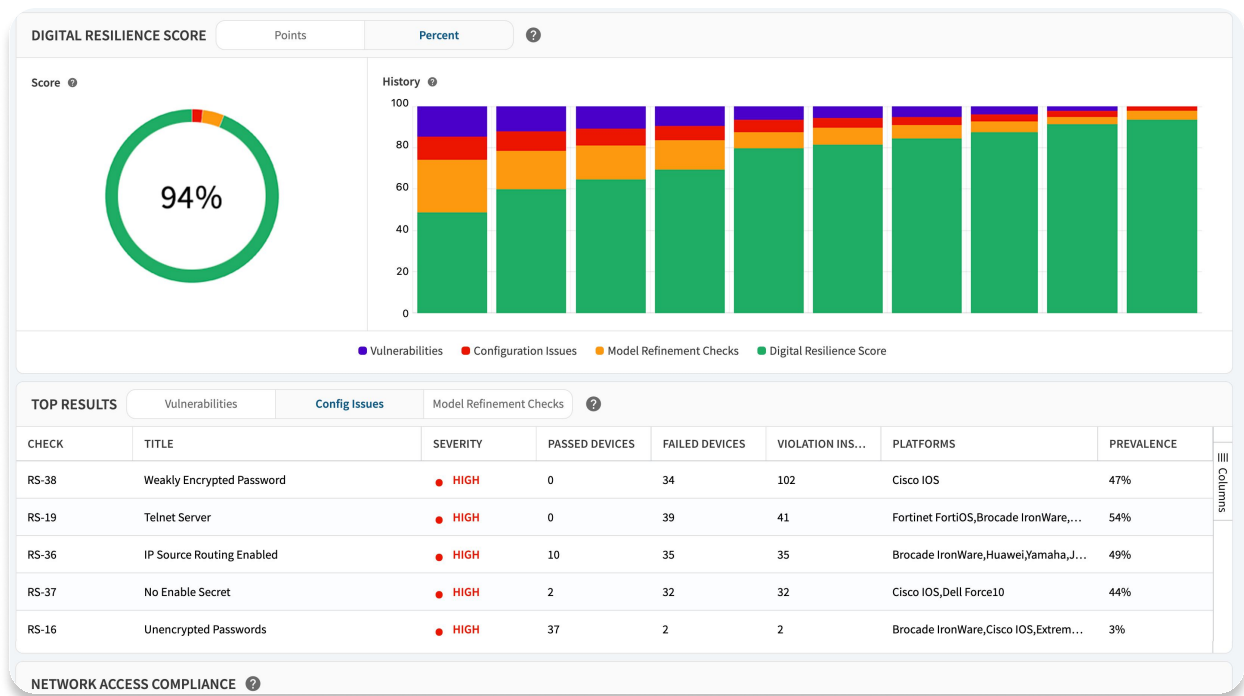
Ensure continuous compliance

On an ongoing basis, RedSeal runs checks against external requirements, best practices, and internal or custom policies, and alerts you to any issues—from governmental regulations and industry standards (e.g., STIG, CIS, NIST, PCI DSS, and HIPAA) to segmentation, password, and patching policies. RedSeal comes with more than 160 best-practice checks built into the platform.

- Fight compliance drift between audits or incidents by proactively and continuously running checks on the whole network
- Identify device configurations, network segmentation, and firewall rules—existing or proposed—that violate security policies
- Measure your network's digital resilience as a board-level metric to report and monitor your security posture over time

SECURE CONFIGURATIONS SUMMARY ⑦

Failed Checks

MAR 03/24 08:35 AM	MAR 03/24 02:20 PM	MAR 04/24 02:22 PM	MAR 05/24 02:23 PM	MAR 08/24 02:24 PM

● High Severity   ● Medium Severity   ● Low Severity

TOP 10 FAILED ASSETS ⑦

ASSET NAME	TYPE	OS	VIOLATION INSTANCES
Campus-dist-2-ios	🖧 Router	IOS	25
junos-redundant-rule	🧱 Firewall	JunOS	24
Edge-internet-1-ios	🖧 Router	IOS	19
screenos-vrf-1-ios	🖧 Router	IOS	16
ios-vrf-ios	🖧 Router	IOS	16
ios-vrf-rd-ios	🖧 Router	IOS	16
ios-NoVrf-ios	🖧 Router	IOS	16

TOP 10 FAILED CHECKS ⑦

CHECK	TITLE	SEVERITY	VIOLATION INSTANCES
RS-38	Weakly Encrypted Password	● HIGH	102
RS-19	Telnet Server	● HIGH	41
RS-36	IP Source Routing Enabled	● HIGH	35
RS-37	No Enable Secret	● HIGH	32
RS-24	IP Proxy ARP	● MEDIUM	25
RS-61	IP Unreachables	● MEDIUM	25
RS-51	Service PAD Enabled	● LOW	34

Reduce audit cycles by running compliance checks and documenting findings ahead of time.

Report your overall network security posture with confidence.

Designed for teams like yours

RedSeal is designed to help different teams, who have different responsibilities and priorities, work better and faster together in the battle against cyber risk. The platform offers a robust set of technical features that deliver a variety of business benefits across your organization.

- **Security operations:** Augment every other security tool you have by adding unmatched network context to any risk assessment
- **Network operations:** Get a level of network understanding you just won't get from other solutions (or patchwork of solutions)
- **Risk and compliance:** Be more proactive and comprehensive about compliance with direct, documented, and actionable insights
- **Executive leadership:** Measurably reduce risk and communicate your network security posture with confidence

Protect your organization from evolving threats

From brute-force hacking to sophisticated phishing and ransomware attacks, the best defense against threats you can't predict is knowing your network better than any adversary does. Human beings alone can't possibly keep track of every connection, understand every risk, or know how to manage them all—and certainly not at the speed and scale of business today. You need an automated solution that's always looking at the bigger picture.

Contact us today to learn how RedSeal can help your organization strengthen cybersecurity and compliance in your hybrid environment with network exposure management.

Contact RedSeal for more information or request a demo today.