REDSEAL

RedSeal Exposure Management Platform

A unified, always-accurate view of the entire environment — with the context to see what's truly exposed, prioritize risk, and act with confidence.

Security teams today are buried under disconnected tools, incomplete inventories, and constant change. Point-in-time scans can't keep pace, leaving blind spots that adversaries exploit. What's missing is a living picture of the entire environment, not just assets, but how they connect, and which exposures truly matter.

RedSeal closes this gap. By unifying visibility across IT (on-prem, cloud, remote workers), OT, and IoT environments, RedSeal delivers the clarity, context, and confidence to focus on what reduces the most risk — faster and more effectively.

RedSeal at a Glance

- ✓ **Continuously Updated Digital Twin**
  A living, enriched environment model that includes hidden configurations and dynamic connections.
- ✓ **Risk Radius™ Prioritization**
  Identifies and ranks exposures by real-world exploitability and potential business impact.
- ✓ **Agentless, Non-Disruptive Integration**
  Rapid integration with 2,000+ security and infrastructure systems and devices across IT (on-prem, cloud, remote workers), OT, and IoT environments.
- ✓ **Proven Resilience at Scale**
  Trusted by Fortune 1000 companies and the U.S. military.

Unified Risk Reduction Across Frameworks

No matter which framework you follow — Zero Trust, National Institute of Standards and Technology (NIST), Continuous Threat Exposure Management (CTEM), or your own — RedSeal simplifies and accelerates risk reduction by delivering a powerful combination of capabilities in a single platform.

Every capability in RedSeal works in concert, each layer deepening the insights from the one before.

Hybrid Environment Modeling builds the foundation: a complete, living model of your entire environment.

Attack Path Analysis overlays this model with the ways threats can traverse it, showing not just where weaknesses exist, but how they could.

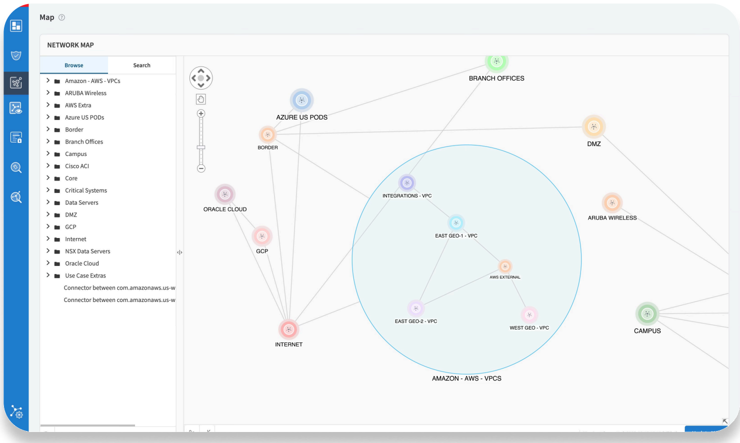
Risk Prioritization then cuts through the noise of endless vulnerability lists by ranking what's truly dangerous, factoring in exploitability and business impact, so teams fix the issues that actually reduce the most risk.

Continuous Compliance ensures your defenses stay aligned with policies and industry standards.

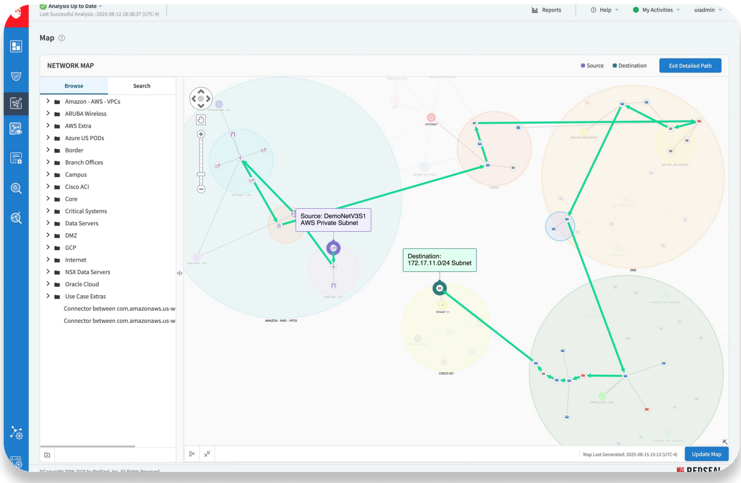
RedSeal integrates with more than 2,000 third-party security and infrastructure systems and devices — unifying data across IT (on-prem, cloud, remote workers), OT, and IoT. Combined with our layered capabilities, this helps your team shift from reactive firefighting to proactive, measurable risk reduction.

How It Works

RedSeal Workflow is an add-on orchestration engine within RedSeal. Customers design workflows with a low/no-code builder, triggered by scheduled events, change requests, or user actions. Workflows connect RedSeal's hybrid environment model with external data, carry out actions like creating scopes or opening tickets, and can include validation steps to re-check exposures after fixes. This closes the loop from detection to resolution.



Get the big picture view – of your entire IT (on-prem, cloud, remote workers), OT, and IoT environment.



Last Successful Analysis : 2025-08-12 18:38:37 (UTC-4)

Source: DemoNetV3S1
AWS Private Subnet

Destination:
172.17.11.0/24 Subnet

Map Last Generated: 2025-08-15 15:13 (UTC-4)

Get a detailed analysis of all potential attack paths from inside or outside the network.

Attack Path Analysis

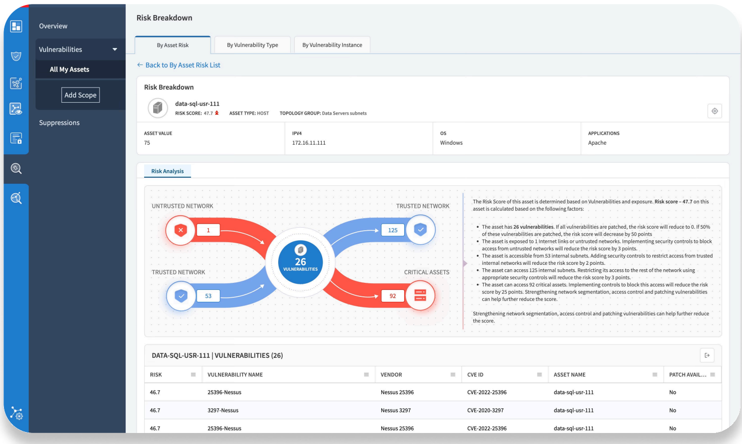
See every way attackers could get in — and where they could go — before they strike.

Attackers don't just exploit a single weakness; they look for ways to enter your environment and move toward high-value targets. RedSeal identifies every possible attack path and goes beyond simple mapping by evaluating your existing security controls. It reveals which paths are truly exploitable, even with defenses in place, and filters out the noise of false positives. The result: a clear, actionable view of real risks so you can shut down the gaps that matter most.

Risk Prioritization

Fix the risks that matter most and skip the ones that don't.

In a perfect world, you could remediate every vulnerability. That wastes precious time and resources on issues that may never be exploited. Security teams face thousands of findings, but most tools can't tell which ones pose real danger. RedSeal Risk Radius™ combines likelihood of compromise with business impact to prioritize exposures that truly matter. By factoring in asset value, attack paths, existing controls, and whether an exposure is internal or external, it helps teams focus on what's both exploitable and consequential, driving the greatest risk reduction with the least effort.



Risk Breakdown

Risk Breakdown

data-sql-usr-111

RISK SCORE: 47.7 ASSET TYPE: HOST TOPOLOGY GROUP: Data Servers subnets

ASSET VALUE	IPV4	OS	APPLICATIONS
75	172.16.11.111	Windows	Apache

The Risk Score of this asset is determined based on Vulnerabilities and exposure. **Risk score – 47.7** on this asset is calculated based on the following factors:

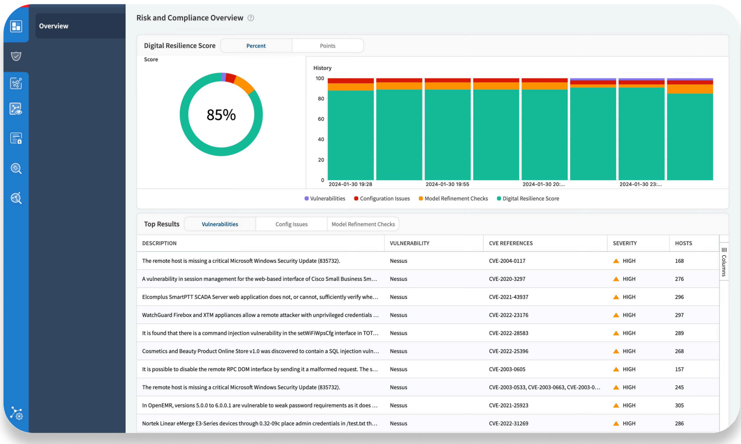
- The asset has **26 vulnerabilities**. If all vulnerabilities are patched, the risk score will reduce to 0. If 50% of these vulnerabilities are patched, the risk score will decrease by 50 points
- The asset is exposed to 1 Internet links or untrusted networks. Implementing security controls to block access from untrusted networks will reduce the risk score by 3 points.
- The asset is accessible from 53 internal subnets. Adding security controls to restrict access from trusted internal networks will reduce the risk score by 2 points.
- The asset can access 125 internal subnets. Restricting its access to the rest of the network using appropriate security controls will reduce the risk score by 3 points.
- The asset can access 92 critical assets. Implementing controls to block this access will reduce the risk score by 25 points. Strengthening network segmentation, access control and patching vulnerabilities can help further reduce the score.

Strengthening network segmentation, access control and patching vulnerabilities can help further reduce the score.

DATA-SQL-USR-111 | VULNERABILITIES (26)

RISK	VULNERABILITY NAME	VENDOR	CVE ID	ASSET NAME	PATCH AVAIL...
46.7	25396-Nessus	Nessus 25396	CVE-2022-25396	data-sql-usr-111	No
46.7	3297-Nessus	Nessus 3297	CVE-2020-3297	data-sql-usr-111	No
46.7	25396-Nessus	Nessus 25396	CVE-2022-25396	data-sql-usr-111	No

Visualize risk with truly transparent scoring that combines vulnerability exposure, network access paths, and business impact to prioritize the assets that pose the greatest threat to your organization.



Risk and Compliance Overview

Digital Resilience Score

Top Results

DESCRIPTION	VULNERABILITY	CVE REFERENCES	SEVERITY	HOSTS
The remote host is missing a critical Microsoft Windows Security Update (835732).	Nessus	CVE-2004-0117	▲ HIGH	168
A vulnerability in session management for the web-based interface of Cisco Small Business Sm...	Nessus	CVE-2020-3297	▲ HIGH	276
Elcomplus SmartPTT SCADA Server web application does not, or cannot, sufficiently verify whe...	Nessus	CVE-2021-43937	▲ HIGH	296
WatchGuard Firebox and XTM appliances allow a remote attacker with unprivileged credentials ...	Nessus	CVE-2022-23176	▲ HIGH	297
It is found that there is a command injection vulnerability in the setWiFiWpsCfg interface in TOT...	Nessus	CVE-2022-28583	▲ HIGH	289
Cosmetics and Beauty Product Online Store v1.0 was discovered to contain a SQL injection vuln...	Nessus	CVE-2022-25396	▲ HIGH	268
It is possible to disable the remote RPC DOM interface by sending it a malformed request. The s...	Nessus	CVE-2003-0605	▲ HIGH	157
The remote host is missing a critical Microsoft Windows Security Update (835732).	Nessus	CVE-2003-0533, CVE-2003-0663, CVE-2003-0...	▲ HIGH	245
In OpenEMR, versions 5.0.0 to 6.0.0.1 are vulnerable to weak password requirements as it does ...	Nessus	CVE-2021-25923	▲ HIGH	305
Nortek Linear eMerge E3-Series devices through 0.32-09c place admin credentials in /test.txt th...	Nessus	CVE-2022-31269	▲ HIGH	286

Use your Digital Resilience Score as a board-level metric to report and monitor your security posture over time.

Continuous Compliance

Stay audit-ready with continuous control validation and policy checks.

Traditional compliance checks are manual and point-in-time creating gaps, false confidence, and last-minute surprises. RedSeal continuously validates your environment against internal policies and standards like NIST, PCI DSS, and CMMC. With automated checks and "what-if" simulations, teams can catch violations early, test changes safely, and ensure security and compliance are maintained.

Reduce risk. Prove resilience.

RedSeal gives you a complete, always-current view of your hybrid environment, pinpoints the exposures that matter most, and delivers actionable results in days, so you can measurably reduce risk and strengthen resilience.

Contact RedSeal for more information or request a demo today.

RedSeal, a leader in exposure management, helps organizations know their environments better than any adversary. By creating a dynamic digital twin, RedSeal delivers comprehensive visibility, strengthens digital resilience, and reduces business risk. Trusted by Fortune 1000 companies and U.S. military branches, RedSeal enhances operational efficiency and improves security outcomes.

www.redseal.net | info@redseal.net | +1 408-641-2200 | 888-845-8169