Know Your Hybrid Environment with RedSeal

A complete guide to the RedSeal exposure management platform

REDSEAL

Table of Contents

Introduction

RedSeal is an exposure management platform that identifies assets in your hybrid environment that are exposed to risk and delivers actionable insights to close defensive gaps. It is the missing link in today's cybersecurity tech stack, providing environmental context other tools don't have and surfacing flaws they can't see. Fundamentally, the RedSeal platform serves as a single source of truth that improves efficiency and collaboration across teams and is a powerful ally in the fight against cyber risk.

As a company, RedSeal has been pioneering and perfecting exposure management for more than two decades. The result is a platform packed with powerful features and benefits for security, network, and compliance professionals. RedSeal covers your entire hybrid environment, across IT (on-prem, cloud, remote workers), OT, and IoT.

This document breaks down the core capabilities of the RedSeal platform, organized around its four fundamental design pillars:

- **Hybrid Environment Modeling**, bringing all assets and connections into a unified, interactive digital twin
- **Attack Path Analysis**, surfacing all the ways threats can spread laterally through an environment
- **Risk Prioritization (Risk Radius™)**, ranking exposures and vulnerabilities according to real business impact
- **Continuous Compliance**, assessing adherence to external requirements, internal policies, and best practices

As you'll see, there's a lot you can do with RedSeal — and a lot RedSeal can do for your organization.

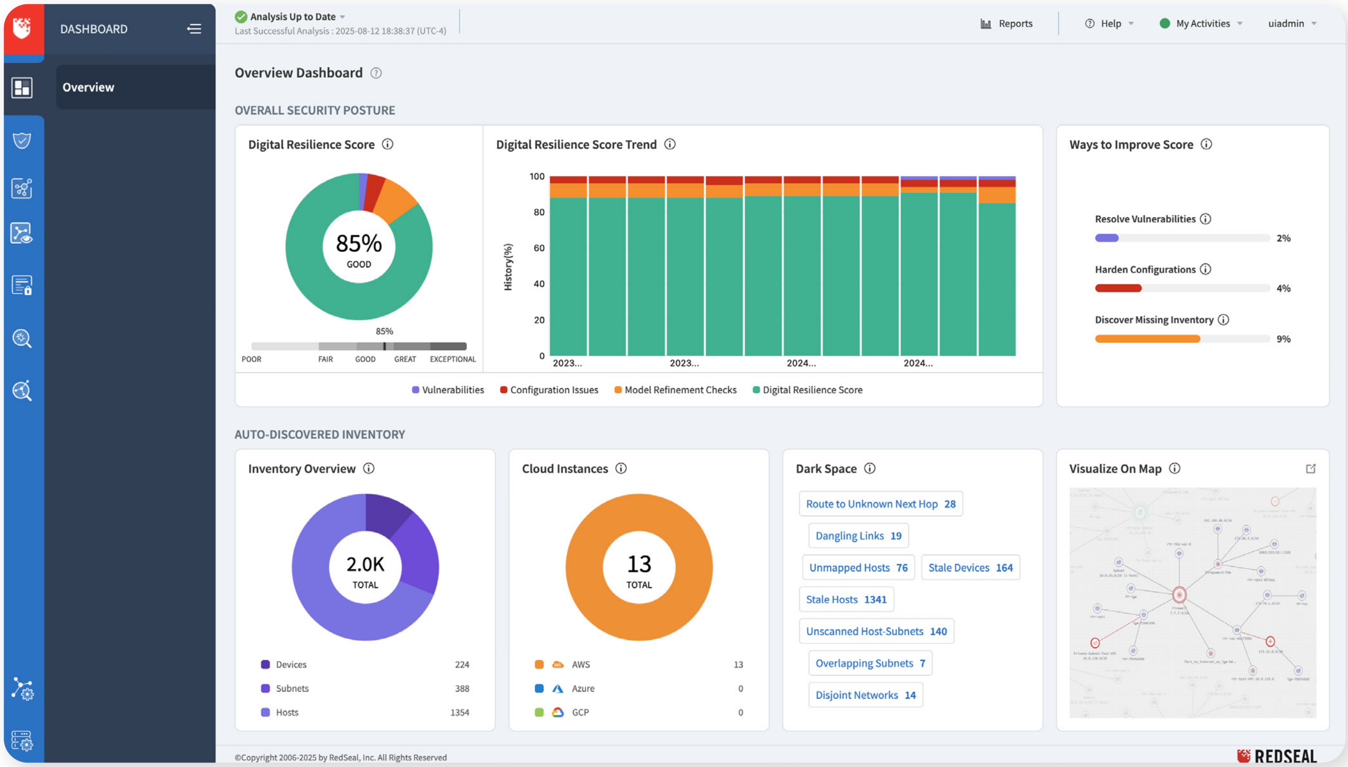
RedSeal is Designed for You

RedSeal helps diverse teams work smarter and faster against cyber risk — combining deep technical capabilities with business outcomes that matter across the organization.

- **Security Operations (SecOps): Get ahead of threats.**
  Uncover exposures across your hybrid environment, prioritize what matters, and give NetOps the evidence to remediate quickly. With clear context, SecOps accelerates response and reduces mean time to resolution.
- **Network Operations (NetOps): Execute fixes with precision.**
  Pinpoint affected assets, see how they're connected, and make changes with confidence. With an always-current model of the environment, NetOps reduces false positives, automates processes, and collaborates seamlessly.
- **Risk & Compliance: Stay audit-ready.**
  Validate continuously against policies and standards, identify gaps before changes go live, and generate audit-ready reports that prove cyber maturity.
- **CISOs & Executives: Measure and report with confidence.**
  Simplify board communication with a single Digital Resilience Score and unified reporting. Track progress, streamline operations, and report on risk posture with clarity.

The RedSeal Advantage

A common operating picture that unites teams, accelerates collaboration, and ensures leadership can trust their risk posture.



RedSeal's executive dashboards and detailed reports help you show measurable risk reduction and a stronger security posture.

How RedSeal works

Enabled by **agentic AI**, RedSeal brings it all together in one platform and delivers focused insights to manage risk efficiently. The platform builds a **comprehensive, dynamic digital twin** of your hybrid environment, showing every asset, how it's connected, and the associated risks. This model becomes the foundation of a proactive cybersecurity strategy — ensuring you know your environment better than any adversary.

RedSeal serves as the source of truth for hybrid environment modeling, attack path analysis, risk prioritization, and continuous compliance.

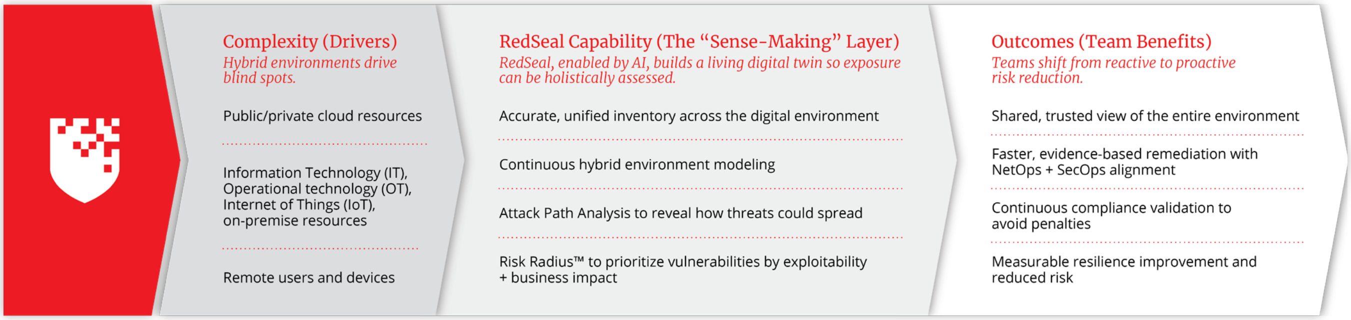
Every capability in RedSeal works in concert, each layer deepening the insights from the one before:

1. Hybrid Environment Modeling creates a complete, living model of your entire environment, letting you see and interact virtually with every asset
2. Attack Path Analysis overlays this model with the ways threats can traverse it, revealing not just where weaknesses exist, but how they could be exploited
3. Risk Prioritization (Risk Radius™) cuts through the noise of endless vulnerability lists by ranking what's truly dangerous — factoring in exploitability and business impact — so teams focus on the issues that reduce the most risk
4. Continuous Compliance ensures your defenses remain aligned with internal policies and industry standards, even as environments and requirements evolve

What RedSeal needs to build the model:

- **Configuration data** from on-premises devices like routers, switches, firewalls, and load balancers.
- **Vulnerability and host data** from scanners and endpoint protection tools.
- **API access** to cloud and virtual infrastructure.

With 2,000+ integrations across security and infrastructure systems and devices, RedSeal ingests this data without agents, span ports, taps, or NetFlow. Patented algorithms and **AI-enabled context** transform it into prioritized insights you can trust.



Complexity (Drivers)

Hybrid environments drive blind spots.

Public/private cloud resources

Information Technology (IT), Operational technology (OT), Internet of Things (IoT), on-premise resources

Remote users and devices

RedSeal Capability (The "Sense-Making" Layer)

RedSeal, enabled by AI, builds a living digital twin so exposure can be holistically assessed.

Accurate, unified inventory across the digital environment

Continuous hybrid environment modeling

Attack Path Analysis to reveal how threats could spread

Risk Radius™ to prioritize vulnerabilities by exploitability + business impact

Outcomes (Team Benefits)

Teams shift from reactive to proactive risk reduction.

Shared, trusted view of the entire environment

Faster, evidence-based remediation with NetOps + SecOps alignment

Continuous compliance validation to avoid penalties

Measurable resilience improvement and reduced risk

RedSeal integrates with 2,000+ security infrastructure systems and devices to build a continuously updated, AI-enabled digital twin of your hybrid environment.

Hybrid Environment Modeling

A living digital twin of your entire environment — continuously updated and AI-enabled

Hybrid Environment Modeling

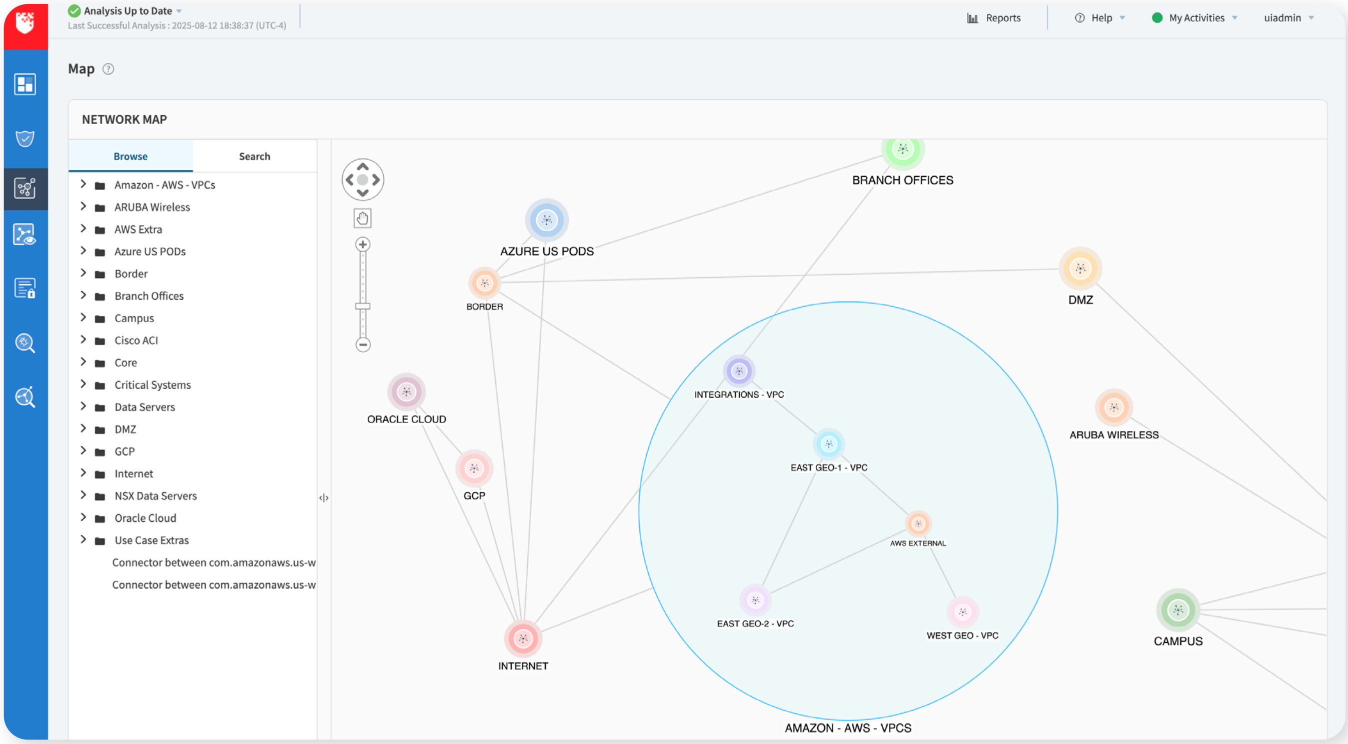
Knowing what's in your environment and how it's all connected is the first step to staying secure and compliant. Blind spots are inevitable if you can't see the bigger picture. RedSeal reveals and makes sense of it all.

What can you do with RedSeal?

- Build an accurate and comprehensive **digital twin** of your hybrid environment
- IT (on-prem, cloud, remote workers), OT, and IoT resources into one consolidated view
- Present the logical layout of assets and groupings in a clear, visual topology
- Map the physical location of assets and their Layer 2 connectivity
- See all available traffic paths among assets, subnets, and internet exposure points
- Discover inconsistencies as well as assets and connections previously unknown or unaccounted for
- Gain visibility into IPv6 usage and connectivity

The RedSeal Advantage

- ✓ Maintain a single source of truth for your hybrid environment that every team can trust
- ✓ Eliminate blind spots by surfacing assets, connections, and exposures other tools miss
- ✓ Gain AI-enabled context that transforms raw data into actionable insights



Get the big picture view—of your entire hybrid environment.

Asset Inventory

RedSeal is meticulous about documenting your environment's assets and keeping asset information current and complete. This ensures your digital twin stays accurate and reflects the full scope of your investments — across IT (on-prem, cloud, remote workers), OT, and IoT resources.

What can you do with RedSeal?

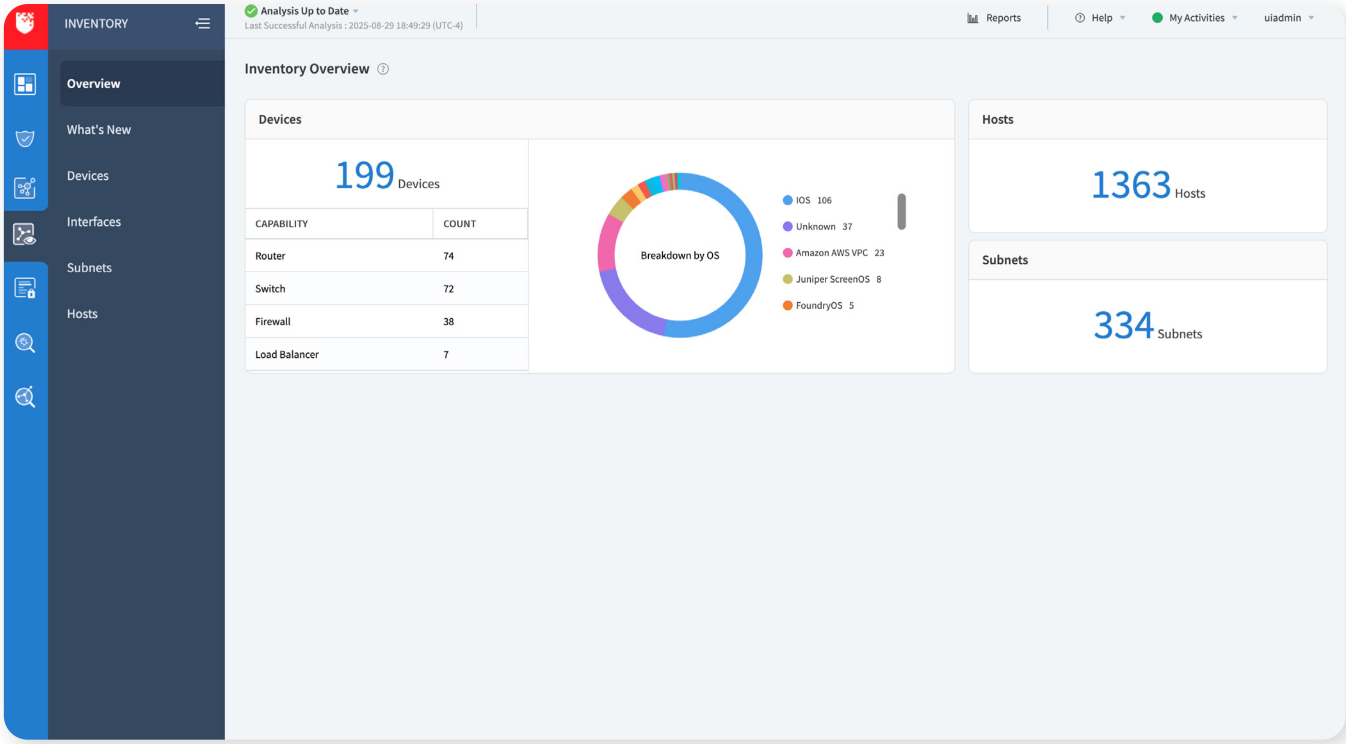
- Discover and inventory all Layer 2 and Layer 3 devices, hosts, and endpoints, including IPv4 and IPv6 connected assets
- Discover and inventory all resources in multiple cloud platforms and SDNs
- Assign business value to assets for smarter risk analysis — automatically or manually
- Identify stale devices, unused credentials, and hidden or missing hosts
- Import, consolidate, deconflict, and store host data from multiple sources (name, location, OS, access, installed patches, apps, and more)
- Detect potentially missing devices and continuously validate completeness of your environment

The RedSeal Advantage

✓ Automatically discover and classify devices & assets across IT (on-prem, cloud, remote workers), OT, and IoT

✓ Continuously monitor the completeness and health of your inventory

✓ Identify stale or missing devices before they create hidden risks



Analysis Up to Date

Last Successful Analysis : 2025-08-29 18:49:29 (UTC-4)

Inventory Overview

Devices

199 Devices

CAPABILITY	COUNT
Router	74
Switch	72
Firewall	38
Load Balancer	7

Hosts

1363 Hosts

Subnets

334 Subnets

Get a complete, searchable inventory of all connected assets, including cloud resources.

Attack Path Analysis

See how threats could move laterally through your hybrid environment — before attackers do

Access & Threat Queries

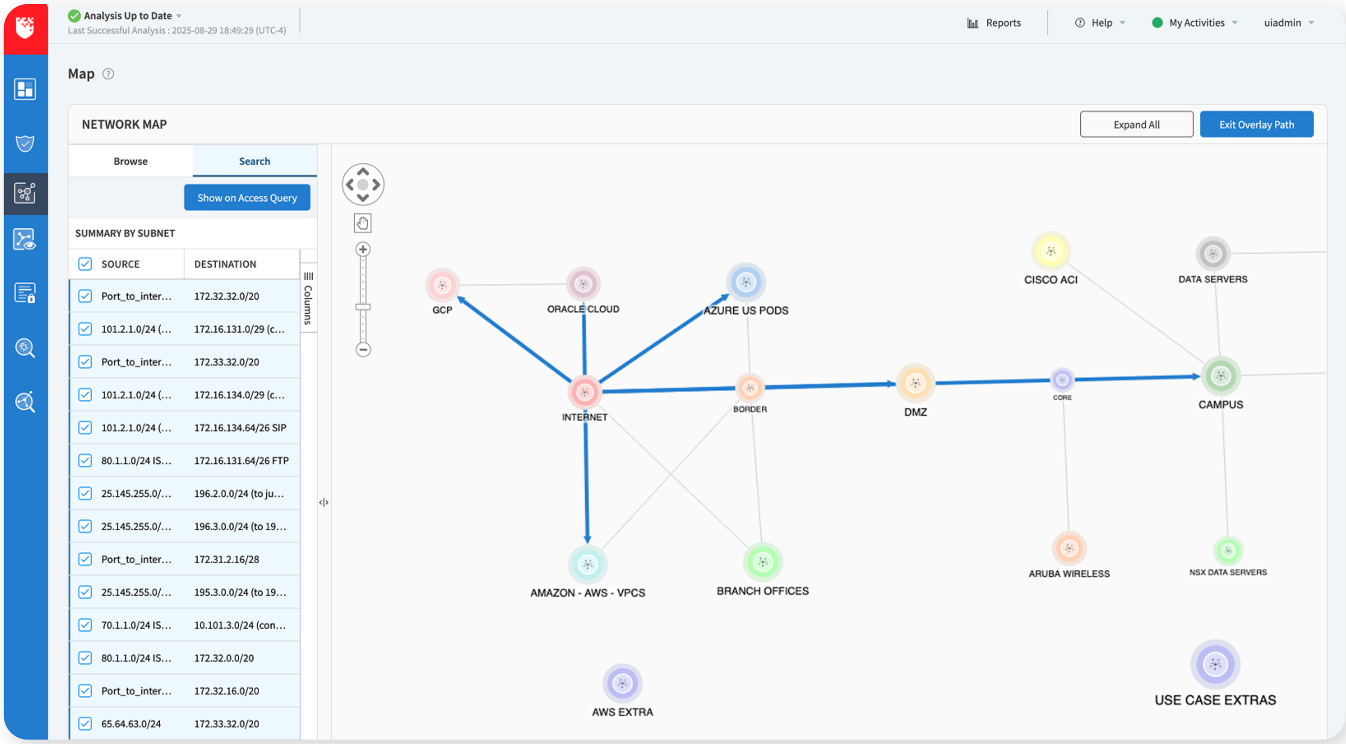
Manually tracing every possible access point and path in today's hybrid environments is impossible. RedSeal enables you to run queries against your living digital twin to visualize exposures and access vectors in just a few clicks.

What can you do with RedSeal?

- Identify and visualize all potential traffic flows and open threat vectors between sources and destinations
- Visualize access and threat vectors between hybrid environments: cloud, SDN, and on-premises
- Reveal exfiltration paths that attackers could exploit
- Visualize access based on L7 App ID tags from next-gen firewalls (NGFWs)
- Calculate Network Address Translation (NAT) mappings to validate how addresses are translated and secured

The RedSeal Advantage

- ✓ Identify all access paths quickly, whether traffic is present or not
- ✓ Improve productivity by running automated queries across all fabrics at once
- ✓ Speed time to insight and remediation with clear, visual evidence of exposures



Analysis Up to Date

Last Successful Analysis : 2025-08-29 18:49:29 (UTC-4)

SUMMARY BY SUBNET

☑	SOURCE	DESTINATION
☑	Port_to_inter…	172.32.32.0/20
☑	101.2.1.0/24 (…	172.16.131.0/29 (c…
☑	Port_to_inter…	172.33.32.0/20
☑	101.2.1.0/24 (…	172.16.134.0/29 (c…
☑	101.2.1.0/24 (…	172.16.134.64/26 SIP
☑	80.1.1.0/24 IS…	172.16.131.64/26 FTP
☑	25.145.255.0/…	196.2.0.0/24 (to ju…
☑	25.145.255.0/…	196.3.0.0/24 (to 19…
☑	Port_to_inter…	172.31.2.16/28
☑	25.145.255.0/…	195.3.0.0/24 (to 19…
☑	70.1.1.0/24 IS…	10.101.3.0/24 (con…
☑	80.1.1.0/24 IS…	172.32.0.0/20
☑	Port_to_inter…	172.32.16.0/20
☑	65.64.63.0/24	172.33.32.0/20

See how assets are connected and the associated risks.

Detailed Path Queries

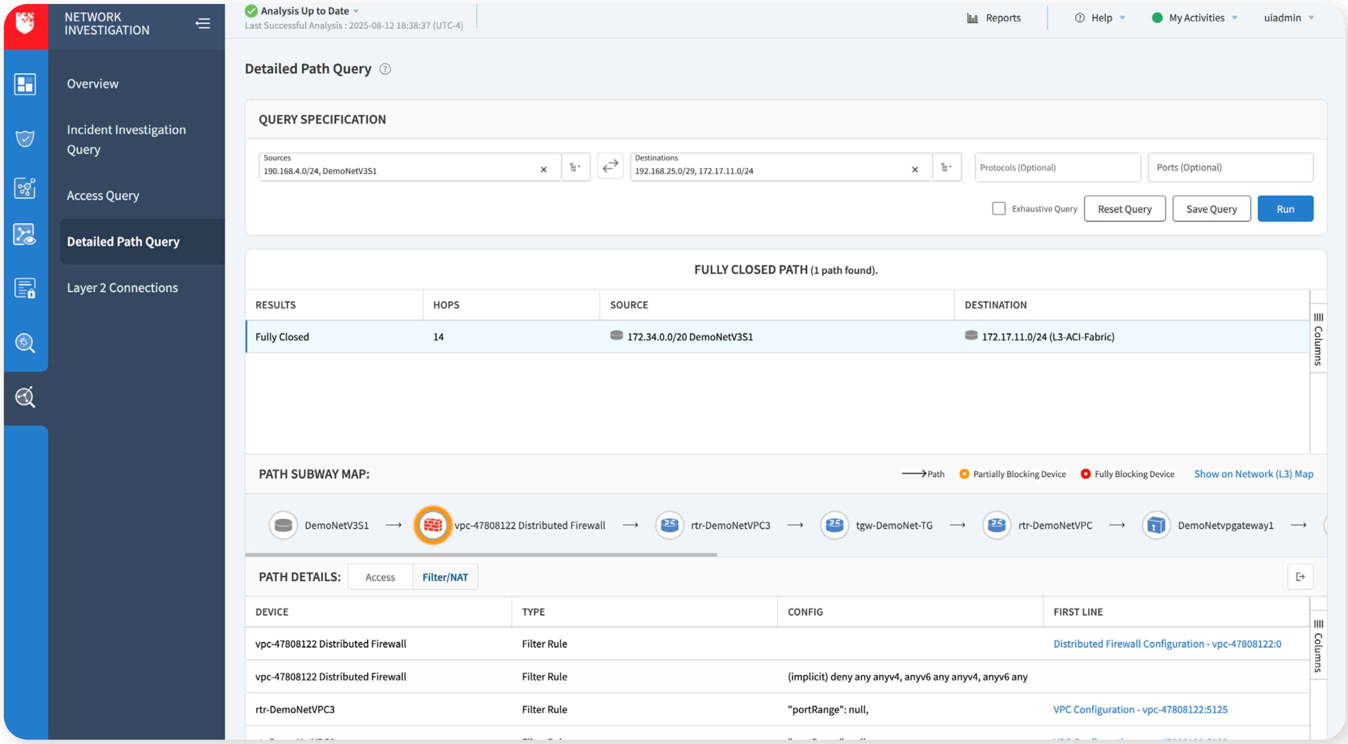
Connectivity in complex hybrid environments isn't linear — and neither are attacks. RedSeal provides hop-by-hop visibility into every possible path, revealing not only where you can get from A to B, but also every step in between.

What can you do with RedSeal?

- Get a hop-by-hop mapping of access from source(s) to destination(s)
- Identify network access paths that circumvent firewalls
- Identify network access paths to/from on-premises network(s) to cloud and/or software defined network(s)
- See all active and inactive access control list (ACL)/Filter rules
- Include virtual IP and IPv6 addresses in queries
- Troubleshoot network access if traffic flow is not working as expected in production environment

The RedSeal Advantage

- ✓ Reduce risk by uncovering connections that expose critical assets
- ✓ Expand your incident containment options by visualizing every possible route to or from a compromised asset
- ✓ Strengthen security proactively by running queries whenever environments change



Analysis Up to Date

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

Detailed Path Query

QUERY SPECIFICATION

Sources: 190.168.4.0/24, DemoNetV3S1

Destinations: 192.168.25.0/29, 172.17.11.0/24

Protocols (Optional)

Ports (Optional)

FULLY CLOSED PATH (1 path found).

RESULTS	HOPS	SOURCE	DESTINATION
Fully Closed	14	172.34.0.0/20 DemoNetV3S1	172.17.11.0/24 (L3-ACI-Fabric)

PATH SUBWAY MAP:

DemoNetV3S1 → vpc-47808122 Distributed Firewall → rtr-DemoNetVPC3 → tgw-DemoNet-TG → rtr-DemoNetVPC → DemoNetvpgateway1 →

PATH DETAILS:

DEVICE	TYPE	CONFIG	FIRST LINE
vpc-47808122 Distributed Firewall	Filter Rule		Distributed Firewall Configuration - vpc-47808122:0
vpc-47808122 Distributed Firewall	Filter Rule	(implicit) deny any anyv4, anyv6 any anyv4, anyv6 any	
rtr-DemoNetVPC3	Filter Rule	"portRange": null,	VPC Configuration - vpc-47808122:5125

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

Virtual Penetration Testing

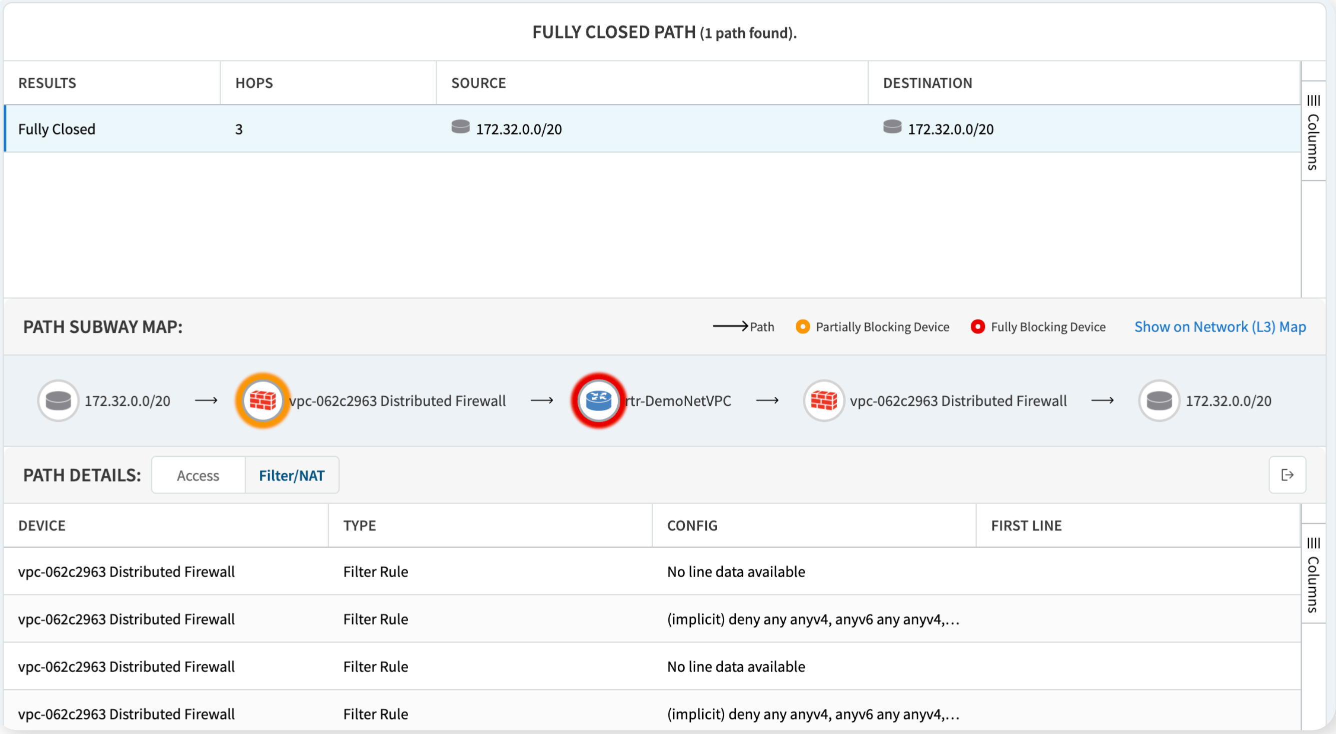
Unlike traditional penetration testing, which samples a subset of the network, RedSeal evaluates every possible way in, out, and through your entire environment. Think of it as continuous, passive red teaming — without the disruption or risk of a breach.

What can you do with RedSeal?

- Simulate cyberattacks against your digital twin
- Reveal vulnerabilities that are actually exploitable in your environment
- Identify all possible attack paths from untrusted network space
- Simulate "what-if" scenarios and zero-day vulnerabilities to better understand impacts to security or policy
- Generate prioritized reports for patching to minimize risk and exploitation impact

The RedSeal Advantage

- ✓ Reduce likelihood of a successful breach by closing exploitable paths
- ✓ Minimize the impact of a breach that does occur
- ✓ Proactively improve your security posture as new threats emerge



FULLY CLOSED PATH (1 path found).

RESULTS	HOPS	SOURCE	DESTINATION
Fully Closed	3	172.32.0.0/20	172.32.0.0/20

PATH SUBWAY MAP: ⟶ Path ● Partially Blocking Device ● Fully Blocking Device Show on Network (L3) Map

172.32.0.0/20 ⟶ vpc-062c2963 Distributed Firewall ⟶ rtr-DemoNetVPC ⟶ vpc-062c2963 Distributed Firewall ⟶ 172.32.0.0/20

PATH DETAILS: Access Filter/NAT

DEVICE	TYPE	CONFIG	FIRST LINE
vpc-062c2963 Distributed Firewall	Filter Rule	No line data available	
vpc-062c2963 Distributed Firewall	Filter Rule	(implicit) deny any anyv4, anyv6 any anyv4,...	
vpc-062c2963 Distributed Firewall	Filter Rule	No line data available	
vpc-062c2963 Distributed Firewall	Filter Rule	(implicit) deny any anyv4, anyv6 any anyv4,...	

Think like an attacker and find every possible way to reach critical assets.

Zero Trust Network Access

Zero Trust depends on complete knowledge of your environment. Identity is essential, but without visibility into **where and how assets connect**, Zero Trust cannot be fully enforced. RedSeal adds the missing hybrid environment context to help organizations advance Zero Trust maturity.

The RedSeal Advantage

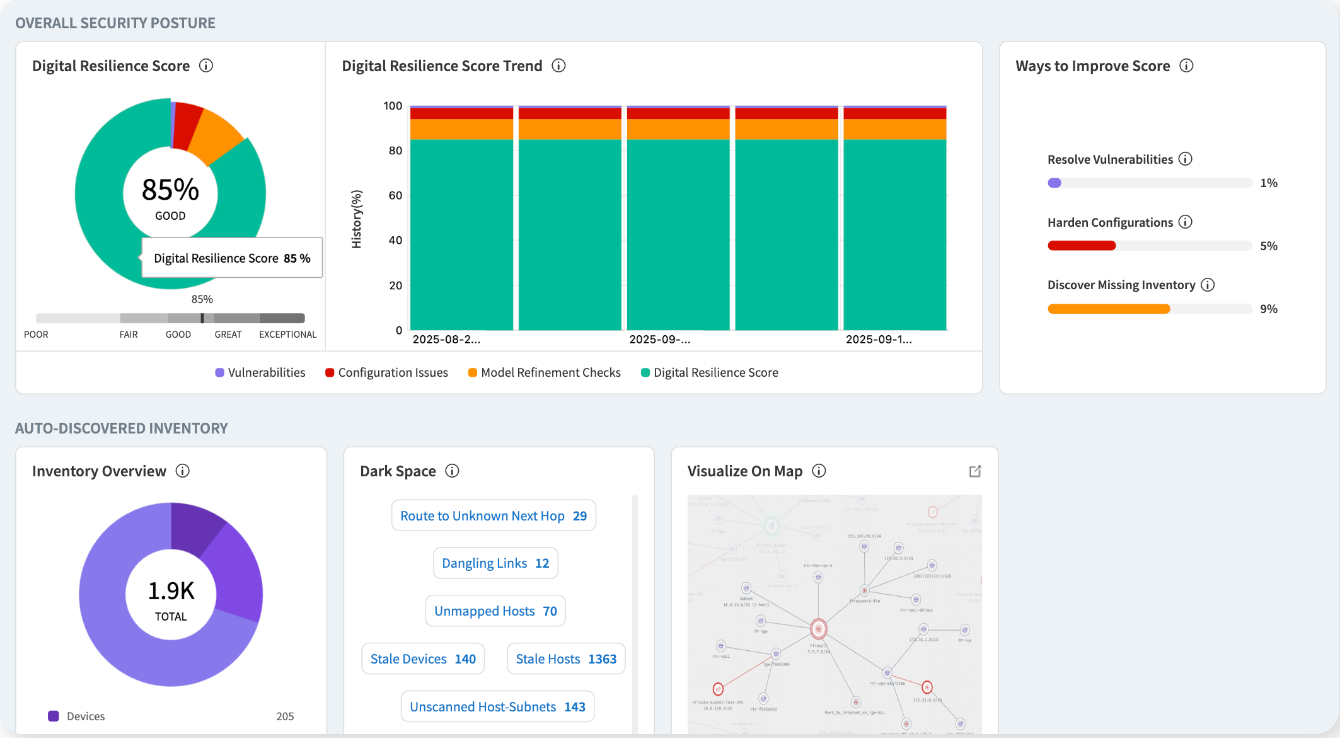
✓ **Enhance your overall security posture with environment-wide context**

✓ **Limit your potential attack surface by enforcing segmentation at scale**

✓ **Support continuous verification of Zero Trust principles**

What can you do with RedSeal?

- Visualize your entire inventory of IT (on-prem, cloud, remote workers), OT, and IoT assets
- Map all possible traffic paths to understand data flows and detect misconfigurations
- Define and enforce policies for macro-segmentation to prevent unauthorized access between different parts of the network (e.g., separating IT and OT systems)
- Pinpoint where micro-segmentation can be applied most effectively
- Manage and enforce detailed micro segmentation policies
- Create more effective software-defined networking (SDN) policies with a detailed understanding of the network structure and potential vulnerabilities



Strengthen the network and environment pillar of your zero trust framework.

Risk Prioritization

Rank all issues and vulnerabilities according to true business impact

Risk Prioritization with Risk Radius™

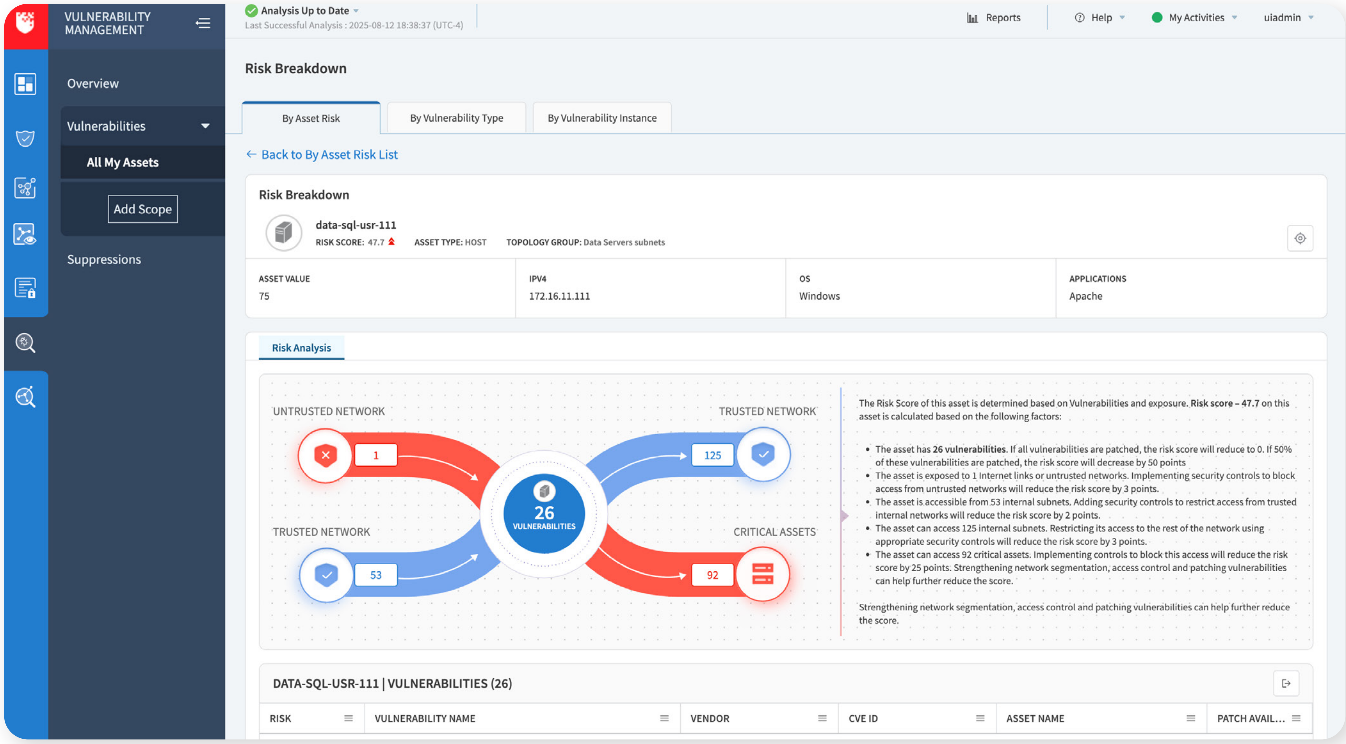
Not all risks are equal. Security teams face endless vulnerability lists that lack context, leaving them to guess what to fix first. RedSeal changes that with **Risk Radius™** — a unique calculation that ranks exposures by both **exploitability and business impact**. With AI-enabled context, RedSeal surfaces what is truly dangerous so teams can focus on the issues that actually reduce the most risk.

What can you do with RedSeal?

- Calculate a **Risk Radius™** to identify exposures that are both reachable and consequential
- Correlate vulnerability scanner data with asset value and connectivity to separate real threats from noise
- Pinpoint the blast radius of unpatched vulnerabilities for faster containment planning
- Consolidate scan data from multiple tools into one trusted source
- Push coverage and prioritization insights back into scanners like Tenable and Rapid7

The RedSeal Advantage

- ✓ Go beyond raw CVSS scores with **Risk Radius™**, combining exploitability and business impact
- ✓ Deliver AI-enabled context to focus teams on exposures that actually reduce risk
- ✓ Provide clear blast-radius analysis to support faster containment and remediation



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

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...

Visualize risk with scoring that combines exposure, access, and business impact.

Vulnerability Management

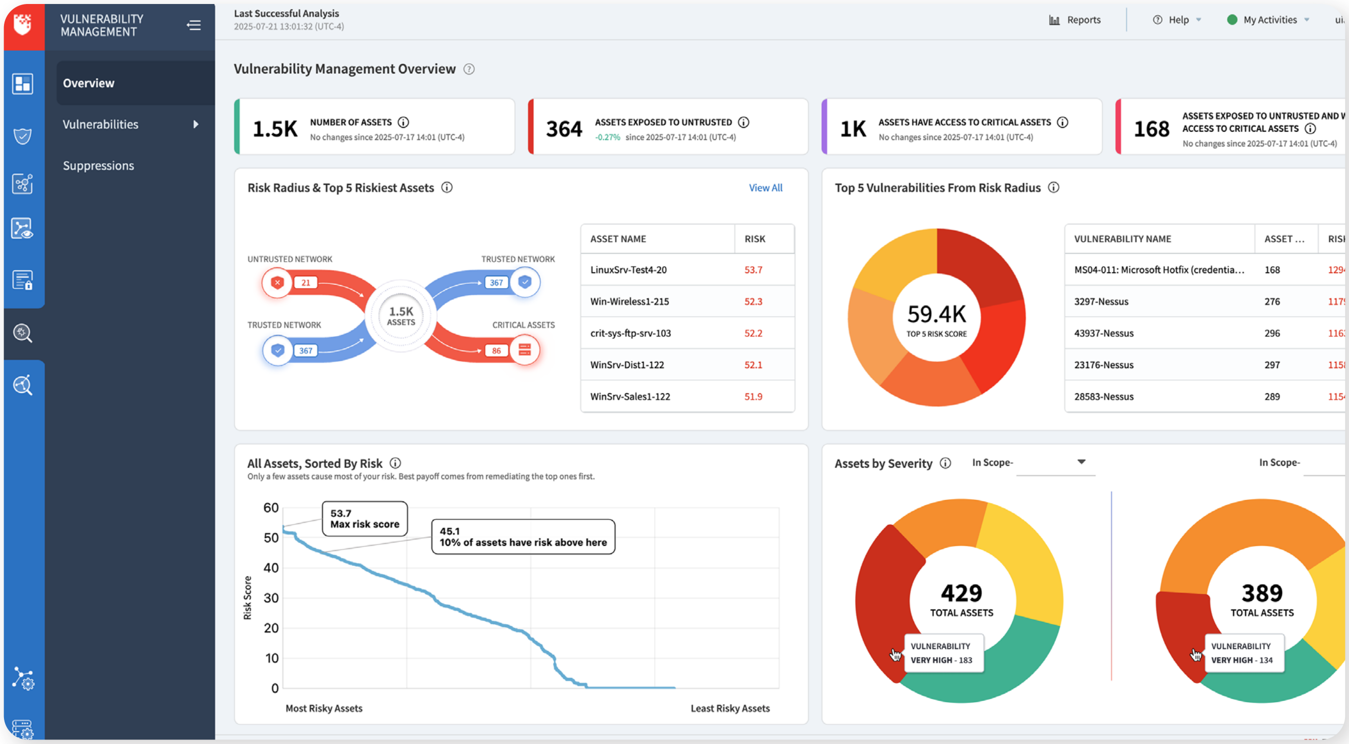
Traditional vulnerability scanners generate overwhelming lists, often missing assets and lacking context about what truly matters. RedSeal strengthens vulnerability management by correlating scanner data with hybrid environment context, ensuring complete coverage and smarter prioritization.

What can you do with RedSeal?

- Report network assets and subnets missed by vulnerability scanners
- Visualize all reachable assets for optimal scanner placement
- Pinpoint network devices and rules preventing scanner access
- Assess vulnerability risk using additional network and business context for more accurate prioritization
- Identify precise access paths and assets for containment of unpatched vulnerabilities
- Consolidate vulnerability data from multiple scanners and vendors
- Push scan coverage analysis to third-party solutions like Rapid7 and Tenable

The RedSeal Advantage

- ✓ Strengthen your security posture by ensuring proper scanner placement and full scan coverage
- ✓ Accelerate risk reduction by focusing teams on fixing the most business-critical vulnerabilities first
- ✓ Improve productivity by unifying results into one clear, actionable picture



Last Successful Analysis
2025-07-21 13:01:32 (UTC-4)

Vulnerability Management Overview

1.5K NUMBER OF ASSETS
No changes since 2025-07-17 14:01 (UTC-4)

364 ASSETS EXPOSED TO UNTRUSTED
-0.27% since 2025-07-17 14:01 (UTC-4)

1K ASSETS HAVE ACCESS TO CRITICAL ASSETS
No changes since 2025-07-17 14:01 (UTC-4)

168 ASSETS EXPOSED TO UNTRUSTED AND W ACCESS TO CRITICAL ASSETS
No changes since 2025-07-17 14:01 (UTC-4)

Risk Radius & Top 5 Riskiest Assets

ASSET NAME	RISK
LinuxSrv-Test4-20	53.7
Win-Wireless1-215	52.3
crit-sys-ftp-srv-103	52.2
WinSrv-Dist1-122	52.1
WinSrv-Sales1-122	51.9

Top 5 Vulnerabilities From Risk Radius

VULNERABILITY NAME	ASSET ...	RISI
MS04-011: Microsoft Hotfix (credentia...	168	129
3297-Nessus	276	117
43937-Nessus	296	116
23176-Nessus	297	115
28583-Nessus	289	115

All Assets, Sorted By Risk
Only a few assets cause most of your risk. Best payoff comes from remediating the top ones first.

Assets by Severity

Put vulnerability details at your fingertips for faster decision making.

Incident Investigation

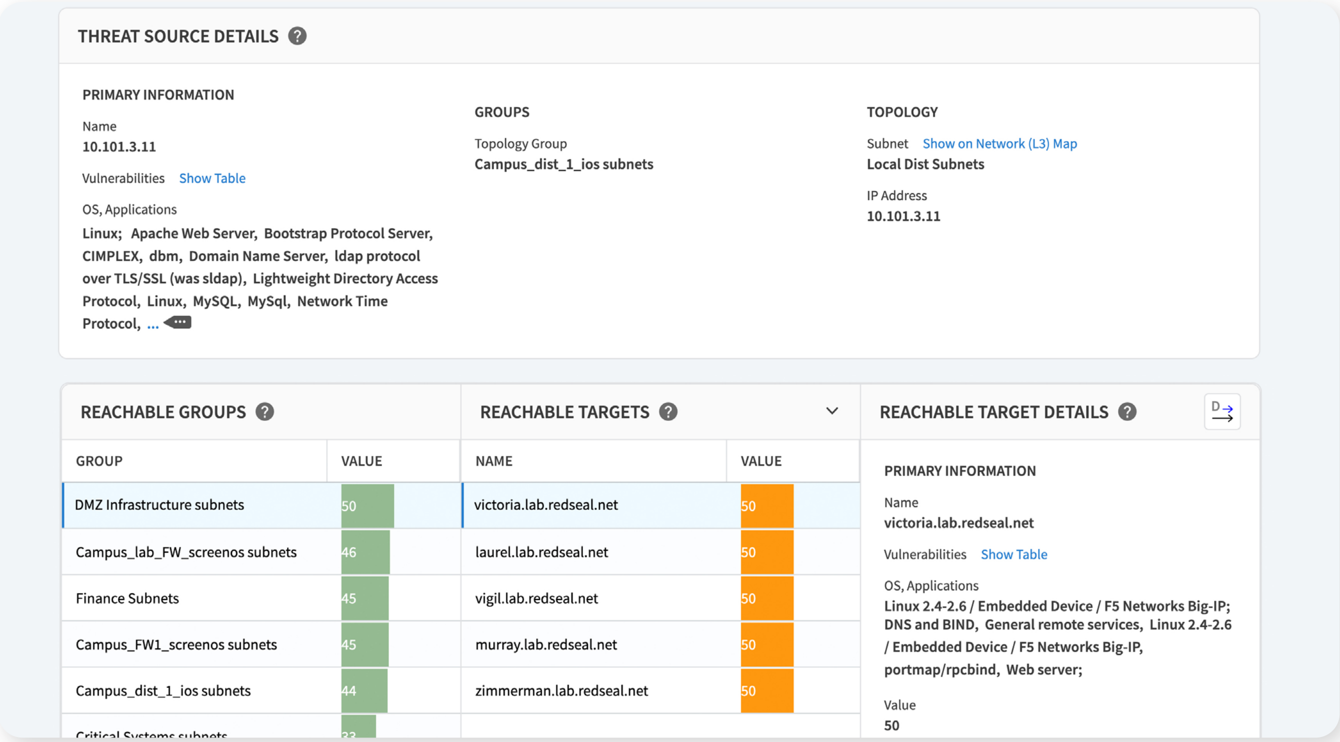
When an incident occurs, every second counts. RedSeal accelerates investigations by providing detailed context about compromised assets, their connections, and the potential blast radius — helping teams contain threats quickly and effectively.

What can you do with RedSeal?

- Automatically validate and prioritize incidents with AI-enabled context
- Get detailed information about a potentially compromised asset, including its precise logical and physical location
- Get detailed information about assets reachable from internal and external threat sources, including the blast radius of any given asse
- Visualize the detailed paths that lead from the threat source to any reachable assets to understand containment options
- Pinpoint the exact configuration enabling unwanted access, even which line to change in a firewall config file
- Aggregate data from disparate SIEM systems to enable a more complete operational picture

The RedSeal Advantage

- ✓ Focus incident response teams on efforts that will have the greatest business impact
- ✓ Accelerate incident response and mean time to resolution (MTTR) with environment and business context
- ✓ Minimize the extent of damage and block similar incidents in the future



THREAT SOURCE DETAILS ?

PRIMARY INFORMATION

Name
10.101.3.11

Vulnerabilities Show Table

OS, Applications
Linux; Apache Web Server, Bootstrap Protocol Server, CIMPLEX, dbm, Domain Name Server, ldap protocol over TLS/SSL (was sldap), Lightweight Directory Access Protocol, Linux, MySQL, MySql, Network Time Protocol, ...

GROUPS

Topology Group
Campus_dist_1_ios subnets

TOPOLOGY

Subnet Show on Network (L3) Map
Local Dist Subnets

IP Address
10.101.3.11

REACHABLE GROUPS ?

GROUP	VALUE
DMZ Infrastructure subnets	50
Campus_lab_FW_screenos subnets	46
Finance Subnets	45
Campus_FW1_screenos subnets	45
Campus_dist_1_ios subnets	44
Critical Systems subnets	33

REACHABLE TARGETS ?

NAME	VALUE
victoria.lab.redseal.net	50
laurel.lab.redseal.net	50
vigil.lab.redseal.net	50
murray.lab.redseal.net	50
zimmerman.lab.redseal.net	50

REACHABLE TARGET DETAILS ?

PRIMARY INFORMATION

Name
victoria.lab.redseal.net

Vulnerabilities Show Table

OS, Applications
Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP; DNS and BIND, General remote services, Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP, portmap/rpcbind, Web server;

Value
50

Focus incident response teams on protecting the highest-value assets first.

Continuous Compliance

Continuously validate policies, configurations, and controls across your hybrid environment — helping you get to compliance and stay there.

Device Configuration Management

Misconfigurations are one of the most common causes of compliance failures. RedSeal continuously validates device configurations against internal policies and industry standards, helping you identify issues early and prevent violations before they impact audits or operations.

By monitoring configurations across your hybrid environment and detecting drift as it occurs, RedSeal helps teams get to compliance faster — and stay there throughout the year.

What can you do with RedSeal?

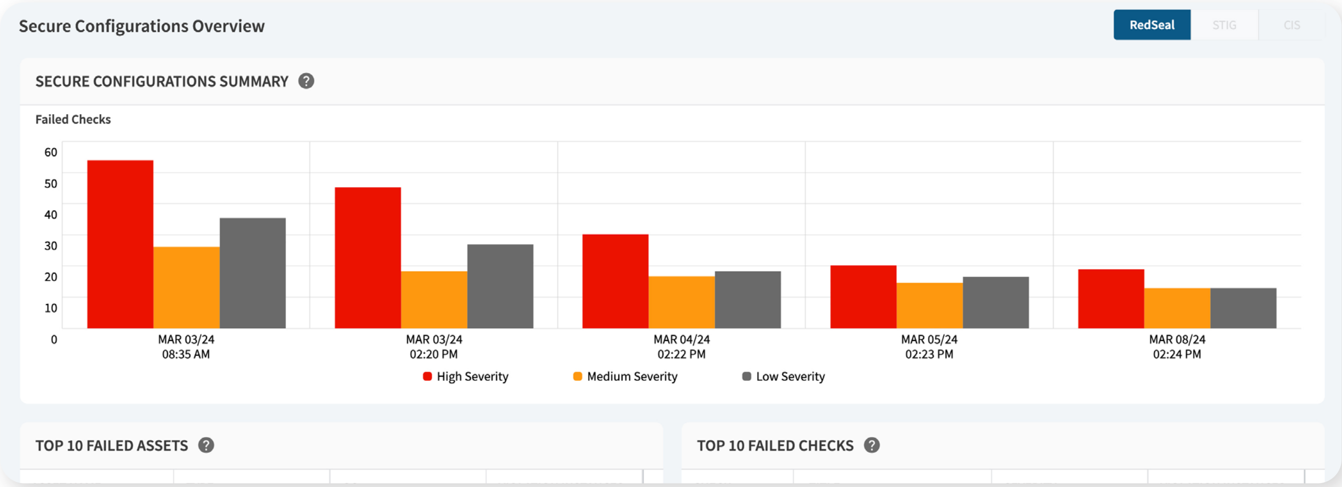
- Identify violations to any user-defined best practices
- Identify violations to industry security best practices (e.g., PCIDSS or HIPAA)
- Identify violations to CIS benchmarks
- Identify violations to DISA STIGs on L2 and L3 network devices
- Support and monitor key NIST controls
- Identify configurations causing hosts to be unreachable from some part of the network (overlapping subnets)
- Identify IP address reuse across network (colliding IPs)
- Identify duplicate VLANs and review for intended or unintended configuration
- View differences between device configurations collected at different points in time

The RedSeal Advantage

✓ **Reduce risk by identifying secure configuration issues quickly**

✓ **Improve productivity by giving compliance teams direct access to findings**

✓ **Reduce audit cycle time by validating configurations ahead of assessments**



Get more than 160 built-in secure configuration checks beyond the STIG/CIS/NIST checks.

Segmentation Validation

Effective segmentation is essential for limiting access and protecting sensitive data. RedSeal continuously validates segmentation and access policies across your hybrid environment to ensure they remain aligned with internal standards and regulatory requirements — helping teams get to compliance and stay there.

What can you do with RedSeal?

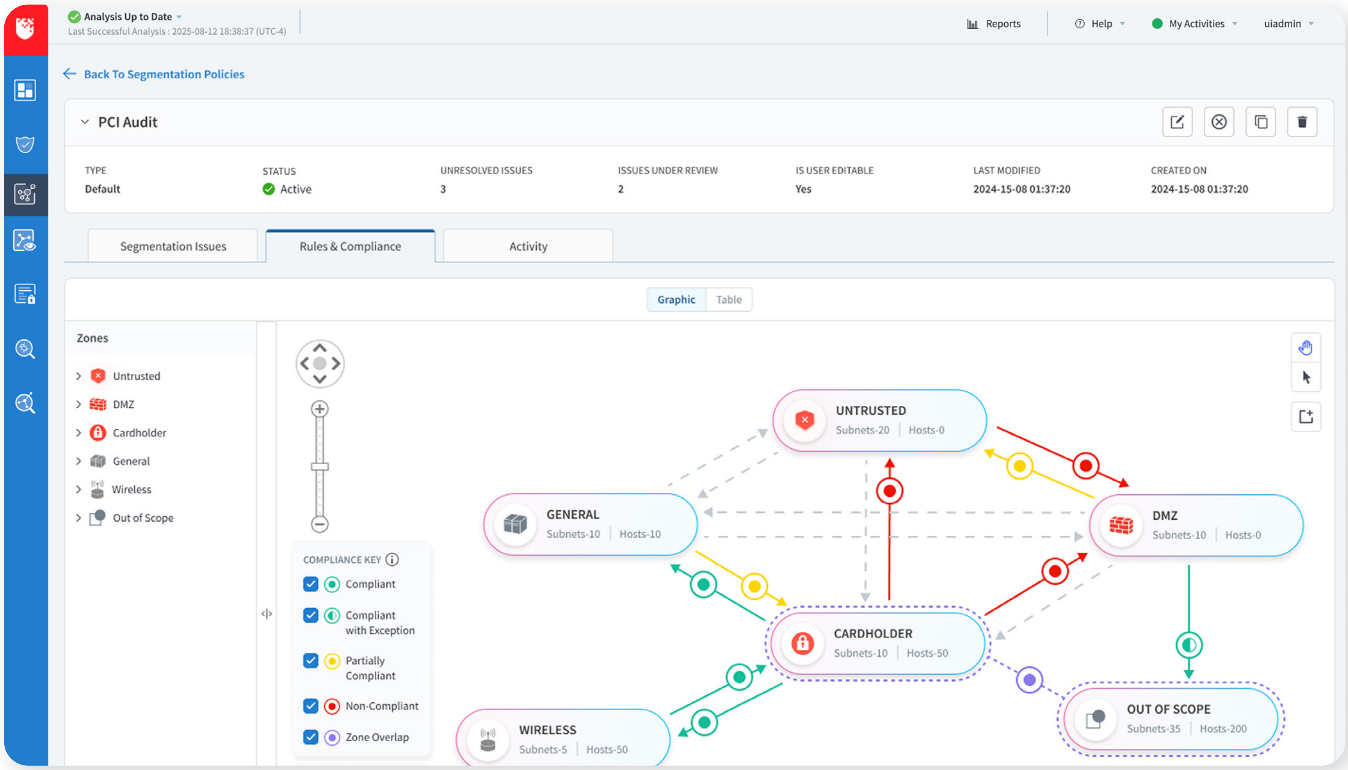
- Validate "all access forbidden" and "approved access only" segmentation policies across IT (on-prem, cloud, remote workers), OT, and IoT
- Validate pre-defined segmentation policy sets required by laws or industry standards, such as GDPR, NIST, PCI DSS, HIPAA, and CMMC
- Define custom segmentation policies and validate them against internal policies, such as IT/IoT/OT and IPv4/IPv6
- Automate vendor segmentation best practices, such as Cisco SAFE
- Send alerts to stakeholders when configurations are out of compliance with policies
- Produce a policy compliance report for all network segmentations

The RedSeal Advantage

✓ Reduce your attack surface with effective segmentation

✓ Save time and effort by automating segmentation validation

✓ Maintain regulatory compliance by preventing policy drift



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

← Back To Segmentation Policies

PCI Audit

TYPE	STATUS	UNRESOLVED ISSUES	ISSUES UNDER REVIEW	IS USER EDITABLE	LAST MODIFIED	CREATED ON
Default	✓ Active	3	2	Yes	2024-15-08 01:37:20	2024-15-08 01:37:20

Zones
- Untrusted
- DMZ
- Cardholder
- General
- Wireless
- Out of Scope

COMPLIANCE KEY
- ☑ Compliant
- ☑ Compliant with Exception
- ☑ Partially Compliant
- ☑ Non-Compliant
- ☑ Zone Overlap

Show all access vectors in a segmentation policy to avoid policy drift and prioritize remediation.

Firewall Rule Management

Firewalls play a central role in enforcing access and maintaining compliance. But without ongoing rule hygiene, outdated or overly permissive rules can introduce unnecessary risk and lead to audit findings. RedSeal continuously analyzes firewall rules to identify issues early and help teams keep policies aligned with security and compliance requirements.

What can you do with RedSeal?

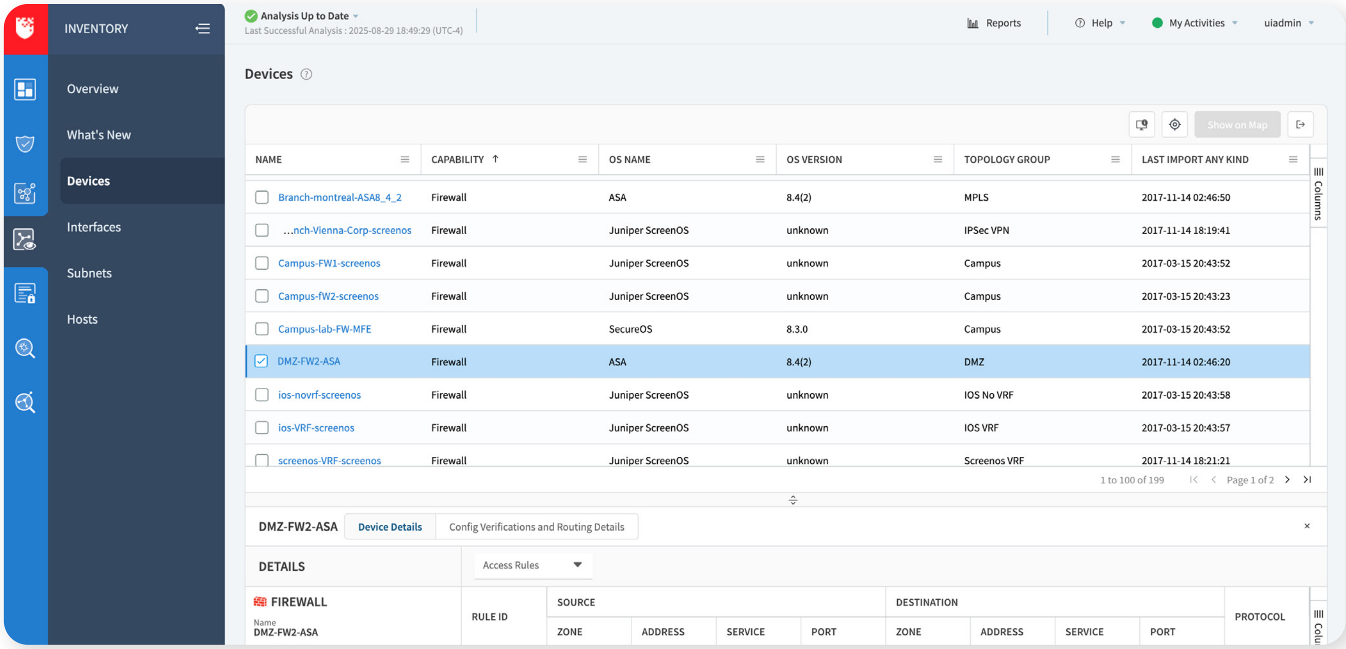
- Report how many packets were processed by individual access rules during a specified period of time
- Identify IP any-any rules
- Identify redundant rules
- Identify disabled rules
- Identify expired rules
- Identify time-constrained rules
- Identify empty objects
- Identify unlogged rules
- Identify rules from unknown sources
- Identify rules from unknown destinations

The RedSeal Advantage

✓ Lower the risk of a cyberattack or compliance violation due to poor rule hygiene

✓ Help firewall teams find and fix risky rules faster

✓ Make your firewalls more efficient and secure by updating outdated and conflicting rules



Analysis Up to Date

Last Successful Analysis : 2025-08-29 18:49:29 (UTC-4)

Devices

	NAME	CAPABILITY ↑	OS NAME	OS VERSION	TOPOLOGY GROUP	LAST IMPORT ANY KIND
□	Branch-montreal-ASA8_4_2	Firewall	ASA	8.4(2)	MPLS	2017-11-14 02:46:50
□	…nch-Vienna-Corp-screenos	Firewall	Juniper ScreenOS	unknown	IPSec VPN	2017-11-14 18:19:41
□	Campus-FW1-screenos	Firewall	Juniper ScreenOS	unknown	Campus	2017-03-15 20:43:52
□	Campus-fW2-screenos	Firewall	Juniper ScreenOS	unknown	Campus	2017-03-15 20:43:23
□	Campus-lab-FW-MFE	Firewall	SecureOS	8.3.0	Campus	2017-03-15 20:43:52
☑	DMZ-FW2-ASA	Firewall	ASA	8.4(2)	DMZ	2017-11-14 02:46:20
□	ios-novrf-screenos	Firewall	Juniper ScreenOS	unknown	IOS No VRF	2017-03-15 20:43:58
□	ios-VRF-screenos	Firewall	Juniper ScreenOS	unknown	IOS VRF	2017-03-15 20:43:57
□	screenos-VRF-screenos	Firewall	Juniper ScreenOS	unknown	Screenos VRF	2017-11-14 18:21:21

1 to 100 of 199 Page 1 of 2

DMZ-FW2-ASA

DETAILS

FIREWALL

Name
DMZ-FW2-ASA

RULE ID	SOURCE				DESTINATION				PROTOCOL
	ZONE	ADDRESS	SERVICE	PORT	ZONE	ADDRESS	SERVICE	PORT	

Quickly identify firewall rules that are candidates for removal or modification.

Change Management

Network changes can introduce unintended access or compliance issues if not reviewed carefully. RedSeal lets teams model proposed changes before they are implemented to see exactly how access, segmentation, and policy alignment will be affected. After changes go live, RedSeal verifies that they were implemented correctly and remain consistent with approved policies, reducing rework and preventing drift.

What can you do with RedSeal?

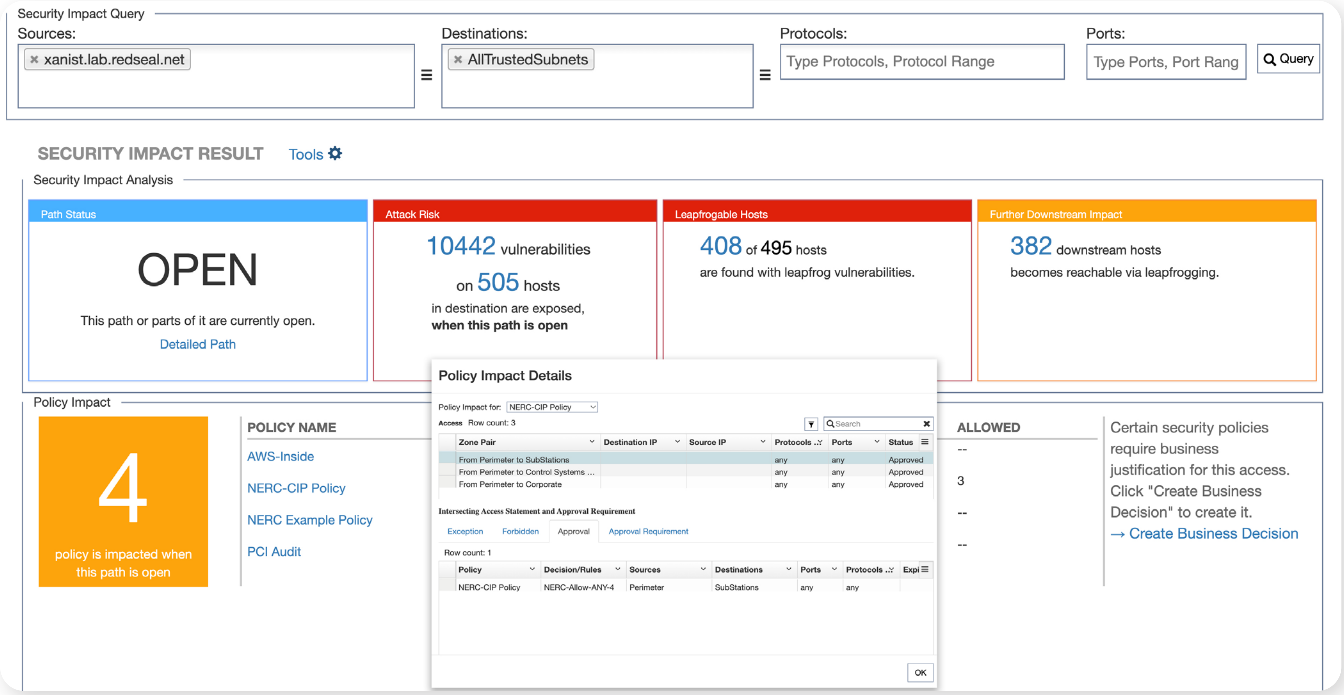
- Model proposed changes before they are implemented
- Predict the introduction of exposures and policy violations, including vulnerabilities, hosts reachable, downstream access, and potential threats
- Get the status of existing and proposed paths between hosts, endpoints, and/or subnets, discovering if certain ports and protocols are open and in use
- After changes are implemented, verify they are properly documented and report on incorrect implementations
- Integrate with SOAR platforms, such as ServiceNow, to help reviewers verify a change request is even needed and to help auditors quickly confirm implementations against authorized tickets

The RedSeal Advantage

✓ Save time by integrating change validation into existing workflows

✓ Accelerate maintenance windows and reduce business disruption

✓ Ensure every change remains aligned with policy and compliance requirements



Security Impact Query

Sources: × xanist.lab.redseal.net

Destinations: × AllTrustedSubnets

Protocols: Type Protocols, Protocol Range

Ports: Type Ports, Port Rang

SECURITY IMPACT RESULT

Security Impact Analysis

Path Status: OPEN. This path or parts of it are currently open. Detailed Path

Attack Risk: 10442 vulnerabilities on 505 hosts in destination are exposed, **when this path is open**

Leapfrogable Hosts: 408 of 495 hosts are found with leapfrog vulnerabilities.

Further Downstream Impact: 382 downstream hosts becomes reachable via leapfrogging.

Policy Impact

4 policy is impacted when this path is open

POLICY NAME	ALLOWED
AWS-Inside	--
NERC-CIP Policy	3
NERC Example Policy	--
PCI Audit	--

Certain security policies require business justification for this access. Click "Create Business Decision" to create it.

→ Create Business Decision

Policy Impact Details

Policy Impact for: NERC-CIP Policy

Access Row count: 3

Zone Pair	Destination IP	Source IP	Protocols	Ports	Status
From Perimeter to SubStations			any	any	Approved
From Perimeter to Control Systems …			any	any	Approved
From Perimeter to Corporate			any	any	Approved

Intersecting Access Statement and Approval Requirement

Row count: 1

Policy	Decision/Rules	Sources	Destinations	Ports	Protocols	Expi
NERC-CIP Policy	NERC-Allow-ANY-4	Perimeter	SubStations	any	any	

Reduce unforeseen complications when making changes in your live environment.

Reporting

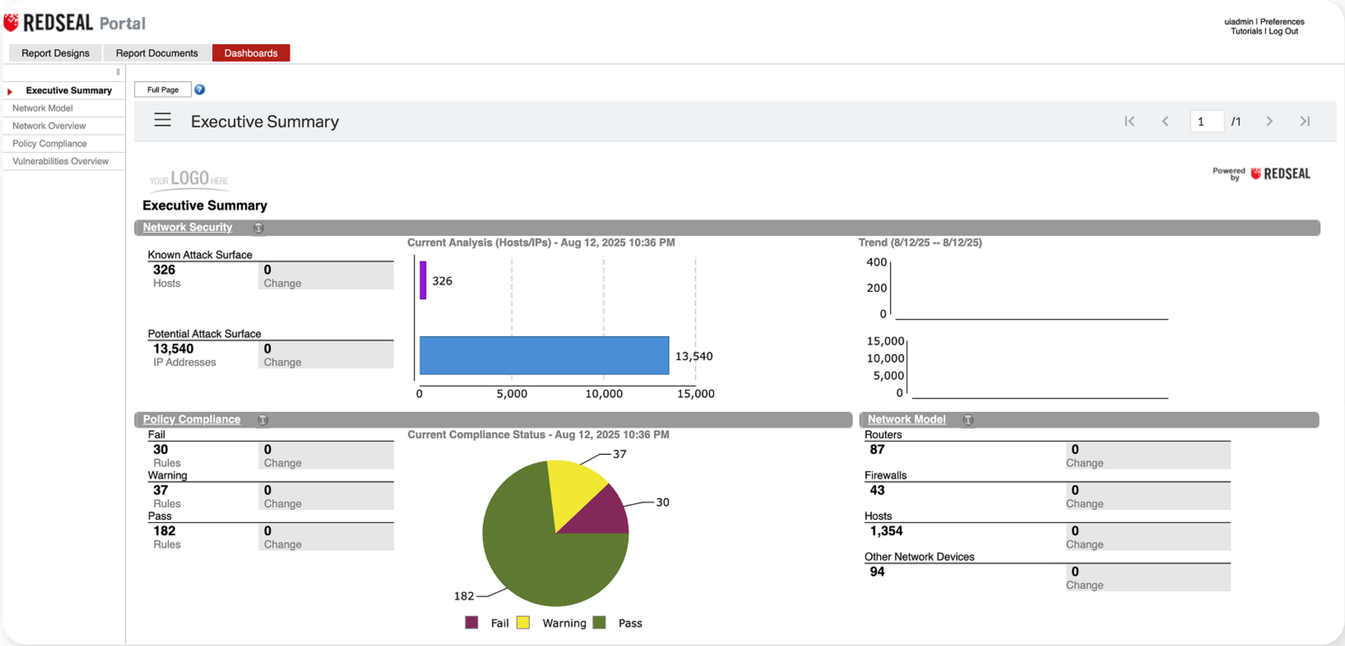
At RedSeal, the goal is to help teams act — but reports play a critical role in proving compliance, supporting audits, and driving collaboration across security, network, and compliance teams. RedSeal makes it easy to generate consistent, defensible documentation that reflects your true compliance posture at any point in time.

What can you do with RedSeal?

- Generate predefined and custom reports
- Generate an executive summary report showing a high-level view of overall security
- Generate a network overview report focusing on attack surfaces and containment efforts
- Generate a network segmentation policy compliance report
- Generate a vulnerability overview report providing detailed vulnerability metrics, including calculation of downstream risk
- Generate a configuration management report on access rule cleanup and best practice checks and violations
- Schedule reports with email to appropriate parties
- Export STIG results to XCCDF for use with STIG Viewer

The RedSeal Advantage

- ✓ Document compliance and security posture consistently
- ✓ Share audit-ready evidence with internal and external stakeholders
- ✓ Demonstrate continuous improvement over time



Executive Summary

Network Security

Known Attack Surface	
326 Hosts	0 Change
Potential Attack Surface	
13,540 IP Addresses	0 Change

Policy Compliance

Fail	
30 Rules	0 Change
Warning	
37 Rules	0 Change
Pass	
182 Rules	0 Change

Network Model

Routers	
87	0 Change
Firewalls	
43	0 Change
Hosts	
1,354	0 Change
Other Network Devices	
94	0 Change

Produce reports that will improve collaboration among security, network, and compliance teams.

Digital Resilience Scoring

Organizations invest heavily in people, processes, and technology to strengthen security and compliance — but measuring progress can be difficult. RedSeal's Digital Resilience Score provides a clear, quantifiable way to track compliance maturity, control effectiveness, and overall environment readiness over time.

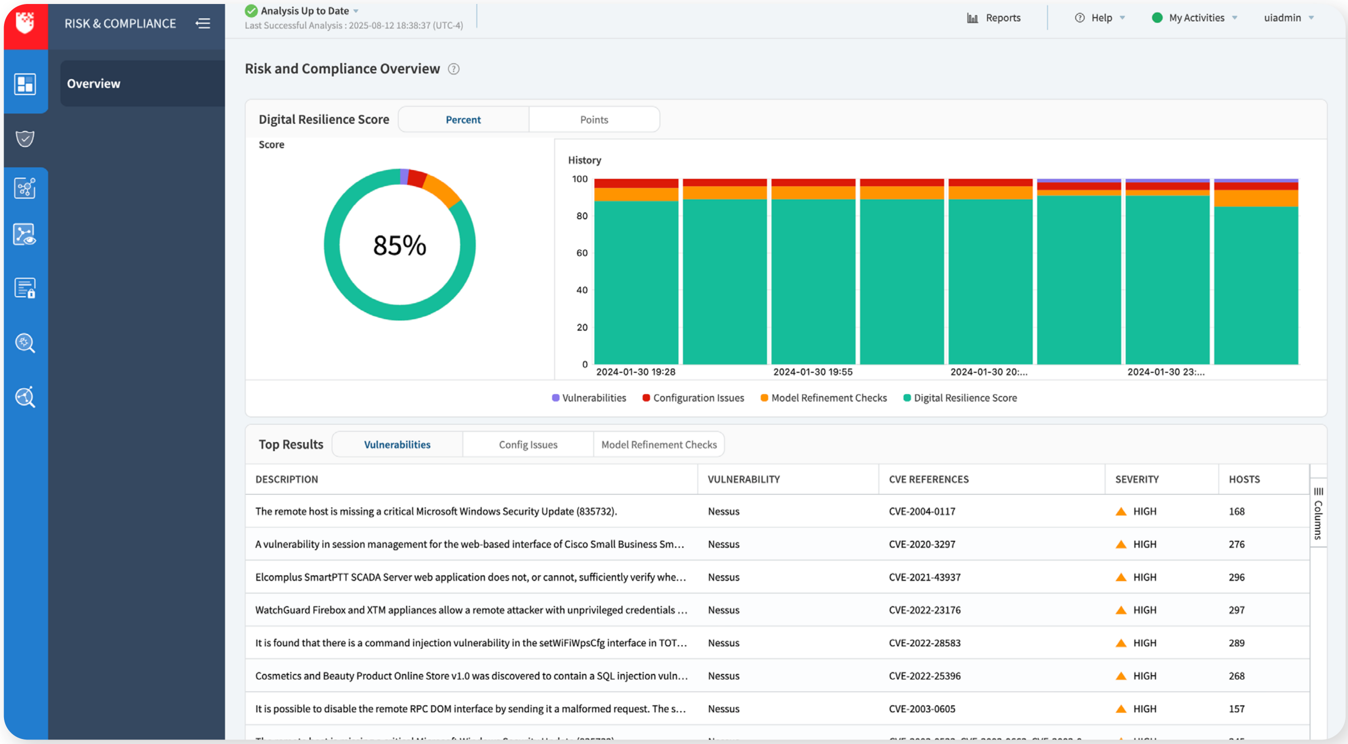
By using a consistent scoring model, teams can show measurable improvement, prioritize efforts, and communicate resilience progress with confidence.

What can you do with RedSeal?

- Measure your environment's digital resilience across vulnerabilities, compliance, and infrastructure completeness
- Make the concept of digital resilience understandable and actionable by using a simple scoring system based on 100%
- Show teams where to focus their efforts to improve resilience faster (patching vulnerabilities vs. completing the inventory vs. hardening network devices)
- Monitor your digital resilience score over time to achieve and maintain an "exceptional" rating

The RedSeal Advantage

- ✓ Report on your overall environment security posture with confidence
- ✓ Track measurable improvement in resilience over time
- ✓ Provide a board-level metric for cyber and compliance readiness



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

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

Summary

Exposure management is a never-ending challenge, especially in complex and highly regulated environments. When done right, it provides a powerful source of truth about an organization's hybrid environment and the risks it faces.

RedSeal simplifies exposure management for cybersecurity and compliance teams that need to work smarter and faster together — whether responding to an incident or proactively strengthening defenses ahead of an audit.

Incorporating more than two decades of innovation and customer insight, the RedSeal platform delivers unmatched capabilities to **see, understand, and secure your entire environment**. With AI-enabled context and agentless integrations, RedSeal helps you assess real risks, prioritize what matters most, and measurably reduce risk while maximizing resilience — **so you truly know your hybrid environment better than any adversary**.

Get Started with RedSeal

Learn more about how RedSeal's extensive set of capabilities works seamlessly together to keep you focused on what's most important.

Request a demo today.

REDSEAL

Contact us today to learn more

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

About RedSeal. RedSeal, a pioneer in proactive exposure management and winner of the SC Award for Best CTEM Solution, helps organizations see, understand, and secure their hybrid digital environments—spanning IT, remote, OT, cloud, and IoT. By dynamically modeling the entire environment, RedSeal uncovers hidden assets, misconfigurations, and lateral attack paths; prioritizes exposures based on business-critical impact with Risk Radius™; and continuously validates compliance with internal policies and industry standards. Trusted by hundreds of Fortune 1000 companies and more than 75 U.S. government agencies, including all five branches of the U.S. military, RedSeal strengthens resilience, streamlines operations, and reduces business risk. Visit www.redseal.net to learn more.