RedSeal Expands Exposure Management Platform with Report Studio and Network Segmentation

New capabilities deliver board-ready reporting and expose configuration gaps and improper access paths to provide a more complete view of attack surface risk

MENLO PARK, CA, UNITED STATES, March 24, 2026 /EINPresswire.com/ -- RedSeal, a pioneer in AI powered exposure management for hybrid enterprise environments, today announced an expansion to the RedSeal platform with the introduction of RedSeal Report Studio and Network Segmentation capabilities. Together, these enhancements help security and network teams better understand, communicate, and reduce risk across complex enterprise and operational technology (OT) environments.

> “Security leaders need visibility into how exposures connect across their environment and the ability to explain risk to executives and boards. Report Studio and Network Segmentation deliver both.”
>
> *Joseph Ward, CTPO*

Security teams today face growing pressure to demonstrate measurable risk reduction, communicate clearly with executives and boards, and meet a widening set of compliance and regulatory requirements. At the same time, organizations must manage exposures that extend beyond traditional vulnerabilities, including configuration weaknesses and unintended network access paths.

RedSeal delivers exposure management through a proven, architecture-driven foundation powered by AI and Agentic capabilities, enabling organizations to move from insight to action with confidence. The latest release addresses security teams growing challenges, making it easier to understand exposure across the network and communicate that risk effectively to stakeholders.

“With these new capabilities, RedSeal is helping organizations see their true attack surface and clearly communicate and reduce that risk,” said Joseph Ward, Chief Technology and Product Officer at RedSeal. “Security leaders need visibility into how exposures connect across their environment and the ability to explain that risk to executives and boards. Report Studio and Network Segmentation deliver both.”

Report Studio: Flexible, Board-Ready Security Reporting

RedSeal Report Studio provides security and networking teams with a flexible, drag-and-drop reporting experience built directly into the RedSeal platform. The capability allows organizations to build customized reports without coding or reliance on consultants.

While many security teams rely on static, pre-built reports that fail to reflect the complexity of modern environments, Report Studio enables organizations to tailor reporting their architecture, operational priorities, and compliance frameworks.

Using an intuitive interface, teams can assemble reports with tables, charts, and heatmaps drawn from RedSeal's exposure model, network topology, vulnerability data, compliance checks (including CIS and STIG), and custom scopes.

Key capabilities include:
- Drag-and-drop report creation using pre-built query blocks and visualizations
- Support for vulnerability, exposure, topology, and compliance reporting
- Customizable reports for executives, analysts, auditors, and operational teams
- Built-in branding with corporate logos, labels, and terminology for board-ready deliverables
- Reduced dependence on manual report building or third-party services

By enabling teams to present exposure trends, segmentation posture, and remediation progress clearly, Report Studio helps organizations communicate risk reduction and operational progress across technical and executive audiences.

Network Segmentation: Visibility Beyond Vulnerabilities

While vulnerability scanners focus primarily on CVEs, many real-world exposures stem from misconfigurations, overly permissive access policies, and segmentation failures that create unintended pathways across the network.

RedSeal's new Network Segmentation capability extends exposure analysis beyond vulnerabilities to reveal these architectural risks.

Using RedSeal's network digital twin, security teams can analyze reachability across hybrid and cloud environments to identify configuration gaps and improper access paths that could allow attackers to move laterally toward critical assets.

With Network Segmentation, organizations can:
- Identify misconfigured network boundaries that create unintended attack paths
- Detect improper access between segments that violate least-privilege policies
- Understand how vulnerabilities combine with network access to create real exposure
- Prioritize remediation based on business impact rather than CVSS scores alone

- Continuously validate segmentation across hybrid IT and OT environments

By combining segmentation visibility with RedSeal's exposure analysis, organizations gain a more complete understanding of their attack surface and the architectural controls required to reduce risk.

These enhancements reinforce RedSeal's mission to help enterprise security teams move from reactive vulnerability management to proactive exposure management, giving organizations the clarity and confidence to understand their network, communicate risk, and take decisive action.

RedSeal Report Studio and Network Segmentation are available today.

For more information, visit www.redseal.net.

Jane Paolucci
RedSeal
+1 415-307-4081
email us here
Visit us on social media:
LinkedIn
YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/901463684

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.