INTEGRATION BRIEF

Federal Agencies: Visualize Your Risk via Vulnerability Attack Paths

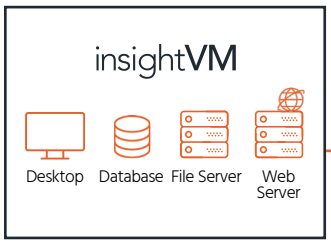
With RedSeal and Rapid7 InsightVM or Nexpose

Federal agencies and systems integrators face unique security challenges. Often the biggest hurdles to staying secure and compliant are gaining visibility into all areas of an ever-changing network, and being able to quickly understand the most likely threat vectors to be leveraged by attackers.

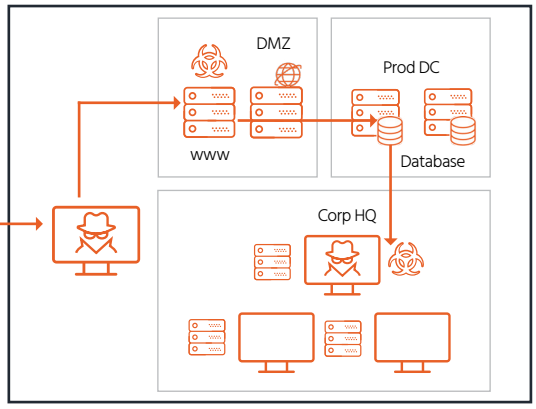
Organizations that integrate the rich vulnerability data from Rapid7's InsightVM or Nexpose with RedSeal are empowered to clearly visualize their network risk and identify discrepancies with DISA STIG compliance. Utilizing RedSeal, security analysts can model real world attacks and analyze full attack paths within the network; that information can then be used to prioritize which vulnerabilities pose the greatest threat if successfully exploited. This joint solution enables increased remediation cycles and easier identification of asset-based network threats.

HOW IT WORKS

An InsightVM* scan is conducted to assess the risk posture of the systems within an organization, with vulnerability results that include a calculated RealRisk™ Score associated with each system. A task in RedSeal is created to query InsightVM on a scheduled basis for the most up-to-date vulnerability information. An XML report is generated via the API to export the results, and the vulnerability data is processed and stored within RedSeal for further analysis.



Assessing Security Posture of Devices



Visualizing Attack Path Analysis

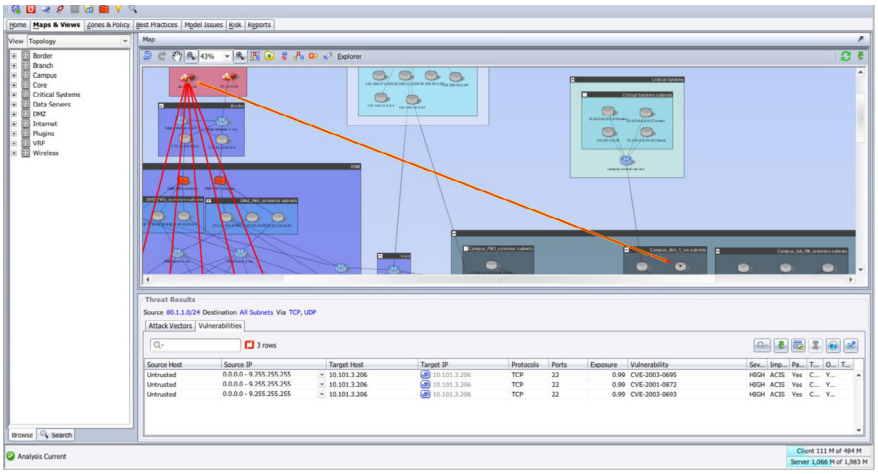
*All mentions of Rapid7 InsightVM associated with its integration with RedSeal also apply to Rapid7 Nexpose.

INTEGRATION BENEFITS

- Continuously monitor and track changes in your L2/L3 devices to respond quickly when something breaks compliance.
- Harden your devices in accordance with STIG compliances to mitigate threat vectors targeted by attackers.
- Remove blind spots in your network to ensure all assets are scanned.
- Use your own threat data and zero-day feeds with a customizable threat library.
- Utilize threat modeling to highlight the pathway attackers can take from a compromised asset, allowing for targeted remediation prioritization and deployment of additional defense layers.
- Ensure compensating controls are effective against difficult-to-patch vulnerabilities.

072117

Figure 1: RedSeal console with vulnerability data



How It Works

- Step 1: InsightVM (or Nexpose) performs a security assessment
- Step 2: A task is created to query InsightVM for latest vulnerabilities
- Step 3: RedSeal calls the InsightVM API for the latest XML report
- Step 4: Vulnerabilities get mapped to the network access context

What You Need

- Rapid7 InsightVM or Rapid7 Nexpose 6.4.47+
- RedSeal 8.4+

SUPPORT

Please contact Rapid7 for support or assistance at +1.866.380.8113 or support@rapid7.com.

SALES

Please contact Rapid7 for sales inquiries at +1.866.7.RAPID7 or federal@rapid7.com.

About RedSeal

RedSeal Networks is the leading provider of network infrastructure security management solutions that continuously provide network visualization and identify critical attack risk and non-compliance in complex security infrastructure. It provides network, security, and risk management teams with a firm understanding of where security is working, where investment is needed, and where greatest cyber-attack risks lie. This understanding, or "security intelligence", enables organizations to allocate resources where needed most, embed best practice into daily operations, and take prioritized action where needed. The world's largest government and commercial organizations use RedSeal security intelligence to build world-class operations that systematically reduce attack risk over time.

About Rapid7

With Rapid7, technology and security professionals gain the clarity, command, and confidence to safely drive innovation and protect against risk. We make it simple to collect operational data across systems, eliminating blind spots and unlocking the information required to securely develop, operate, and manage today's sophisticated applications and services. Our analytics and science transform your data into key insights so you can quickly predict, deter, detect, and remediate attacks and obstacles to productivity. Armed with Rapid7, technology professionals finally gain the insights needed to safely move their business forward. To learn more about Rapid7, visit www.rapid7.com.