REDSEAL

REDSEAL & RAPID7
ADD NETWORK CONTEXT TO VULNERABILITY PRIORITIZATION

SOLUTION OVERVIEW

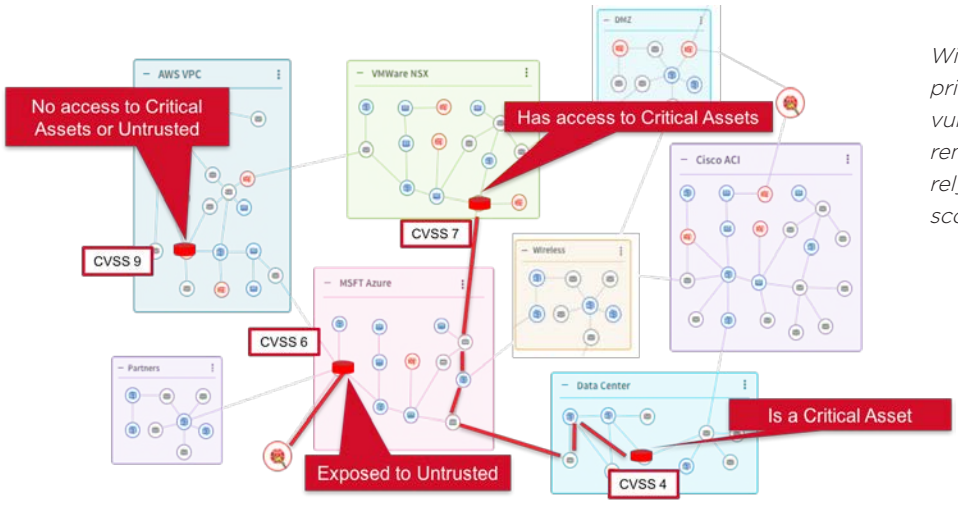
Network vulnerability assessments often overwhelm organizations with too many “high” and “critical” results. Compounding this problem is the sheer number of new vulnerabilities that surface each year and the large number of assets that need patching. Add to this the fact that many organizations are still running legacy systems whose vulnerabilities do not have patches. And finally, it is not easy to know whether all network devices were actually scanned.

VULNERABILITY PRIORITIZATION

RedSeal and Rapid7 have teamed up to add network context to Nexpose’s vulnerability prioritization. RedSeal looks at three factors to refine Nexpose’s initial prioritization:

First, it determines if a vulnerable host can be exploited from an untrusted network. Second, it determines if the vulnerable host can reach and potentially exploit downstream assets. And, third, it factors in the criticality of the assets in question. If access is permitted and assets are of high value, the priority increases. On the other hand, if layered defenses are preventing access and the hosts are not high value, the priority is reduced.

RedSeal prioritizes vulnerable hosts based on access to untrusted networks and the potential to infect other assets:



With network context, prioritize which vulnerabilities to remediate first, rather than relying on just the CVSS scores

INTEGRATION BENEFITS

- Mitigate critical threats with targeted patching
- Patch vulnerabilities that can be exploited from untrusted networks first
- Prioritize hosts that can infect critical downstream assets
- Discover gaps in scan coverage
- Contain vulnerabilities that don’t have patches

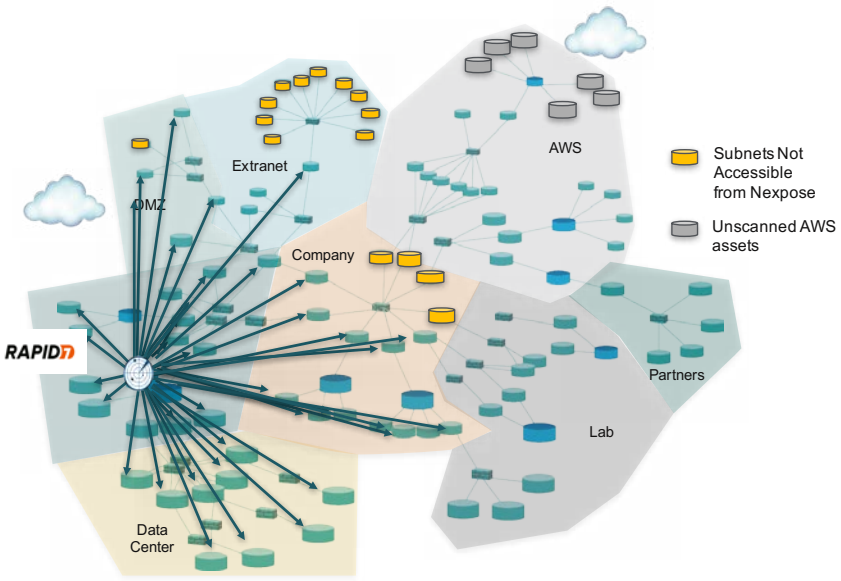
WHAT YOU NEED

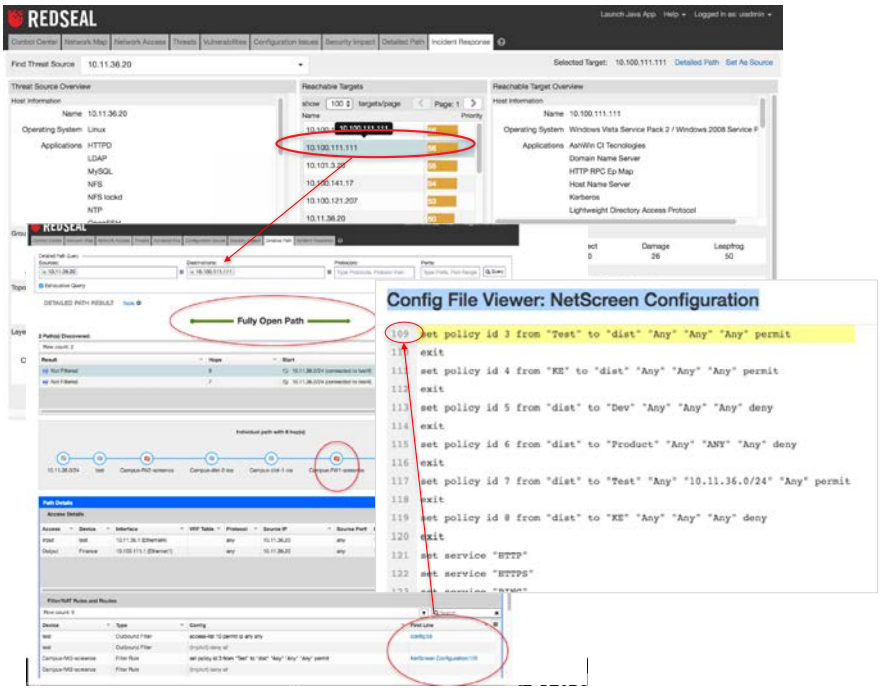
- RedSeal 8.3
- Rapid7 Nexpose 6.4.x

REDSEAL & RAPID7
ADD NETWORK CONTEXT TO VULNERABILITY PRIORITIZATION

GAPS IN SCAN COVERAGE

RedSeal can determine if all assets have been scanned by Nexpose. It is not uncommon for Nexpose to be denied access by a firewall, access control list (ACL) or other device. RedSeal can query its model and see all the access paths available to Nexpose. If a network segment has not been scanned, RedSeal will show you the unscanned subnet and the firewall rule or ACL that prevented the scan.





Detailed Path: RedSeal can show you the exact line of code in the configuration file to remediate.

CONTAINMENT

RedSeal can also help when there are no patches available for a legacy system.

RedSeal will identify a firewall, router, switch or other device that can be configured to prevent access to the vulnerable device.

REDSEAL

940 Stewart Drive, Sunnyvale, CA 94085

+1 408 641 2200 | 888 845 8169 | redseal.net/integration-apps