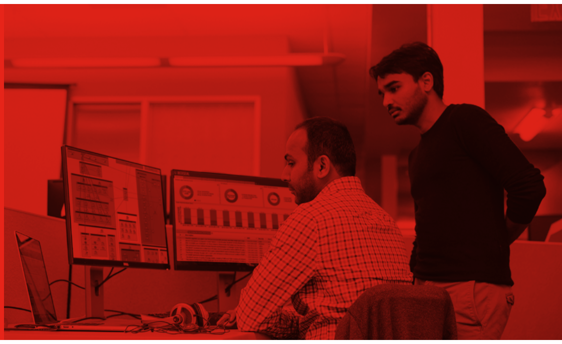
REDSEAL

EXPAND YOUR CYBER TERRAIN INFORMATION WITH ALL AVAILABLE ENDPOINT DATA



THE CHALLENGE

Enterprises get host information from a variety of sources, including endpoint protection (EPP), endpoint detection and response (EDR), network scanners, vulnerability scanners, and network access control. Each product's data provides discrete information on the endpoints in your network. They don't answer important network context questions, like: Where is this asset, physically and logically? What is the asset exposed to or exposing access to? What would happen if the asset was breached? Moreover, each information source has its own interface, making it nearly impossible to correlate data from one source to another. It has required a lot of manual labor – exporting the data to spreadsheets so it can be combined, sorted and analyzed. What's been missing is a single source of endpoint information, one common network picture that combines all endpoint data.

SOLUTION OVERVIEW

RedSeal's network modeling and risk scoring platform addresses this need, consolidating and modeling all available endpoint information. You'll have one source with information from vulnerability scanners, EPP and EDR, as well as from other applications such as Active Directory. The result is the most complete network model available. It includes public and private clouds, physical assets and endpoint sources, so you can confidently validate your security posture, accelerate investigation and improve the productivity of network and security teams.

RedSeal allows you to import, intelligently merge, deconflict and store host data from multiple sources. You can add network context to EDR, EPP, active directory, and scanners. You'll be able to make requests such as:

- Show me all the Windows hosts directly exposed to an untrusted network, where EDR reports a specific DLL exists
- Show me all webservers where the vulnerability scanner shows a particular Apache-related CVE, and where the location is data-center-1
- Sort, filter, and view RedSeal-prioritized vulnerabilities by group, tag, geographic location, or any custom grouping
- Show me all hosts directly exposed to an untrusted network and display their business value, downstream risk, physical location, operating system and whether they have any exposed CVEs

BENEFITS

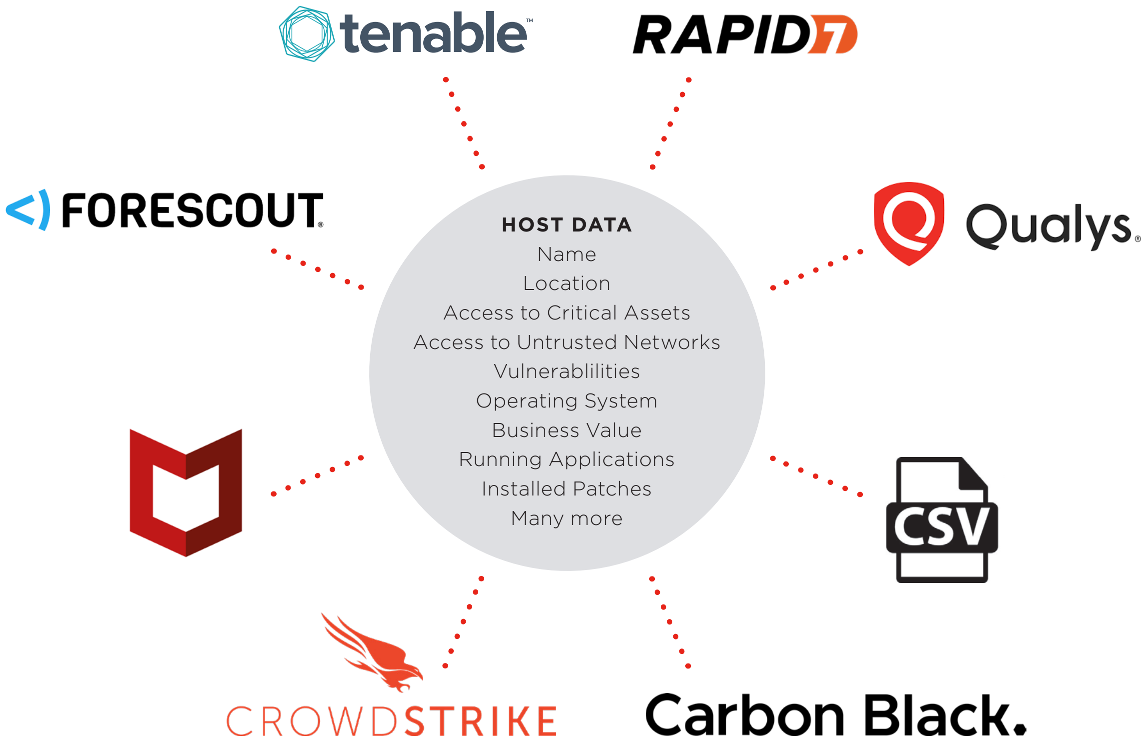
- Total cyber terrain mapping. Model your network at Layers 2, 3, 4 and 7 with networking devices and host information in one place across public cloud, private cloud and physical environments.
- Accelerate your incident response and threat hunting capabilities by adding network context to hosts and their vulnerabilities

REDSEAL AND ENDPOINT DATA

With RedSeal's network modeling and risk scoring platform you can now:

- Import and store host data from multiple sources
- Add unified network context from public cloud, private cloud and physical environments to EDR, EPP, and other applications such as Active Directory
- Get and continuously monitor the most complete network model available
- Consolidate all host data in one place
- Search all consolidated host data

REDSEAL COMBINES ENDPOINT DATA FROM ALL SOURCES, SO YOU CAN FIND ALL AVAILABLE INFORMATION ABOUT ANY HOST IN YOUR NETWORK.



HOST DATA
Name
Location
Access to Critical Assets
Access to Untrusted Networks
Vulnerablilities
Operating System
Business Value
Running Applications
Installed Patches
Many more

Sample of endpoint data sources RedSeal can combine.