REDSEAL

FEDERAL CIVILIAN AGENCY SAVES THE DAY

Two years ago, a federal government civilian agency had a problem. Nation state actors were targeting the agency, creating numerous cyber events and breaches every day. The media was all over the story. They faced enormous pressure to change the cybersecurity status quo.

The agency's cybersecurity team knew that they were in reaction mode. They had a gut feeling that they didn't know as much about their networks as they needed to. Vulnerability scanners were in place, patching was done on schedule, yet incidents kept happening. Were the scanners accurate? Were there missing components on their networks?

After extensive review and testing of the cybersecurity analytics tools on the market, the agency selected RedSeal—initially to manage the findings of the vulnerability scanners and to determine what to fix first, based on risk to high value assets. After expanding the program to thirteen locations, the agency integrated RedSeal enterprise-wide for network mapping and vulnerability prioritization.

The audit team manager said, "Just last week, using RedSeal, we conducted an assessment of a location with 1,500 endpoints and correlated 5,000 vulnerabilities. Further automated analysis by RedSeal showed that only four were a critical threat and should be prioritized for remediation. Normally, the local network engineering staff would have been overwhelmed by 5,000 findings. We saved them a massive amount of work, lowered the risk of a breach and gave them an accurate model of their network for the first time."

The agency's Cybersecurity Assessment Team found that with RedSeal the team's functionality, speed and accuracy was significantly improved. Intuitively, the team members are able to set up RedSeal instances and map the network with a minimum of training and outside consultants. They are also able to easily create reports customized to the needs of each site's particular mission and responsibilities.

"RedSeal is the must-have tool for any cybersecurity assessment team," was the agency's conclusion.

> **"Back then, no one had an overall depiction of the network. What we needed was a tool that, on day one, could map the network, figure out the high value assets, find the vulnerabilities and prioritize them."**
>
> *Manager of the Independent Verification, Validation Assessment and Audit Team*