REDSEAL

CASE STUDY

Vulnerability Assessment: Clear ROI for RedSeal Deployment

CHALLENGE

An intelligence agency was struggling with a costly and inefficient vulnerability assessment program. The program, managed by two internal employees and 16 contractors, required significant resources and time.

Each assessment for a data center took anywhere from two months to a full year to complete. The process involved manually inventorying data centers, reviewing configurations for security compliance, and creating network maps—only for the maps to quickly become outdated. This resulted in incomplete vulnerability assessments and a lack of real-time network visibility, making it difficult to keep up with a constantly evolving threats.

SOLUTION

After extensive research and recommendations from other government cybersecurity teams, the agency turned to RedSeal. RedSeal's continuous monitoring of network configuration files allowed the agency to maintain an up-to-date network map at all times. This eliminated the delays and inaccuracies of the previous process. In-Q-Tel experts reviewed and swiftly approved the solution, and within just a few days, RedSeal was deployed across 14 instances, providing agency-wide coverage.

RESULTS

With RedSeal in place, the agency transitioned to continuous vulnerability assessments year-round, across all data centers. The need for expensive contractors was eliminated, drastically reducing program costs. Real-time, accurate assessments enabled more effective decision-making and significantly improved the agency's cybersecurity posture. The agency now has full, ongoing visibility into its network, ensuring that vulnerabilities are continuously addressed before they can escalate.

"We realize now that we can't leverage the other cybersecurity tools unless we have RedSeal. RedSeal is core to our cybersecurity plan".

-Intelligence Agency Customer