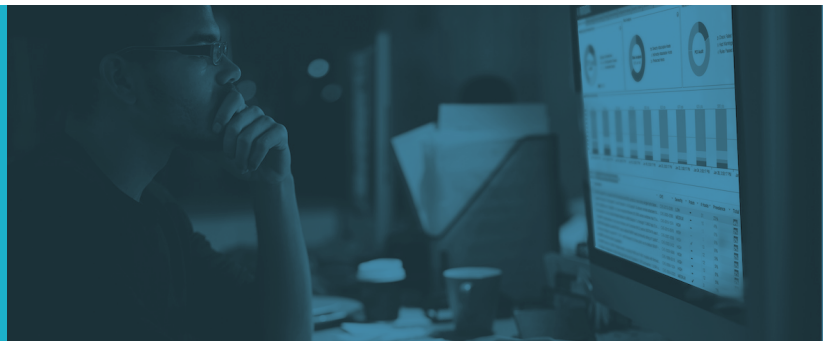
REDSEAL

REDSEAL AND FEDERAL CIVILIAN AGENCIES



PROACTIVE CYBER DEFENSE SUPPORTING NETWORK RESILIENCE

After the OPM breach last year, federal civilian agencies have had to face the pervasiveness of cybersecurity threats and breeches. The resulting OMB 30-day Cybersecurity Sprint resulted in a strategy to enhance federal cybersecurity and overhaul information security practices, policies and governance.

The first three objectives of the Cybersecurity Strategy Implementation Plan (CSIP) for federal civilian agencies are:

- Prioritized identification and protection of high value information and assets;
- Timely detection of and rapid response to cyber incidents;
- Rapid recovery from incidents when they occur and accelerated adoption of lessons learned from the Sprint assessment;

To meet these objectives, agencies have to overcome the challenge that their networks have grown so large and complex they've outpaced human ability to manage every aspect of them. Agencies want proactive defense and predictive analysis, but need help to achieve them. Specifically, federal civilian agencies need to:

- Create interactive models of their entire 'as built' networks – including those parts hosted in the cloud –and calculate all the ways data (and intruders) can move from one point to any other.
- Discover previously unknown devices, so they have a complete network picture.
- Fix the highest-risk and most-exposed vulnerabilities first.
- Continuously monitor potential attack paths
- Evaluate their actual network build against their policies.
- Test and measure network changes before implementing them.

"RedSeal is a security tool, a compliance tool, a management tool and an incident response tool. It gives us a lot more visibility into what is happening on our network."

— US POSTAL SERVICE

"Continuous monitoring technologies such as RedSeal will enable the U.S. Intelligence Community to effectively operate the complex, dynamic network defenses that protect critical information and systems. We believe RedSeal's capabilities have widespread applicability throughout the federal government as agencies strive to improve their security posture."

— IN-Q-TEL

"The RedSeal platform helps government agencies better prioritize vulnerability remediation efforts, dramatically cut compliance costs and optimize their security architectures."

— HOMELAND SECURITY TODAY

REDSEAL AND THE DEPARTMENT OF DEFENSE

MAXIMIZE DIGITAL RESILIENCE WITH REDSEAL

RedSeal's cybersecurity analytics platform allows you to maximize your network's digital resilience by first building an accurate model of your network, including your physical, cloud and virtual networks. RedSeal creates this complete model from Layer 2 and 3 device configuration data -- retrieved dynamically or offline. Then, it adds vulnerability assessment data from your vulnerability managers.

This network knowledge allows RedSeal to evaluate and prioritize vulnerabilities by their severity and the value of information on each affected computer, as well as how accessible they are. RedSeal can show you every possible network path and recognize whether a target is even open to compromise.

Finally, by using the configuration files and computing all the access paths, RedSeal uncovers undocumented network pieces, network "unknowns" in your constantly morphing network. This comprehensive inspection allows RedSeal to provide a risked-based audit of your network and to continuously monitor your security posture. You can track how your network resilience is trending over time, why it is improving or degrading, and what is causing those changes. RedSeal is a comprehensive continuous monitoring solution for diverse and dynamic networks.

If a breach does occur, and it will, RedSeal empowers your first responders by giving them an up-to-date network diagram so they can identify hosts that are most at risk. They can see what's directly attackable, what's indirectly attackable and what's protected.

The RedSeal platform has been widely adopted by commercial, civilian, intelligence and DoD enterprises.

KEY REDSEAL CAPABILITIES

- End-to-end network topography construction: physical, virtual, cloud
- Risk-based security audit and assessment
- Vulnerability remediation prioritization through heat map technology
- Network device compliance checking
- Enclave and segmentation policy analysis
- Advanced threat scenario modeling and simulation
- Attack vector analysis
- Virtual penetration testing
- Historical breach forensic analysis
- BYOD support
- Security ecosystem integration

To schedule a demo or for more information, go to www.redseal.co/federal

REDSEAL

1600 Technology Drive, San Jose, CA 95110

+1 408 641 2200 | 888 845 8169 | redseal.net

AUGUST 2019