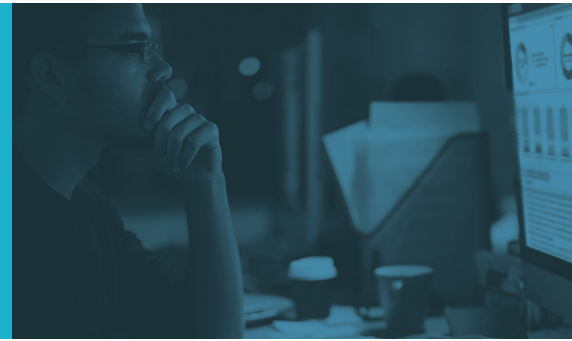**REDSEAL**

REDSEAL AND THE
INTELLIGENCE COMMUNITY

PROACTIVE CYBER DEFENSE DELIVERING NETWORK RESILIENCE

RedSeal helps the intelligence community fight persistent threats with resilience.

Both the 2015 and the 2016 Worldwide Threat Assessments of the U.S. Intelligence Community put global cyber risk at the top of the list. The Assessment characterizes cyber threat as ongoing and persistent.

Since the cyber threat cannot be eliminated, cyber risk must be managed.

Networks have grown so large and complex they've outpaced our human ability to manage every aspect of them. RedSeal gives you what you need for proactive defense and predictive analysis, so you can:

• Create interactive models of your entire 'as built' network, including those hosted in the cloud.

• Visualize all the ways data—and intruders—can move from one point to any other.

• Discover previously unknown devices for a complete network picture.

• Prioritize the highest-risk and most exposed vulnerabilities to fix.

• Continuously monitor potential attack paths.

• Evaluate your actual network build against defined policies.

• Test and measure network changes before implementing them.

"Every conflict in the world has a cyber dimension.."

— ADM Michael Rogers, Commander of U.S. Cyber Command and Director of the National Security Agency

"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 providing a comprehensive view of your as built network and security infrastructure. RedSeal does this by creating a model of your network that provides an accurate map of your physical, cloud, and virtual networks. RedSeal creates a complete network construct by utilizing two components of information that can be retrieved dynamically or offline: configuration data from network devices and vulnerability assessment data from scanned hosts.

This combination of data allows RedSeal to see all host and access paths across the network, plus all vulnerabilities that put them at risk. With this knowledge, RedSeal takes network access into account when prioritizing vulnerabilities. This allows RedSeal to not only distinguish every possible network path, but to recognize whether a target is even open to compromise.

Finally, by using the configuration files and vulnerability assessment data as a check and balance, RedSeal locates network misconfigurations such as dangling links, undocumented network segments, and un-scanned hosts. In essence, RedSeal uncovers network "unknowns" in your constantly morphing network environment. This comprehensive inspection allows RedSeal to create 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.

When a breach occurs, 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. With operational certifications such as NIAP Common Criteria, APLs such as DADMS and UCAPL*, and ATOs from the USMC, US NAVY, DISA and more, RedSeal was chosen as the continuous monitoring component of the JRSS program that is currently the security stack for the Joint Information Environment (JIE).

KEY REDSEAL CAPABILITIES

- End to end network topography construction (living network diagrams): physical, virtual, cloud
- Risk-based security audit and assessment
- Vulnerability remediation prioritization
- Network device best practice checking
- Enclave / segmentation policy analysis

- Advanced threat scenario modeling
- Enclave and segmentation policy analysis
- Attack vector analysis
- Virtual penetration testing
- Digital resilience analysis
- Security ecosystem integration

RedSeal is a trusted partner in the intelligence community.

To schedule a demo or for more information, go to www.redseal.net/government