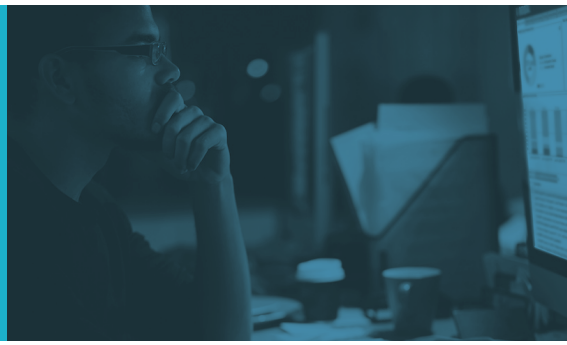
REDSEAL

REDSEAL AND THE DEPARTMENT OF DEFENSE



The Department of Defense's Choice for Defensive Cyber Operations

2017 is bringing major tactical and strategic changes to the way the Department of Defense conducts Defensive Cyber Operations (DCO). The Joint Force Commander's Guide to Cyberspace Operations says, "The ultimate goal of DCO is to change the current paradigm where the attacker enjoys significant advantage. DCO provide the ability to discover, detect, analyze and mitigate threats to include insider threats. As opposed to DODIN Ops, we should think of DCO as mission focused and threat specific."

RedSeal: The Foundation for Defensive Cyber Operations

RedSeal understands and improves the resilience of every element, segment, and enclave of your network, enabling cyber situational awareness for DCO. RedSeal works with your existing security stack and network infrastructure —including cloud and SDN — to automatically and continuously visualize a logical model of your "as-built" network.

RedSeal's network modeling and risk scoring platform is designed to enable cyber operators to act with speed and efficiency. With RedSeal, you can visualize end-to-end access, intended and unintended, between any two points of the network to speed incident response for CPTs. You can visualize detailed access and attack paths for individual devices in the context of exploitable vulnerabilities to speed cyber operators' decision making during a mission.

RedSeal builds a complete model of your network using network device configuration files retrieved either dynamically or completely offline. This Layer 2/3 configuration data includes devices such as routers, firewalls, switches, VPN concentrators, and load balancers — whether physical, in the cloud or in software-defined networks. RedSeal builds a comprehensive network map showing every possible way in, out, and through your network, detailing all possible attack vectors. RedSeal checks all your devices to see if they comply with industry best practices and standards such as DISA STIGs and NIST guidelines. This proactive automation greatly reduces audit prep time (CCRI, others) and assists with speedy remediation.

"We are overwhelmed with data and underwhelmed by information. RedSeal allows us to prioritize with actionable intelligence and stop playing whack-a-mole."

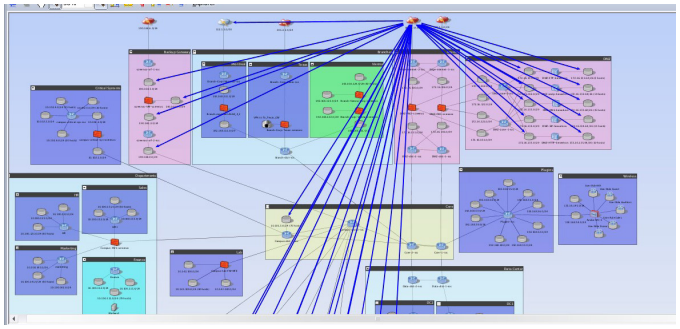
— DOD CUSTOMER

"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

REDSEAL AND THE DEPARTMENT OF DEFENSE

RedSeal connects to your vulnerability managers to import assessment data in standard CVE format from scanned hosts (i.e. ACAS). This data allows RedSeal to include all scanned hosts and other IP data across the network, plus all vulnerabilities that put them at risk. RedSeal then takes network access into account when prioritizing vulnerabilities for mitigation, showing you if a target is even open to compromise. This entire data summary and detail can be viewed in the platform, in report formats, or through an API to integrate with familiar dashboards.



This comprehensive, continuous inspection allows RedSeal to report a risked-based audit of your network and then to continuously monitor your security posture. Operators and leadership can track how defensive operations are trending over time via the Digital Resilience Score, which also measures vulnerability management, secure configuration management, and understanding of your network.

The RedSeal platform has been widely adopted by commercial, civilian, intelligence, and DoD enterprises. With operational certifications such as NIAP EAL 2, DADMS, and ATOs from USMC and DISA, RedSeal was chosen as the continuous monitoring component of the JRSS program that is currently the security stack for the Joint Information Environment (JIE).

All DCO functions require real-time understanding and a model of the cyber terrain to discover, detect, analyze and mitigate threats and deliver resilience to the mission. RedSeal is the unique foundational platform to enable DCO.

Key RedSeal Capabilities

- End-to-end network mapping and modeling
- Attack vector analysis
- Enclave/segmentation policy analysis
- Virtual penetration testing of entire network
- Advanced threat scenario modeling and simulation
- Incident response acceleration
- Vulnerability prioritization with network context
- Layer 2 & 3 device compliance checking
- Works with existing security products
- Unified network model, including physical, SDN, hybrid and cloud networks
- Risk-based security audit and assessment

Battle Tested: RedSeal Department of Defense Clients

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

REDSEAL

940 Stewart Drive, Sunnyvale, CA 94085

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