REDSEAL

AUTOMATICALLY VALIDATE YOUR STIG COMPLIANCE

For the convenience of the Department of Defense and other organizations that have adopted STIGs* (DISA's Security Technical Implementation Guides), RedSeal offers product modules for STIG compliance validation—including support for the DISA-defined STIG categories most relevant to networking:

- Firewalls
- Network infrastructure routers and L3 switches
- Network perimeter routers and L3 switches
- L2 switches

These network-relevant STIGs are incorporated within RedSeal's existing secure configuration checks. You can set RedSeal to alert you if or when any network device doesn't comply. RedSeal will also provide you with detailed remediation guidance for each non-compliant device—including the precise configuration file line you need to modify.

RedSeal's automatic STIG compliance checks and remediation guidance greatly reduce the time and effort required to keep your network in compliance and audit-ready.

RedSeal's STIG product modules include: Cisco IOS, Cisco ASA, Cisco NX-OS, Juniper Junos OS, Palo Alto Networks PAN-OS, and F5 BIG-IP. New and updated STIGs will be included as they become available.

* A STIG, or Security Technical Implementation Guide, is a Department of Defense document created by DISA. Field Security Operations for hardware and software products. A STIG provides secure configuration guidance for a product to reduce its attack surface.

DISA

WHAT OUR CUSTOMERS SAY

"Using RedSeal to map site infrastructure and test for compliance against DISA STIGs, as well as the ability to compare the documented architecture against the real architecture, has not only saved us hundreds of man hours but increased our coverage from representative sampling to total assets"

-U.S. Marine Corps

REDSEAL

940 Stewart Drive, Sunnyvale, CA 94085

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

NOV 2018