Automatically Validate

STIG and SRG Compliance

Make audits routine: DISA STIG and SRG compliance and reporting

For the U.S. Department of Defense and other organizations, RedSeal offers a product extension for validating compliance with DISA's Security Technical Implementation Guides and Security Requirement Guides (DISA STIG and SRG.) This extension includes support for the DISA-defined STIG and SRG categories most relevant to networking.

These network-relevant checks are incorporated within RedSeal's existing automatic secure configuration checks. You can set RedSeal to alert you if or when any network device does not comply with DISA standards. RedSeal provides detailed remediation guidance for each non-compliant device, including the precise configuration file line you need to change.

With automatic compliance checks for DISA STIG and SRG and the remediation guidance RedSeal provides, you can keep your network in compliance and make audits routine.

RedSeal's product extension includes the following modules. New and updated DISA STIG and SRG checks will be included as they are released.

Cisco
Platform: Cisco IOS Router
Platform: Cisco IOS Switch
Platform: Cisco IOS XE Router
Platform: Cisco IOS XE Switch
Platform: Cisco (Cisco FWSM v2, Cisco PIX - ASA - FWSM, Cisco PIX v6
Platform: Cisco NX-OS

Juniper
Platform: Junos OS Router RTR
Platform: Junos OS Router NDM
Platform: Junos OS Layer 2 Switch SRG
Platform: Junos OS Firewall SRG

F5 Networks
Platform: F5 BIG-IP AFM
Platform: F5 BIG-IP DM
Platform: F5 BIG-IP LTM

Palo Alto Networks
Platform: PAN-OS ALG
Platform: PAN-OS IDPS
Platform: PAN-OS NDM
Platform: PAN-OS Firewalls

VMware NSX
Platform: NSX Manager
Platform: NSX Distributed Firewall
Platform: NSX Distributed Logical Router

REDSEAL

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