AUTOMATICALLY VALIDATE YOUR STIG COMPLIANCE

For the convenience of the Department of Defense and other customers who have adopted STIGs* (DISA's Security Technical Implementation Guides), RedSeal offers a product extension for STIG compliance validation-- including support for the DISA-defined STIG families most relevant to networking:

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

New and updated STIGs will be included as they become available.

These network-relevant STIGs are incorporated within RedSeal's existing automatic checks. You can set RedSeal to alert you if or when any network device doesn't comply. For each STIG, in addition to the familiar detailed description, RedSeal provides detailed remediation guidance for each non-compliant device – including the precise configuration file line you need to change.

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

* 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.