REDSEAL

REDSEAL AND FORTINET

Prevent Unintended Access Across Your Hybrid Network

The challenge: Unintended network access

Large, complex networks require implementing and managing thousands of access rules across your infrastructure. Determining the devices and rules responsible for unintended access can often be challenging. Unintended and accidental exposure that contains vulnerabilities can leave organizations open to attack and allow an intruder to gain access to critical data and systems.

Fortinet and RedSeal have partnered to deliver an industry-leading security solution that enhances your attack surface visibility by bringing network context, connectivity, and exposure information into a comprehensive view of your security posture.

RedSeal + Fortinet integrated security solution

The RedSeal network exposure management platform integrates with Fortinet FortiManager, FortiGate NGFW (Next-Generation Firewall), and FortiSwitch, ensuring uniform visibility, defense, and ongoing management of an organization's firewall and network device infrastructure. Together, Fortinet and RedSeal allow organizations to visualize their hybrid network topology, validate end-to-end access routes, import vulnerability scan data to prioritize remediation efforts, and continuously monitor and track changes to maintain compliance.

FORTINET

Integrated solution benefits

- Asset discovery and inventory with end-to-end hybrid network visibility
- Analysis of all possible access to critical assets, on premises and in the cloud
- Predictive threat modeling and metrics
- Access policy configuration drift and impact assessments
- Automated, exposure-based remediation prioritization
- Unparalleled protection with the Fortinet Security Fabric and RedSeal

Solution components

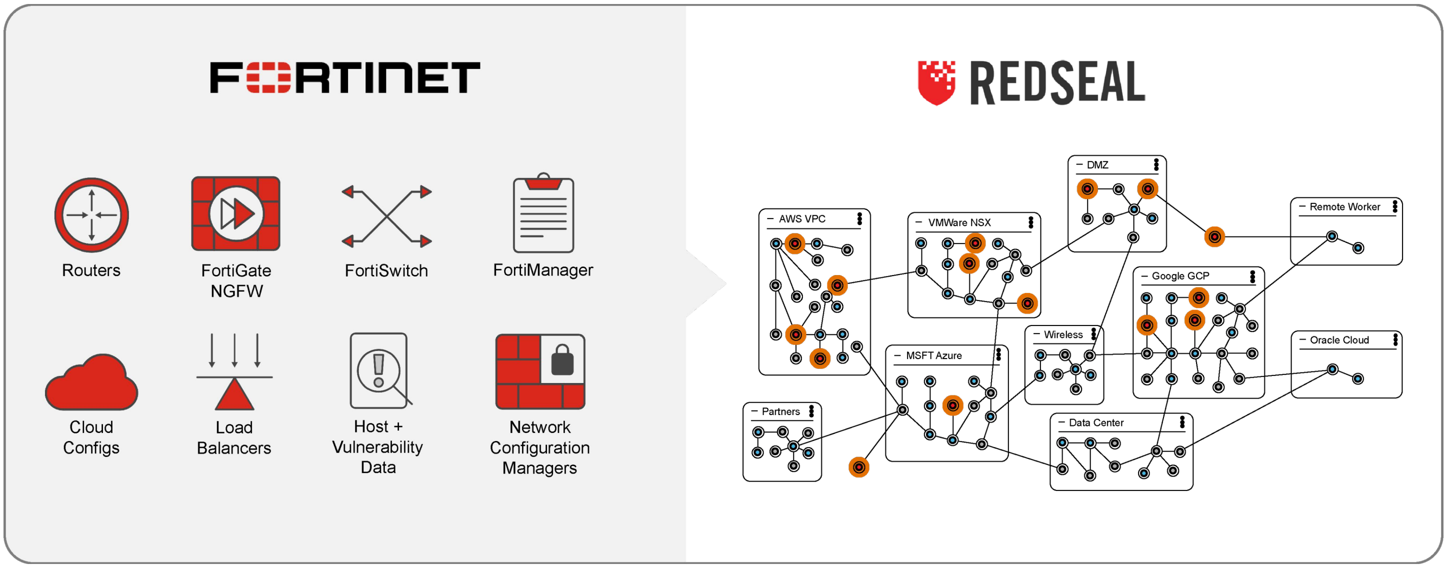
FortiManager provides automation-driven centralized management of your Fortinet devices from a single console. This process enables full administration and visibility of your network devices through streamlined provisioning and innovative automation tools. This integration includes the management of FortiSwitch and FortiGate NGFW with Secure SD-WAN.

FortiGate NGFW with Secure SD-WAN utilizes purpose-built security processors and threat-intelligence security services from artificial intelligence (AI)-powered FortiGuard labs to deliver top-rated protection and high-performance inspection of clear-textured and encrypted traffic. NGFWs reduce cost and complexity with complete visibility into applications, users, and networks and provide best-of-breed security.

FortiSwitch managed network switches can intuitively adjust to ensure peak performance within your network automatically. Ethernet switching from Fortinet works directly with FortiGate to create a secure, simple-to-manage architecture with a single point of management and configuration.

RedSeal is a network exposure management platform that enables organizations to take a more proactive, holistic, and continuous approach to cybersecurity. It uniquely offers four foundational capabilities in a single platform:

- **Network visualization,** for building an accurate model (network digital twin) of the entire environment and discovering all connected resources across public cloud, private cloud, and on-premises environments
- **Attack path analysis,** for uncovering every exposure and assessing the full impact from internal, external, direct, and indirect (or downstream) access, whether intentional or accidental
- **Risk prioritization,** for focusing mitigation and remediation efforts on exploitable exposures that have the greatest potential impact on the organization
- **Compliance checks,** for managing and reporting adherence to internal policies, external regulations, and best practices—from CTEM, Zero Trust, and PCI DSS to CIS, STIG, NIST, and others



RedSeal ingests and analyzes complex infrastructure data to build a network digital twin and prioritize risks.

RedSeal leverages the configuration, policy, and network information from Fortinet and other infrastructure devices, including hosts, to provide the organization with a holistic view of the entire network across on-premises and cloud environments. RedSeal calculates a Digital Resilience Score (DRS), modeled after a credit score, so you'll have one metric to help manage and improve your network security posture. RedSeal's understanding of your network helps you verify compliance with internal policies and external regulations and accurately prioritize your risks and vulnerabilities. Knowing your network and its detailed access paths will also accelerate incident response efforts.

Use case #1: Network-wide validation of firewall security policies

Challenge: Validating access policies in the context of end-to-end network access within an enterprise network is not trivial.

Solution: Enterprises deploying Fortinet FortiGate can leverage RedSeal to visualize access and validate policies at the application levels (Layer 7) and networking levels (Layers 2, 3, and 4) across on-premises and cloud deployments. This level of visibility within and between their hybrid network environments (physical assets, private cloud, and public cloud) helps teams understand and prioritize incidents and vulnerabilities wherever they are.

Use case #2: Government and industry-driven compliance

Challenge: It is difficult to build and maintain a security profile in line with industry best practices across cloud and on-premises infrastructure. You need to eliminate configuration settings known to be insecure, protect the organization from known threats, and offload unnecessary cyber risk by narrowing the attack surface to only what is necessary.

Solution: RedSeal validates Fortinet FortiGate configurations against governmental and industry regulations, as well as internally defined security policies, with the following modules:

- STIG Module for Fortinet FortiGate
- CIS Benchmarks for Fortinet FortiGate

Validate Fortinet configurations and policies with RedSeal

As organizations use more cloud-based services, the attack surface grows in size and complexity. Understanding network connectivity and all possible access to critical resources is paramount to staying ahead of increasingly sophisticated adversaries. With a comprehensive, network-level view of hybrid infrastructure, RedSeal helps Fortinet users prevent unintended connectivity and access across their hybrid environment by proactively identifying exposures due to misconfigurations and policy violations.

Contact RedSeal for more information or request a demo today.

RedSeal, a leader in network exposure management, offers proactive insights to close security gaps in hybrid environments. It creates a network digital twin for comprehensive visibility and protection. Trusted by Fortune 1000 companies and U.S. military branches, RedSeal enhances operational efficiency, boosts productivity, and reduces business risk.
www.redseal.net | info@redseal.net | +1 408-641-2200 | 888-845-8169