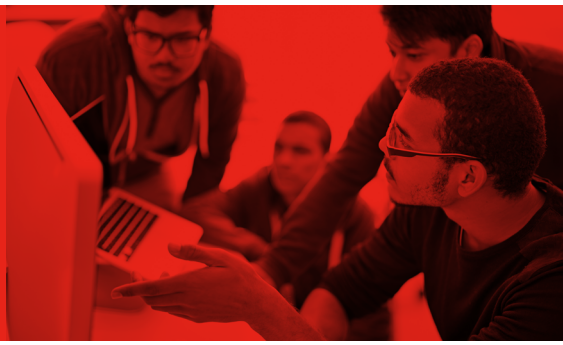
REDSEAL

IDENTIFY HIGH-RISK ENDPOINTS

BASED ON REDSEAL'S RISK SCORE



FORESCOUT

SOLUTION OVERVIEW

A single end point, reachable from an untrusted network and with access to critical assets, can compromise an entire organization. In addition, network devices that don't comply with your security policies can expose your network to cyberattacks.

RedSeal's security analytics platform builds and provides an accurate, up-to-date model of your network so you can visualize access paths, check for policy and compliance violations and prioritize what to fix, to protect your most valuable assets. Forescout CounterACT® agentless technology discovers, classifies and assesses devices the instant they connect to your network. RedSeal and Forescout have partnered to help organizations improve real-time visibility, enforce policy-based network access control and end point compliance, accelerate incident response and automate threat mitigation to ensure your organization is meeting its security requirements.

Understand with Network Context from Redseal; Control and Orchestrate with Forescout CounterACT

RedSeal ingests device configurations from different vendors (including SDN vendors) to construct an "as-built" network model. This includes a full understanding of what's in your network and how it all connects. This network situational awareness is critical to make sense of huge volumes of data and prioritize issues. Without it, incident response teams struggle the same way a firefighter would, knowing only that a fire is happening—over there. No firefighter would go in without an area map. RedSeal provides a network map of where the hot spots are, with detailed access paths to critical assets. Forescout CounterACT allows you to control access by restricting, blocking or quarantining non-compliant or compromised devices, automating common workflows and accelerating system-wide response to quickly mitigate risks and data breaches.

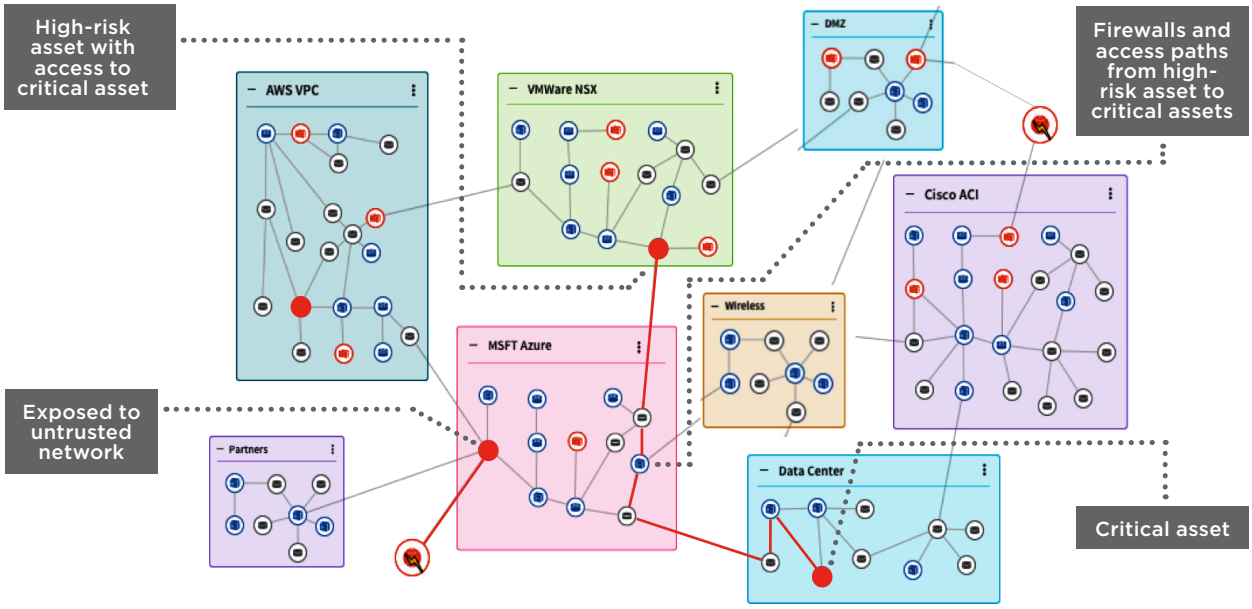
BENEFITS

- Identify high-risk end points based on RedSeal's risk score
- Use RedSeal to identify risk to critical assets; use Forescout CounterACT to automate risk mitigation
- Discover devices that have STIG or other configuration violations
- Display results within Forescout CounterACT
- No additional resources or specific RedSeal training needed

WHAT YOU NEED

- RedSeal 8.3.1+
- Forescout CounterACT 7.1.1

IDENTIFY HIGH-RISK ENDPOINTS



REDSEAL'S RISK SCORE IDENTIFIES HIGH RISK ENDPOINTS

RedSeal provides policy templates within Forescout CounterACT to extend visibility past the high-risk end points to your critical assets. It calculates a risk score for your end points. These scores provide key metrics for executing a range of responses depending on the severity of the problem.

For each of these end points, RedSeal computes a risk score based on:

- The presence of known vulnerabilities
- Whether or not an untrusted network can access it
- Whether the end point can reach critical assets—and the value of those assets

RedSeal's policies provide a list of high-risk end points and another list of those that can reach critical assets. For each end point on these lists, you'll see:

- The end point's risk score
- Whether it is accessible from an untrusted network
- A list of critical assets it can reach
- Detailed path information to each critical asset—with information on which devices and configuration changes you can use to mitigate the risk

Once Forescout CounterACT discovers a security problem on a device, its sophisticated policy manager can automatically execute a range of responses depending on the severity of the problem, from an email notification to the end user, to mandatory remediation (software patching), to actions such as blocking or quarantining the device.

IDENTIFY DEVICES WITH CONFIGURATION ISSUES

RedSeal evaluates network device configurations—of routers, switches, firewalls, load balancers, and wireless access points—against industry standards, including STIGs. RedSeal policy provides a list of the devices with configuration issues and how severe the issue is: high, medium or low. Forescout CounterACT can enforce the appropriate level of control from modest to stringent based on your security policies.

REDSEAL

1600 Technology Drive, San Jose, CA 95110

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

AUGUST 2019