ARE YOUR CORPORATE ASSETS AND REMOTE WORKFORCE PROTECTED AS YOU DEPLOY MERAKI DEVICES?

Cisco's Meraki products provide a seamless connection for your remote workforce, but are you confident that they are securely connected? A misconfiguration can unintentionally expose your corporate assets to unauthorized users—or provide an unmonitored path for data exfiltration. Validating all Meraki devices across your network can be a formidable challenge. Visibility into Meraki devices and their connections wherever they are, offers both validation and peace of mind.

RedSeal's experienced team of cybersecurity consultants can give you the intelligence you need by showing you what's on your network, how it's connected and what's at risk. Redseal gives you visibility across hybrid cloud and on-premise environments—from Meraki devices to your data centers. Our security professionals can provide all the necessary insights and explain the associated risks so that you can make an informed decision.

RedSeal: Discover, Investigate, and Act

- Discover new and existing devices
- Investigate devices to determine if they're securely configured and comply with organizational policies
- Act to remediate and mitigate risks

DISCOVER
INVESTIGATE
ACT

REDSEAL

Discover all your Meraki devices

See all your connected Meraki devices—MR series wireless access points; MS series switches; and MX and Z series firewalls—wherever they are on your network, including remote locations.

Investigate to determine if devices are securely configured and comply with organizational policies

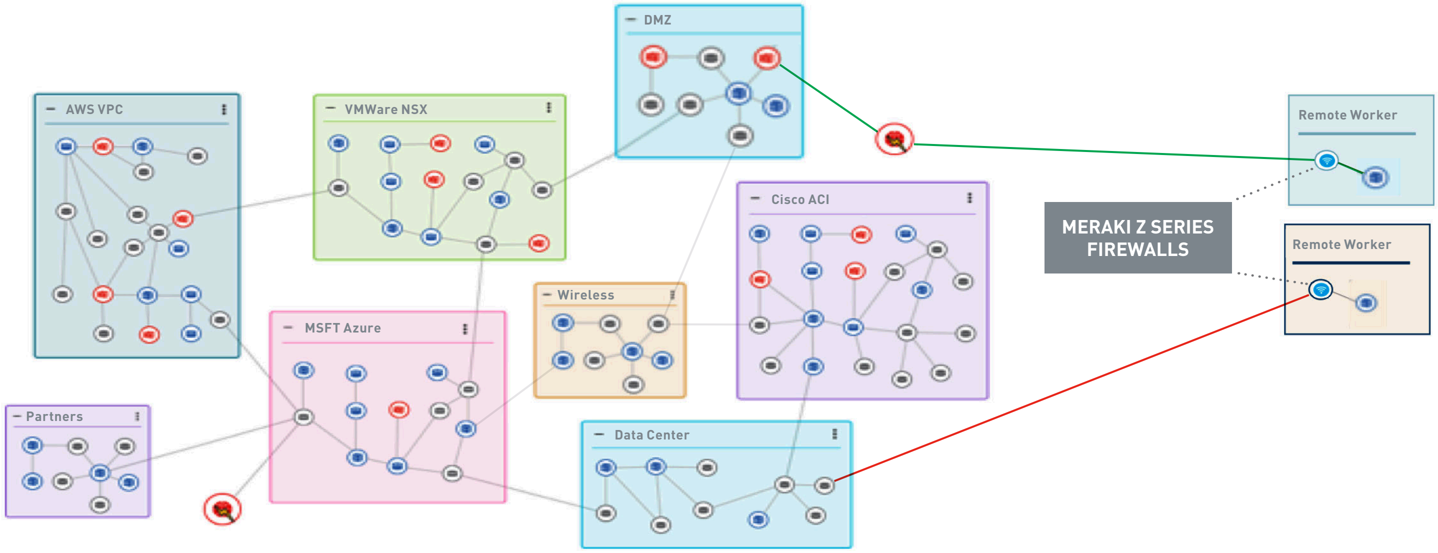
Ensure all your Meraki devices are configured securely and adhere to both your policies and industry best practices. Review them for misconfigurations and to see if they allow unintended network access. Where you have both guest and corporate Wi-Fi networks, RedSeal will identify any cross-over between trusted and untrusted network spaces, preventing bad actors from using unmonitored connections to inject ransomware or exfiltrate data. Uncover access to untrusted connections, such as the internet or a third-party. Or where unauthorized employees have access to key corporate data, whether it's in the cloud or on-premise.

Act to remediate and mitigate risks

RedSeal security experts work with you and your key stakeholders to investigate security findings and coordinate remediation actions to mitigate risks. They'll review ongoing changes in your network and provide periodic assessments as you bring new Meraki devices and any other on-premise or cloud devices into your network. And, they'll work with your teams to remediate segmentation or zero-trust policy violations so you can meet your internal and external compliance requirements.

Contact us today and we'll show you how you can get the visibility, validation and verification you need.

REDSEAL SHOWING UNINTENDED ACCESS TO AND FROM MERAKI DEVICES


DMZ
AWS VPC
VMWare NSX
Remote Worker
Cisco ACI
MERAKI Z SERIES FIREWALLS
Wireless
Remote Worker
MSFT Azure
Partners
Data Center