BACKBOX
SOLUTION BRIEF

CISCO

Cisco Meraki and BackBox Integrated Network Cyber Resilience Solution

Trusted Network and Security Device Automation

Solution Highlights

- View your entire device infrastructure lifecycle through a single platform solution.
- Ensure configuration compliance (NIST, CIS) across all vendors.
- Develop and implement automation workflows across Meraki, traditional Cisco, Fortinet, and others.
- Vulnerability intelligence aids in simplifying the CVE review, prioritization, and remediation process.

The Challenge

Modern enterprise networks are exceedingly complex and require constant adjustments to maximize uptime and minimize vulnerabilities. The diversity of device types and vendors worsens this complexity, presenting a more challenging situation for network visibility, security, and compliance, particularly with the emergence of cloud-managed network environments like Cisco Meraki.

Additionally, managing Meraki devices at scale can be challenging due to limited control over device imports and the need to ensure compliance before deployment. Without proper validation, non-compliant configurations may be pushed into production, resulting in security risks and operational disruptions.

The Solution

To tackle these challenges, organizations need a trusted network cyber resilience platform that can make repetitive network tasks efficient and reliable, work with existing network architecture and operations — on-prem and cloud-managed — and scale for enterprise and MSP deployments.

BackBox delivers this with a unified view of cloud and on-prem network infrastructure, with one platform to help achieve visibility and compliance.

- Easily configure Meraki integration settings within BackBox.
- Schedule regular device imports while specifying which Meraki device types to include.
- Import devices into a staging environment to validate compliance before moving to an actively managed environment.
- Identify orphaned devices (previously imported but no longer found within the Meraki Dashboard) to ensure inventory accuracy.
- Validate Meraki device configs against industry standards (NIST, CIS) or custom policies.
- Interrogate the security of Meraki devices to surface CVE workaround and mitigation guidance.

Use Case 1

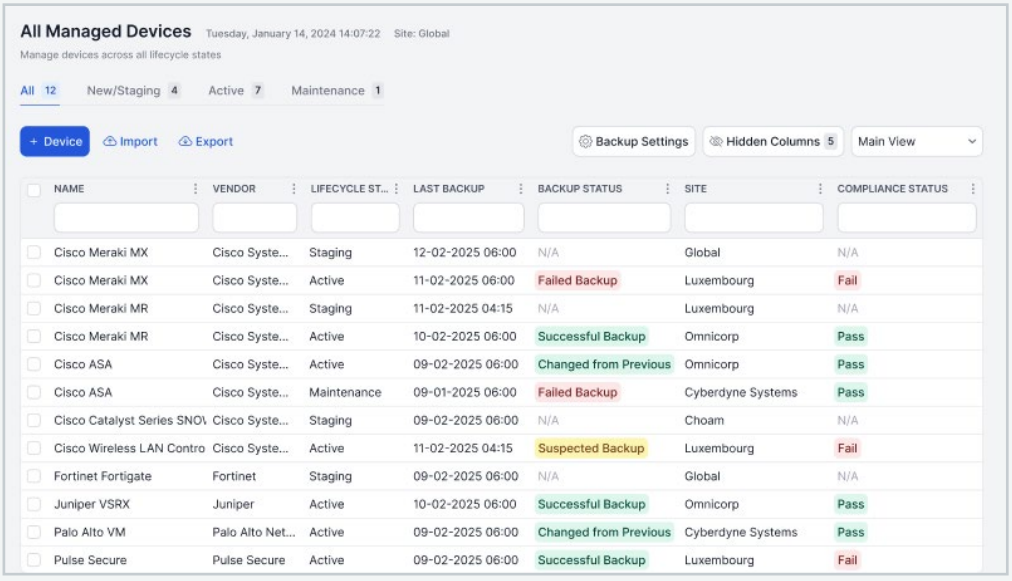
MERAKI DEVICE LIFECYCLE WORKFLOW MANAGEMENT

Challenge:

Network and security teams have built, tailored, and tweaked their device lifecycle management workflows. Now they are integrating their Meraki devices into the current processes, which is challenging, especially if their device lifecycle management workflows lack maturity.

Solution:

BackBox knows the modern network better than anyone. With support for over 180 network device vendors — on-prem and cloud-managed — users can implement a device lifecycle management workflow that matches every vendor, no matter the environment.



Use Case 2

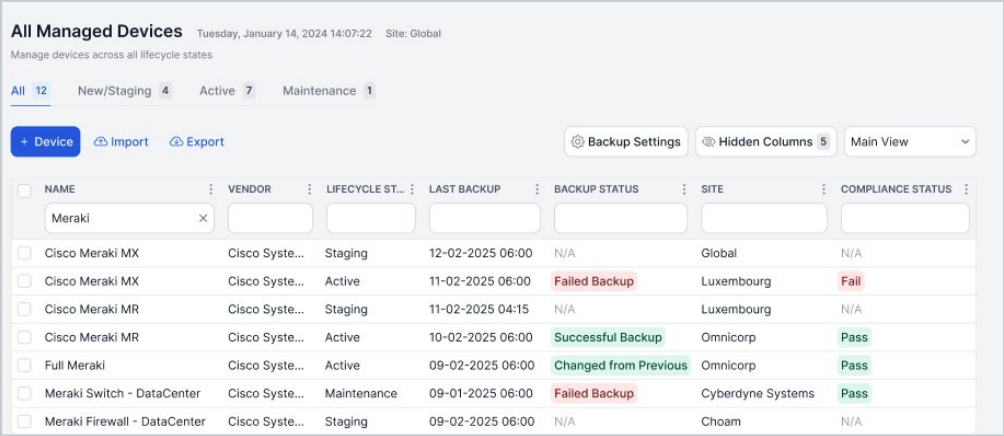
ENFORCE COMPLIANCE WITH INTERNAL POLICIES & INDUSTRY BENCHMARKS

Challenge:

With Building, maintaining, scheduling, and analyzing compliance results at scale is difficult. This is especially true because configuration updates are more frequent due to the acceleration of new threats and malicious actors.

Solution:

BackBox eliminates the need for manual checks of device configuration compliance by providing contextually aware automation templates. This streamlines the process, reduces risk, and ensures that configurations for Cisco Meraki devices and other vendors align with best practices. Users can easily trigger any automation (backups, automated tasks, compliance checks) using SNMP traps or Syslog messages for greater control and flexibly. These can run daily or at their preferred frequency. Administrators are notified of configuration drift and can automatically remediate to restore organizational compliance.



Use Case 3

SIMPLIFY CVE REVIEW, PRIORITIZATION, AND REMEDIATION

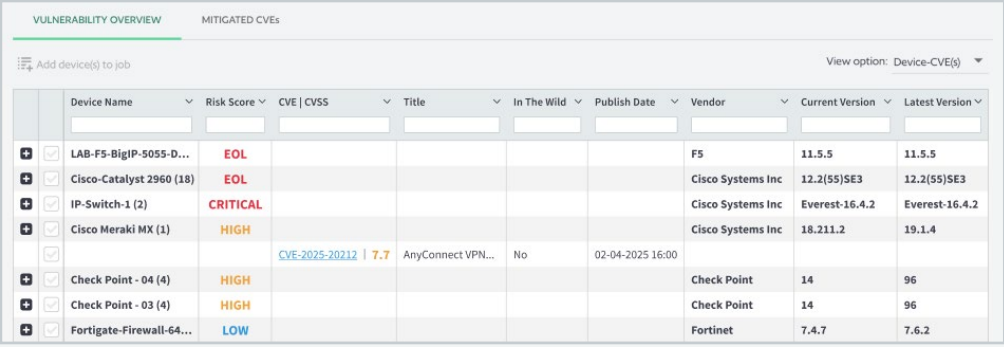
Challenge:

Every month, network security admins receive thousands of CVEs and data from CISA and device vendor sites. They must determine which CVEs are relevant for each device, both on-prem and cloud-managed. Then, they review the extensive list of CVE data to assess its organizational impact and prioritize based on active vulnerability exploitation. Once they decide which CVEs to address, they make necessary OS updates and configuration changes. This entire process is manual, prone to errors, complicated, and time-consuming.

Solution:

BackBox vulnerability intelligence turns raw vulnerability data into insights, helping you take action to reduce remediation effort and time while increasing its efficacy and accuracy.

- **Discovery and Mapping:** BackBox models your network's configuration inventory and maps it to a threat intelligence feed using CVEs to evaluate the threat level.
- **Risk Level and Analyticss:** Risk level, update recommendations, and end-of-life information are utilized to propose automations that address vulnerabilities, helping prioritize device patching according to network risk.
- **CVE Mitigation:** Search device configuration files for specific vulnerable configurations to assess the relevance of any given CVE. If a vulnerability is identified, it can be mitigated through automation.
- **Remediation Prioritized by Risk Analysis:** Risk analysis data establishes consensus and offers a comprehensive overview of the priority for vulnerability patching, while pre-built automations facilitate the deployment of updates.



BACKBOX

About BackBox

Over 500 enterprises worldwide trust BackBox as their preferred network cyber resilience platform. BackBox supports network devices from over 180 vendors, offering thousands of pre-built automations and a no-code way to create new ones. BackBox empowers teams with the confidence to automate critical network processes, maintain business continuity during disruptions, and recover swiftly. From backups and OS updates to configuration compliance and vulnerability management, BackBox ensures that automations deliver consistent, reliable outcomes.

To learn more, visit backbox.com

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide technology leader that is revolutionizing the way organizations connect and protect in the AI era. For more than 40 years, Cisco has securely connected the world. With its industry leading AI-powered solutions and services, Cisco enables its customers, partners and communities to unlock innovation, enhance productivity and strengthen digital resilience. With purpose at its core, Cisco remains committed to creating a more connected and inclusive future for all.

Discover more, visit cisco.com