

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

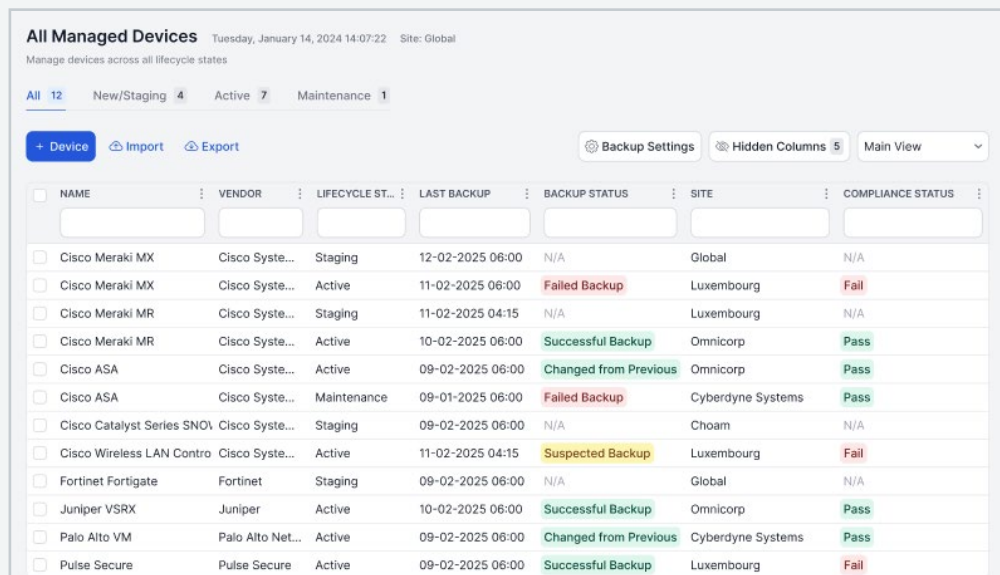
MERAKI DEVICE LIFECYCLE WORKFLOW MANAGEMENT

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.



The screenshot displays the 'All Managed Devices' dashboard. At the top, it shows the date and time (Tuesday, January 14, 2024 14:07:22) and the site (Global). Below this, there are filters for device counts: All 12, New/Staging 4, Active 7, and Maintenance 1. There are also buttons for '+ Device', 'Import', and 'Export', along with 'Backup Settings', 'Hidden Columns 5', and 'Main View' dropdown. The main table lists various devices with their respective vendors, lifecycle states, last backup times, backup statuses, sites, and compliance statuses.

NAME	VENDOR	LIFECYCLE ST...	LAST BACKUP	BACKUP STATUS	SITE	COMPLIANCE STATUS
<input type="checkbox"/> Cisco Meraki MX	Cisco Syste...	Staging	12-02-2025 06:00	N/A	Global	N/A
<input type="checkbox"/> Cisco Meraki MX	Cisco Syste...	Active	11-02-2025 06:00	Failed Backup	Luxembourg	Fail
<input type="checkbox"/> Cisco Meraki MR	Cisco Syste...	Staging	11-02-2025 04:15	N/A	Luxembourg	N/A
<input type="checkbox"/> Cisco Meraki MR	Cisco Syste...	Active	10-02-2025 06:00	Successful Backup	Omnnicorp	Pass
<input type="checkbox"/> Cisco ASA	Cisco Syste...	Active	09-02-2025 06:00	Changed from Previous	Omnnicorp	Pass
<input type="checkbox"/> Cisco ASA	Cisco Syste...	Maintenance	09-01-2025 06:00	Failed Backup	Cyberdyne Systems	Pass
<input type="checkbox"/> Cisco Catalyst Series SNOI	Cisco Syste...	Staging	09-02-2025 06:00	N/A	Choam	N/A
<input type="checkbox"/> Cisco Wireless LAN Contro	Cisco Syste...	Active	11-02-2025 04:15	Suspected Backup	Luxembourg	Fail
<input type="checkbox"/> Fortinet Fortigate	Fortinet	Staging	09-02-2025 06:00	N/A	Global	N/A
<input type="checkbox"/> Juniper VSRX	Juniper	Active	10-02-2025 06:00	Successful Backup	Omnnicorp	Pass
<input type="checkbox"/> Palo Alto VM	Palo Alto Net...	Active	09-02-2025 06:00	Changed from Previous	Cyberdyne Systems	Pass
<input type="checkbox"/> Pulse Secure	Pulse Secure	Active	09-02-2025 06:00	Successful Backup	Luxembourg	Fail

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 flexibility. These can run daily or at their preferred frequency. Administrators are notified of configuration drift and can automatically remediate to restore organizational compliance.

All Managed Devices Tuesday, January 14, 2024 14:07:22 Site: Global
Manage devices across all lifecycle states

All 12 New/Staging 4 Active 7 Maintenance 1

+ Device Import Export Backup Settings Hidden Columns 5 Main View

NAME	VENDOR	LIFECYCLE ST...	LAST BACKUP	BACKUP STATUS	SITE	COMPLIANCE STATUS
Meraki						
Cisco Meraki MX	Cisco Syste...	Staging	12-02-2025 06:00	N/A	Global	N/A
Cisco Meraki MX	Cisco Syste...	Active	11-02-2025 06:00	Failed Backup	Luxembourg	Fail
Cisco Meraki MR	Cisco Syste...	Staging	11-02-2025 04:15	N/A	Luxembourg	N/A
Cisco Meraki MR	Cisco Syste...	Active	10-02-2025 06:00	Successful Backup	Omnicorp	Pass
Full Meraki	Cisco Syste...	Active	09-02-2025 06:00	Changed from Previous	Omnicorp	Pass
Meraki Switch - DataCenter	Cisco Syste...	Maintenance	09-01-2025 06:00	Failed Backup	Cyberdyne Systems	Pass
Meraki Firewall - DataCenter	Cisco Syste...	Staging	09-02-2025 06:00	N/A	Choam	N/A

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 Analytics:** 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.

VULNERABILITY OVERVIEW MITIGATED CVEs

Add device(s) to job View option: Device-CVE(s)

Device Name	Risk Score	CVE CVSS	Title	In The Wild	Publish Date	Vendor	Current Version	Latest Version
LAB-F5-BigIP-5055-D...	EOL					F5	11.5.5	11.5.5
Cisco-Catalyst 2960 (18)	EOL					Cisco Systems Inc	12.2(55)SE3	12.2(55)SE3
IP-Switch-1 (2)	CRITICAL					Cisco Systems Inc	Everest-16.4.2	Everest-16.4.2
Cisco Meraki MX (1)	HIGH	CVE-2025-20212 7.7	AnyConnect VPN...	No	02-04-2025 16:00	Cisco Systems Inc	18.211.2	19.1.4
Check Point - 04 (4)	HIGH					Check Point	14	96
Check Point - 03 (4)	HIGH					Check Point	14	96
Fortigate-Firewall-64...	LOW					Fortinet	7.4.7	7.6.2



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