BACKBOX
SOLUTION BRIEF

Securing Modern Networks

Unified View to Enhance Network Visibility, Security, and Compliance

Solution Highlights

- A single source of truth for assets is crucial to building a robust and adaptable cyber resilience framework.
- Correlate known vulnerabilities with your network device inventory, prioritize them by risk, and reduce remediation effort and time.
- Proactive device checks ensure compliance with industry standards (NIST, CIS) or custom policies, automatically resolving issues before they affect the network.
- Utilize a comprehensive automation library with over 3,000 prebuilt automations for various devices and environments, enhancing team efficiency.

The Challenge

As digital transformation accelerates and remote work becomes the norm, businesses are adopting a distributed workforce that relies on diverse network environments, including physical and virtual devices from various vendors across cloud and on-premises infrastructure.

There has been a significant shift in Secure Access Service Edge (SASE), moving networking into the software layer through a software-defined network approach (SDN). Device configuration management is now cloud-based and dynamically pushed to devices, meaning security is managed in two separate locations.

The diversity of device types and vendors complicates network visibility, security, and compliance, especially in cloud-managed environments. This expands the attack surface for threat actors, increasing the risk of unnoticed vulnerabilities and attacks.

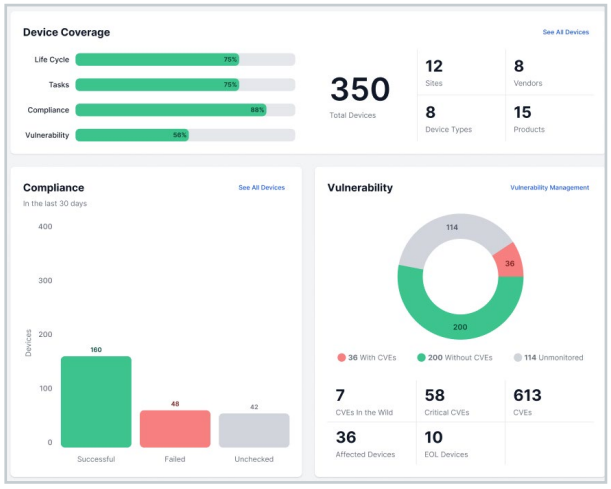
- **Cyber Resilience is Complex:** On-prem and cloud technologies must coexist to support remote work, but ensuring cyber resilience across modern networks is challenging without a centralized system.
- **Too Many Tools:** Enterprises struggle with managing various tools — cloud services, security applications, and data security plans — while often overlooking the vital network infrastructure that supports them.
- **Limited Visibility:** Many organizations lack visibility into their diverse networks and configurations, needing a unified view to improve security and compliance.

The Solution

BackBox provides a straightforward method to continuously enhance network cyber resilience through centralized, automated security, compliance, and lifecycle management for all network devices, whether on-premises or cloud-managed. This offers organizations improved visibility, compliance, and security while saving time, money, and resources.

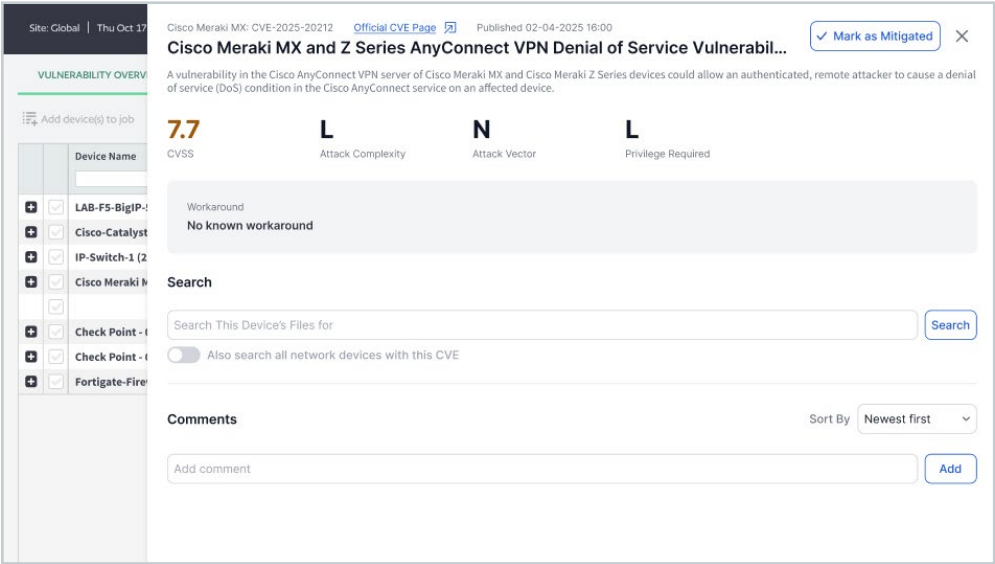
Unified View for a Consistent Experience

Realizing the importance of a comprehensive view and a single source of truth for assets is essential for building a robust and adaptable cyber resilience framework. BackBox provides a unified view of modern network infrastructure to help ensure visibility, security, and compliance.



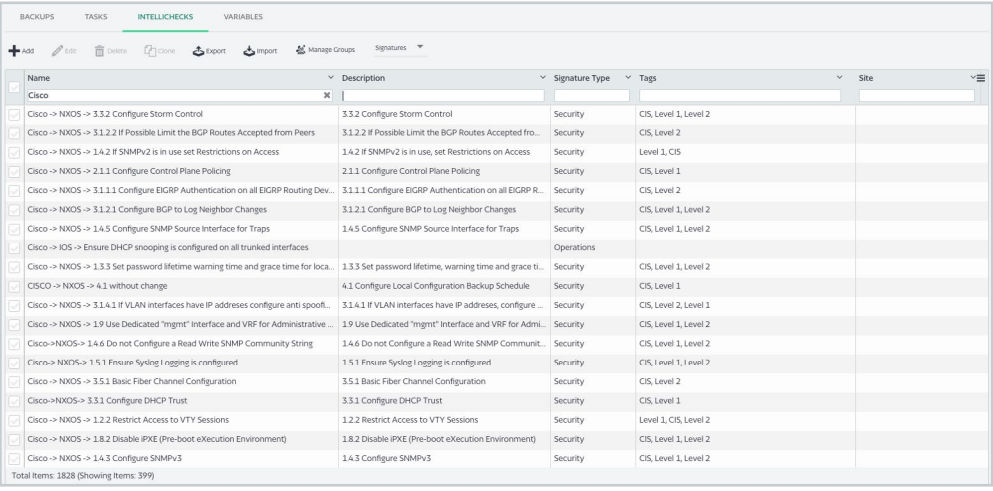
Multi-vendor Vulnerability Intelligence

Only BackBox transforms raw vulnerability data into actionable insights. We correlate known vulnerabilities with your network device inventory — whether on-prem or cloud-managed — prioritize these vulnerabilities based on risk, and assist you in reducing the remediation effort and time.



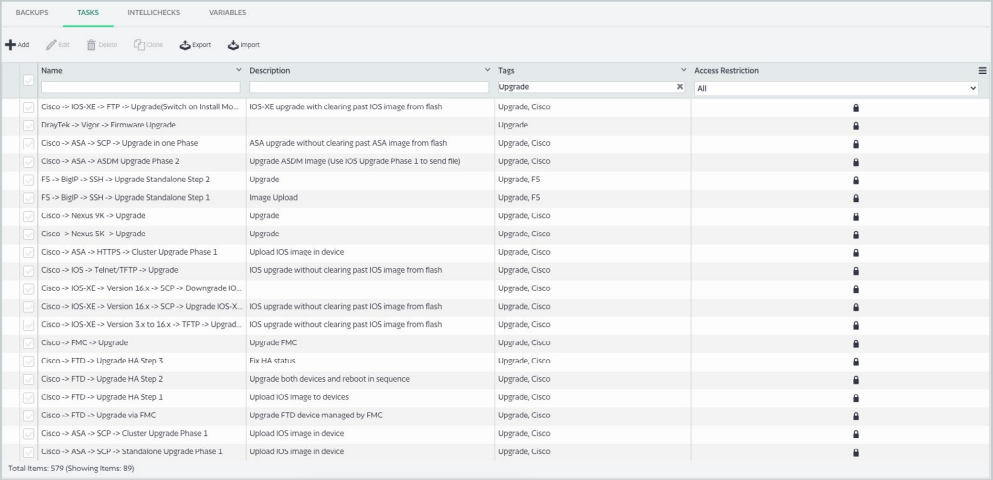
Enforce Configuration Compliance

Validate device configurations against industry standards (NIST, CIS) or custom policies. BackBox has you covered—it automates configuration audits and drift remediation across all your network devices, whether on-prem or cloud-managed.



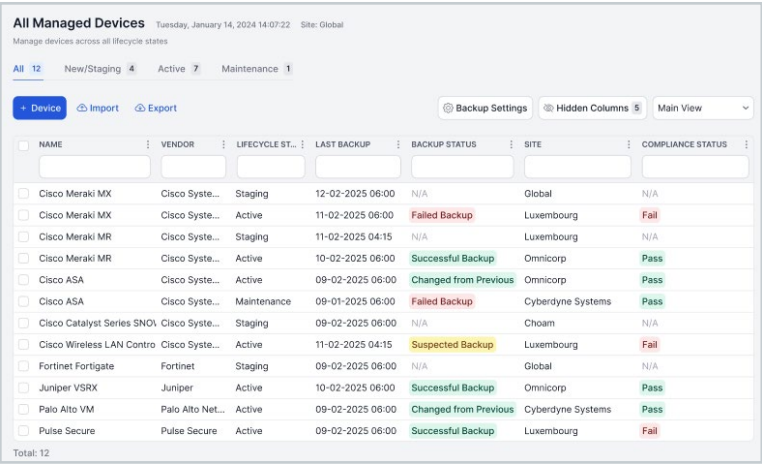
Automation Workflows Across All Devices & Environments

BackBox integrates seamlessly into standard workflows, allowing you to quickly open trouble tickets, resolve compliance violations, and streamline compliance audits, ensuring smooth and secure operations.



Visibility Into Your Full Infrastructure Lifecycle

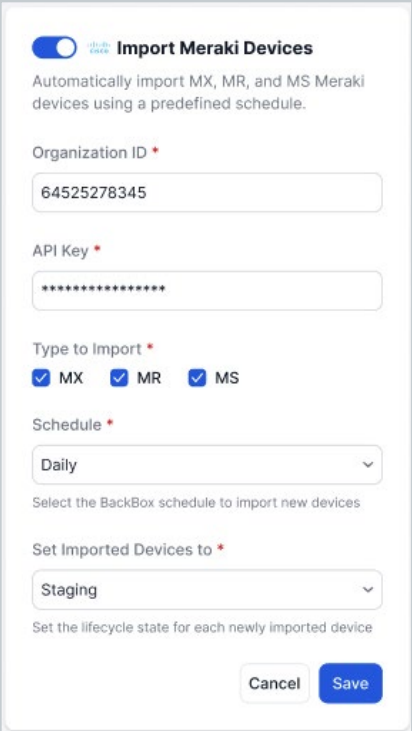
BackBox provides comprehensive lifecycle state management for your modern network infrastructure, enabling teams to onboard, promote, and manage devices throughout the entire network. Lifecycle states such as Staging, Actively Managed, Maintenance, and Ignored are available directly in device metadata and support automation behavior, compliance checks, and license allocation.



SASE Integration

Our integration with Cisco Meraki MX, MR, and MS devices captures inventory details and configuration parameters available through the Meraki portal to simplify operational tasks. This integration allows users to:

- Manage Meraki devices alongside other network infrastructure devices using a single platform.
- Effortlessly adjust Meraki integration settings within BackBox.
- Schedule regular device imports, specifying which Meraki device types to include.
- Import devices into a staging environment to validate compliance prior to deployment in production.
- Identify orphaned devices (previously imported but no longer present) to ensure inventory accuracy.
- Validate Meraki device configurations against industry standards (NIST, CIS) or custom policies.
- Detect and identify vulnerabilities in Meraki devices and take proactive measures.



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**