BACKBOX
SOLUTION BRIEF

Automating Zero Trust for Modern Networks

Key Controls Simplify Zero Trust Alignment for Network Operations

Solution Highlights

- Manage administrator rights and ensure consistent processes using role-based access controls integrated with credential vaults and tied to automations.
- Centralize audit and permission rights with role-based access controls, immutable logs, session replay, and rollback capabilities.
- Automate configuration compliance and vulnerability management during the onboarding process.
- Continuously assess and enforce configuration compliance and vulnerability remediation, providing rich reporting to demonstrate Zero Trust alignment.

The Challenge

Zero trust is a well-known term for an evolving set of cybersecurity paradigms that shift defenses from static, network-based perimeters to focus on users, assets, and resources. This shift to continually assess risk and trust levels based on identity and context is becoming increasingly ubiquitous as organizations transition to modern network environments that include both physical and virtual devices across cloud and on-premises infrastructure.

Most organizations have a Zero Trust strategy led by cybersecurity teams. Increasingly, IT leaders, including network teams, are being asked to implement Zero Trust concepts into their network infrastructure and operations. Nearly one-third of enterprises cite Zero Trust security as a major driver of their overall approach to network operations.

Network teams understand secure remote access, network segmentation, and the impact of Zero Trust on network performance. However, the complexity of modern networks and fragmented tools hinders their ability to influence and engage in Zero Trust projects.

- **Diverse Network Environments:** Implementing Zero Trust principles across a combination of on-prem and cloud-managed environments with consistency requires a unified view that integrates Secure Access Service Edge (SASE) with on-prem network observability.

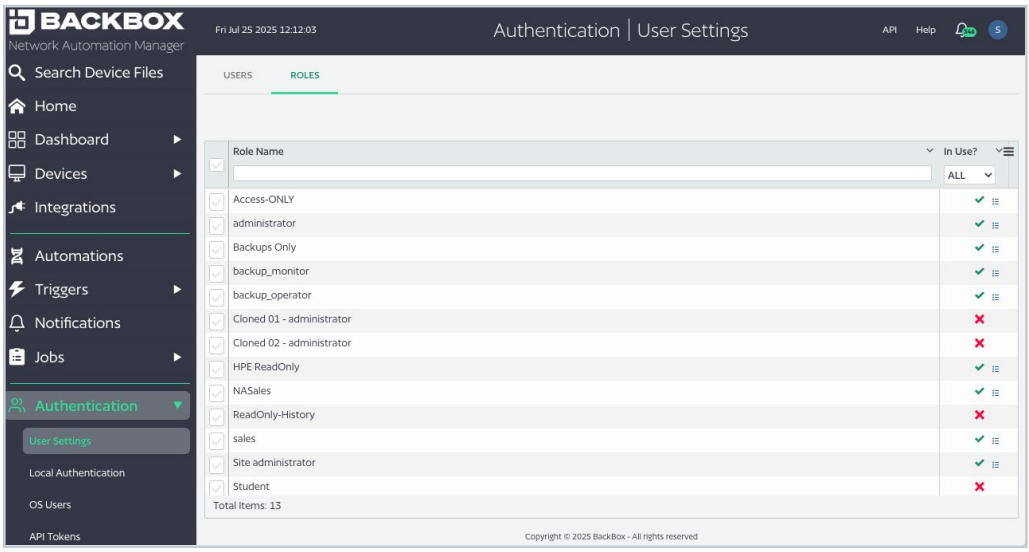
- **Too Many Devices and Tools:** Network engineers must support both new and older network devices from various vendors simultaneously, which makes it incredibly difficult to piece together an accurate assessment of risk and trust to enforce network resilience.

The Solution

BackBox simplifies Zero Trust for network teams, enabling key controls around network devices and an easy way to automate them, ensuring risk and trust are continuously assessed and resilience is seamlessly enforced from onboarding to daily operations.

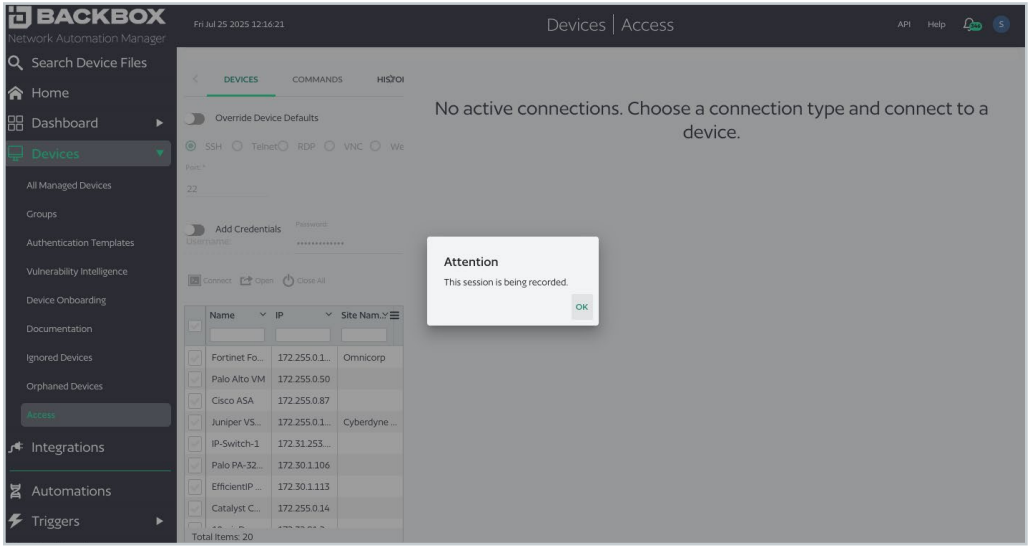
CONSISTENT ACCESS MANAGEMENT

Manage administrator rights and compliance through role-based access controls integrated with credential vaults and tied to automations. Administrators can have access associated with the right automations for their role, allowing them to standardize processes for device management and perform their jobs with consistency.



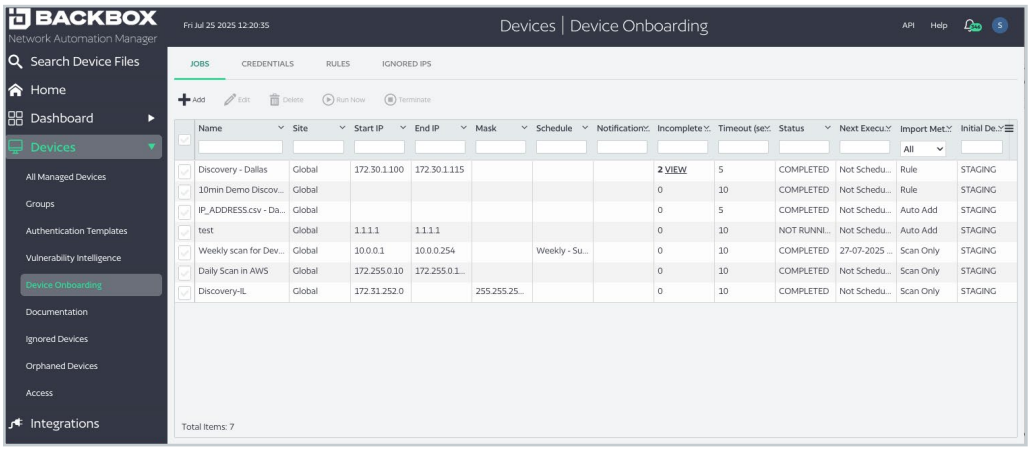
CENTRALIZED AUDIT AND CONTROL

BackBox offers a centralized location to audit and record administrator sessions for compliance. All network device changes are logged to an immutable record, with the ability to record sessions for replay and roll back changes from this centralized access point as needed.



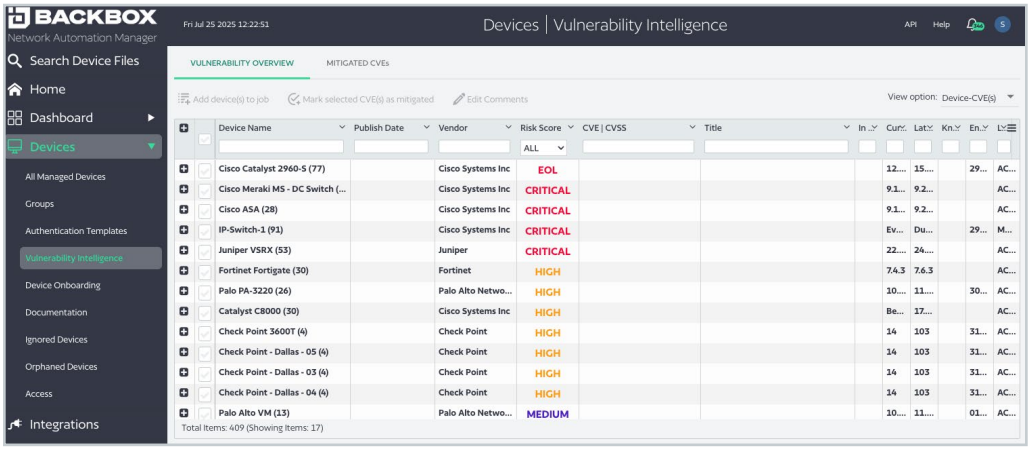
COMPLIANT ONBOARDING

BackBox automatically checks devices during onboarding to verify that configurations align with company policies. Non-compliant devices are automatically enforced with policies. Automated remediation reduces manual errors and speeds up onboarding new devices to the network.



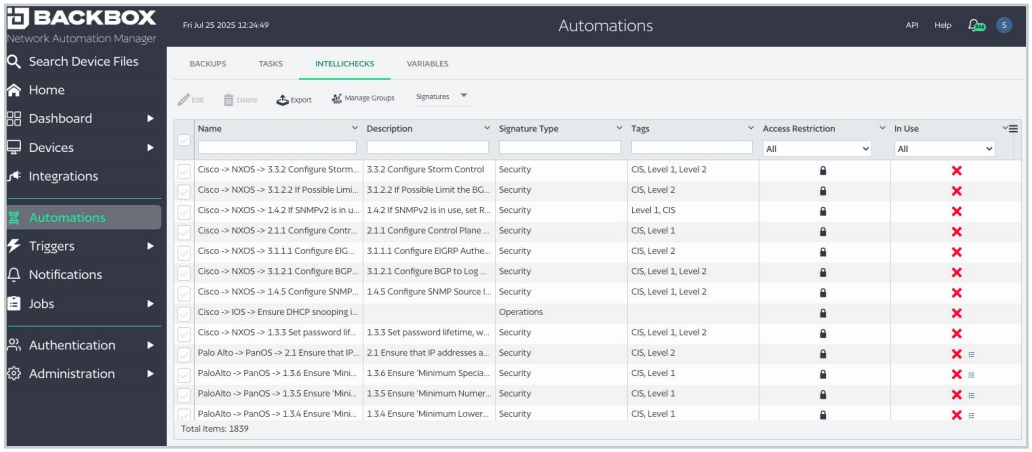
PROACTIVE VULNERABILITY REMEDIATION

During the onboarding process, devices are checked for known vulnerabilities. Based on vulnerability intelligence and recommended actions, patches, updates, or workarounds can be implemented before adding the device to the network to remediate the issue proactively.



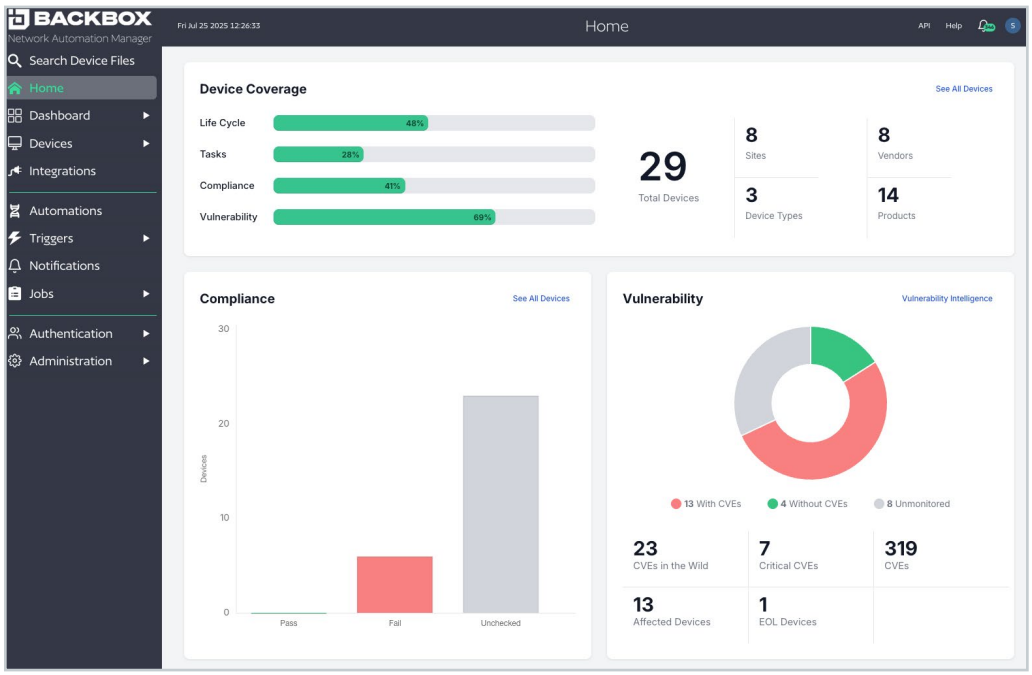
SMART ASSESSMENT

BackBox continuously assesses devices for configuration compliance and new vulnerabilities. When configuration drift is detected, configurations can be automatically groomed into compliance, or notifications can be sent to alert administrators of non-compliance. Similarly, as new vulnerabilities are discovered and prioritized for remediation, they can be patched or devices can be updated, based on vendor recommendations.



UNIFIED VISIBILITY AND REPORTING

Rich reporting and visibility ensure that teams communicate and are aware of the steps taken to protect the network. Reports can be configured to highlight actionable data, helping security and networking teams keep the network aligned with Zero Trust principles.



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**