# BACKBOX
## SOLUTION BRIEF

**CHECK POINT**

# Check Point and BackBox Integrated Network Cyber Resilience Solution

---

Trusted Network and Security Device Automation

## Solution Highlights

- Automate OS updates and vulnerability patches for Check Point devices across your network in a timely manner, to prevent exposure to known vulnerabilities. This includes automating multistep updates and support for older devices.

- Automate the backup process for Check Point Next Generation Firewalls (NGFWs) and other security devices. Each backup is validated to ensure its integrity, allowing for a one-click restoration. Backups and restores become so simple that they can easily be incorporated into any potentially destructive automation for rapid recovery.

- Backups can be stored off-site and encrypted with a longer history of backups saved to help with troubleshoot or in the event of an undetected vulnerability.

- Provide comprehensive support for CIS Benchmark compliance out-of-the-box, including an initial gap analysis, continuous automated configuration audit, drift prevention, reporting, and optional automated remediation.

- Ensure your CMDB is always up-to-date and that security vulnerabilities don't go undetected with Dynamic Inventory capabilities.

## The Challenge

Modern enterprise-class networks are highly complex and require continuous updates to maximize uptime and minimize vulnerabilities. This complexity is exacerbated by the pace of change within networks to support new applications and services for businesses and their customers. Manually configuring all network and security devices to ensure business continuity can often be challenging, time-consuming, and prone to human error.

In fact, 92% of our customers say they face more updates to their networks than they can accomplish.

Network and security devices require constant OS updates, patches, and configuration changes to protect from vulnerabilities and be cyber resilient. Failure to perform these updates in a timely manner exposes the network to security threats and the potential for costly downtime. Similarly, in the absence of regular backups, which often happens when backups are complex to perform or require manual steps, networks experience slower recovery from downtime following outages.

## The Solution

To tackle these challenges, organizations need a trusted automation platform that can efficiently and reliably perform repetitive network administration tasks, work with existing network architecture and operations, and scale for both enterprise and Managed Service Provider (MSP) deployments.

BackBox delivers such a platform with out-of-the-box capabilities for backup, OS updates, compliance auditing and auto-remediation, Dynamic Inventory Reporting, and closed-loop management of vulnerability patching.

## Check Point and BackBox Integrated Solution

The Check Point and BackBox solution provides automated backup and single-click recovery of Check Point NGFWs and other devices, eliminating the need for time-consuming and error-prone manual processes or creating and managing in-house scripts.

BackBox Dynamic Inventory collects granular asset information from Check Point NGFWs and other devices and then reports on inventory information, including license information, device model, serial numbers, and more. Inventory information can also be passed to other systems, like an ITSM or CMDB, via the BackBox API.

BackBox allows users to change operating system-level parameters on multiple devices with one click. This enables the delgation of administrative tasks to individuals who do not require full policy access which helps reduce the risk of human errors that can lead to costly downtime.

BackBox also provides seamless integration to verify that Check Point devices are configured in alignment with internal and industry security policies and regulations, such as CIS Benchmarks, and can automatically remediate configuration drift.

**| BENEFITS OF THE COMBINED SOLUTION:**

- Automated OS updates of Check Point devices to protect from vulnerabilities, even when updates require multiple steps to complete.
- Automated, validated backups for Check Point devices.

- Single-click restore and disaster recovery.
- Validation and automatic remediation of configurations against policies and regulations.
- Automated discovery of newly connected Check Point devices for easy asset management.

# BackBox Network Cyber Resilience Platform

BackBox is the most trusted network automation platform, focused on automating network security and operations at scale for enterprises and Managed Service Partners.

Flexible automation empowers our customers to enhance the health, performance, and security of over 100,000 networks worldwide.

We believe network automation should be easy and reliable, providing customers unprecedented time savings and reduced risk.

# Check Point Quantum™ Network Security

Check Point Quantum Next Generation Firewall Security Gateways enable enterprises to deploy the industry-leading threat prevention capabilities at all infrastructure points, scaling security with Maestro Hyperscale according to their changing business needs. This enables enterprises to prevent even advanced, zero-day attacks before they can disrupt business.

Check Point Maestro brings scale, agility, and elasticity of the cloud on premise with efficient N+1 clustering based on Check Point HyperSync technology, maximizing the capabilities of your existing security gateways. Users can create their own virtualized private cloud on premise by stacking multiple Check Point security gateways together. Group them by security feature set, policy, or the assets they protect and further virtualize them with virtual systems technology.

# Use Case 1

**CENTRALIZE AND AUTOMATE OS UPDATES AND VULNERABILITY PATCHES**

**Challenge:**

OS updates and patch management are a critical aspect of maintaining network security. The versions of OS that run on the network infrastructure must be closely managed to ensure continuity of service and remediation of known security vulnerabilities. However, manually keeping track of the frequent OS updates and patches of firewalls and other network and security devices is getting more challenging, especially with limited resources.

**Solution:**

BackBox offers automated OS updates and patches for Check Point Quantum NGFWs and will do the same for network and security devices from 180 other vendors, all from a centralized location. This eliminates the need to hop from one tool to another to update different devices, saving time and resources. With a single click, users can use BackBox to update the OS of Check Point devices alongside hundreds of devices seamlessly.

# Use Case 2

**ENFORCE COMPLIANCE WITH CIS BENCHMARKS**

**Challenge:**

With configuration updates getting more frequent due to the acceleration of new threats and malicious actors, ensuring all security and network devices, such as firewalls, are up-to-date and compliant with CIS Benchmarks, internal policies, and industry regulations is challenging.

**Solution:**

Eliminating the need to check device configuration for compliance manually, BackBox provides contextually-aware automation templates that remove the drudgery and reduce risk by validating that a specific configuration for Check Point devices meets best practices, and can automatically remediate those that do not. Rechecks can be scheduled to run daily or at whatever frequency desired. Administrators receive notifications of configuration drift to manually correct or can auto-remediate to bring the organization back into compliance.

# Use Case 3

**AUTOMATE BACKUPS**

**Challenge:**

Manual  backups for network and security devices like firewalls are time-consuming and prone to human error. In addition to security infrastructure, network engineers must perform regular backups on routers, switches, and other network devices from multiple vendors, via numerous user interfaces, further increasing risk.

**Solution:**

Seamless integration between BackBox and Check Point devices enables automated, centralized, and secure backups for all configuration information from Check Point devices and devices from other vendors. This ensures rapid recovery and minimal downtime.

**BACKBOX**

# About BackBox

More than 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 Check Point

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to
governments and corporate enterprises globally. Its solutions protect customers from cyber-
attacks with an industry leading catch rate of malware, ransomware and other types of attacks.
Check Point offers a multilevel security architecture that defends enterprises' cloud, network
and mobile device held information, plus the most comprehensive and intuitive one point of
control security management system. Check Point protects over 100,000 organizations of all
sizes.

Learn more at **www.checkpoint.com**