BACKBOX
SOLUTION BRIEF

Automate CIS Compliance with BackBox

Ongoing, Automated Configuration Audit, Remediation, and Drift Prevention

Overview

The Center for Internet Security (CIS) Benchmarks™ are vendor-specific configuration recommendations to help organizations reduce risk and demonstrate compliance with various government and industry regulations. Network operations and network security teams use the recommendations and best practices to safeguard devices against today's evolving cyber threats that exploit vulnerabilities to exfiltrate data and disrupt operations.

Implementing these guidelines typically requires significant manual and administrative work with a strong potential for human error. For every single device, every step in the process requires manual intervention – from checking configurations for compliance to remediating when needed, creating reports, and staying current with updates. In single-vendor environments, CIS compliance is unwieldy, but in multi-vendor environments, it can become overwhelming quickly.

Fortunately, there's a better way for network operations teams and service providers of all types to keep networks up to date on the latest CIS guidelines.

AUTOMATION ADVANTAGE

- **Teams accelerate CIS compliance** with the ability to quickly download automation templates into the BackBox Automation Library and complete CIS Benchmark checks in under a minute.
- **Teams maintain compliance** and prevent configuration drift with contextually-aware, automated rechecks, remediations, and updates.
- **Teams respond faster to compliance audits** with comprehensive, detailed reporting.
- **Teams increase bandwidth** to focus on more strategic initiatives by reducing manual work and the potential for errors.

Let's look at a typical scenario of applying CIS Benchmarks without BackBox and compare that process to what it's like with BackBox.

Without BackBox

Using Check Point as an example, the CIS Benchmark for Check Point Firewall is a 118-page document with more than 40 Level 1 configuration profiles. Achieving and maintaining CIS compliance is tedious, time-consuming, and error-prone.

Network engineers must manually:

- Sort through the document and long list of checks, develop a tracking spreadsheet, check every device for compliance with the configuration guidelines, and update the spreadsheet.
- If a device is not compliant, remediate the device and update the spreadsheet.
- Recheck every device regularly to ensure compliance is maintained and remediate as needed.
- Export data from the spreadsheet and manually compile reports to validate and report on compliance.
- Download the updated CIS Benchmark, revise the spreadsheet, run the updated CIS checks, remediate the device, and update the spreadsheet every time Check Point updates a device.

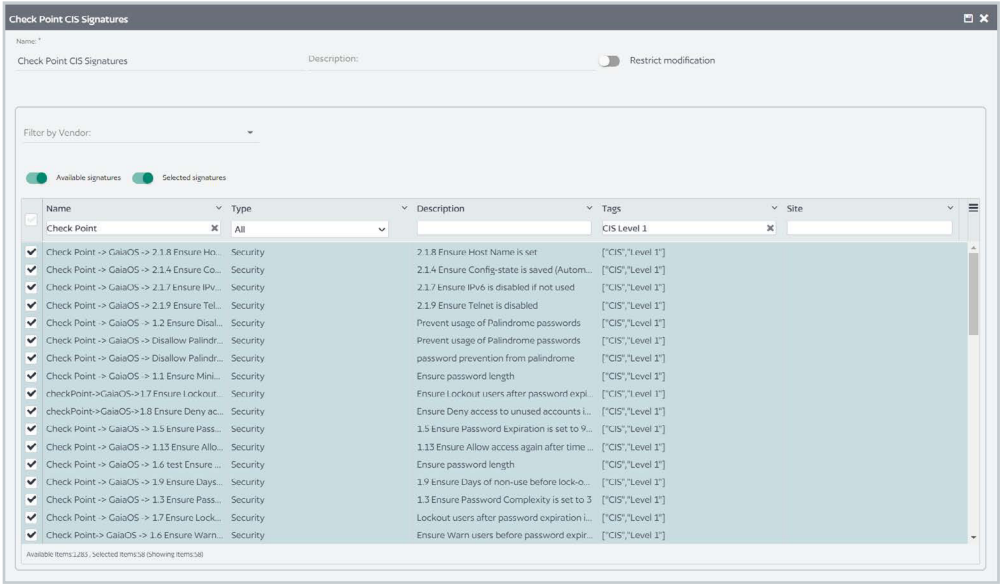
Even in a single-vendor environment, depending on the number of devices, the process can become incredibly complex and a headache to manage. Some organizations may choose to build their automations for CIS checks. But supporting these automations may not be scalable as a business or an operator typically won't have the capacity also to automate remediations and support updates.

Now imagine a multi-vendor environment that requires creating and maintaining this process across devices from various vendors, and introduces the added complexity of having to check multiple dashboards and compile disparate reports into a single, comprehensive report. Confidently say the organization is CIS compliant typically requires a massive investment of time and resources. So, organizations are sometimes in the difficult position of prioritizing the devices they maintain based on their risk profile and budget and hope for the best.

With BackBox

BackBox has turned CIS's 118-page Check Point Firewall Benchmark document into approximately 40 contextually aware automations focused on key device types. These automations remove the drudgery and reduce risk by validating that a specific configuration meets CIS best practices and can automatically remediate those that do not. From a single pane of glass console, network engineers simply:

- Download the automation templates into the Automation Library, and either load them via API or import the file from the UI.
- Select the CIS checks for the devices in their environment, give the group a name, and save it.



- Launch an automated procedure to run checks periodically on a schedule they set and send notifications when devices drift out of compliance.
- Turn on automated remediation if they choose.
- Click to run a unified report to demonstrate compliance of devices, even across multi-vendor environments.

Organizations can confidently report on CIS compliance because all checks and status updates are in one place and easy to see. BackBox also updates the relevant automations whenever a vendor updates a device, and CIS updates the Benchmarks, so CIS checks are always current.

In the case of Check Point, BackBox automation templates cover 90.5% of CIS Level 1 configuration recommendations (three CIS actions must be completed manually). That's a 90% time savings over manual methods.

In addition to Check Point, BackBox offers CIS Automation Templates for Cisco, F5, Fortinet, Juniper, Palo Alto, and others.

CONTROL WHERE IT NEEDS TO BE – A REAL WORLD SCENARIO

Alignment with CIS best practices is not just about the execution of the check but the procedures put in place to maintain that compliance.

For instance, when an employee is no longer with a company, CIS best practice is to ensure the denial to unused accounts. But what happens when an employee's manager contacts the help desk because they need access to the former employee's account to pull some information? The help desk is focused on supporting business operations, not compliance, and provides access to the account. Likely the network engineer is not in the loop, and the organization is out of compliance until the engineer manually rechecks the device, which could be weeks or months later.

With BackBox automation templates, rechecks can be scheduled to run daily or at whatever frequency aligns with internal policies and best practices to mitigate time of exposure. Network engineers receive notifications of configuration drift and can automate remediation to bring the organization back into compliance. Control stays where it needs to be – with the teams responsible for configuration compliance and network device security.

Conclusion

BackBox eliminates the tedious, time-consuming, and error-prone activity of implementing CIS Benchmarks manually. For organizations considering building their automations, BackBox offers a sustainable, scalable, and trusted alternative by automating all aspects of compliance – not just checks, but also remediation, comprehensive reporting, and support for device updates.

From single to multi-vendor environments and from enterprises to service providers of all types, BackBox ensures device configurations are set to align with CIS best practices and, if not, can automatically bring them up to date safely and efficiently.

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**