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 take advantage of 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 that includes 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 single device for compliance with the configuration guidelines, and update

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

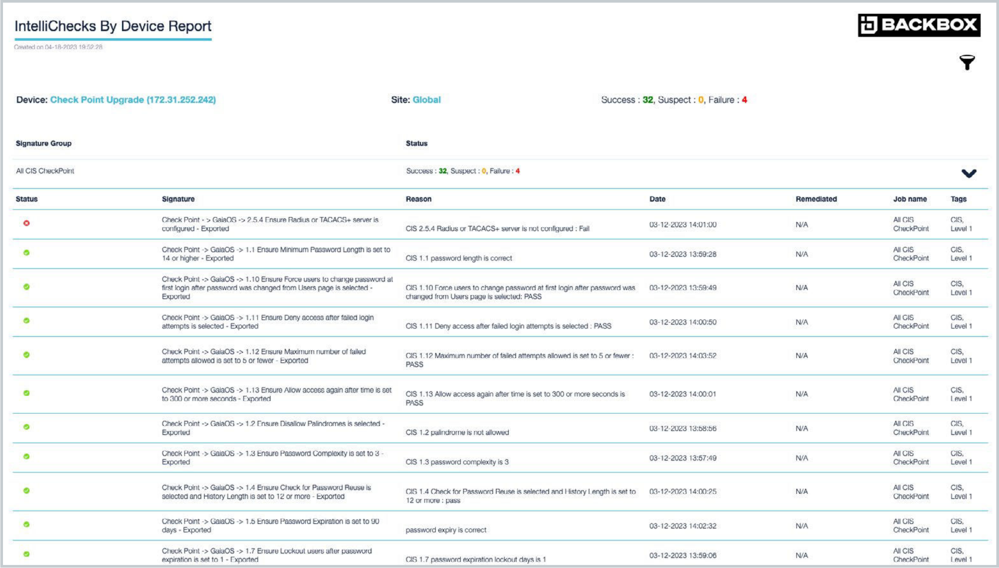
Now imagine a multi-vendor environment which requires creating and maintaining this process across devices from multiple vendors, and introduces the added complexity of having to check multiple dashboards and compile disparate reports into a single, comprehensive report. Being able to confidently say the organization is CIS compliant typically requires a massive investment of time and resources. So, organizations are sometimes in the difficult position of having to prioritize 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 file import 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.



IntelliChecks By Device Report

Created on 04-18-2023 19:52:28

Device: Check Point Upgrade (172.31.252.242) Site: Global Success : 32, Suspect : 0, Failure : 4

Signature Group	Status
All CIS CheckPoint	Success : 32, Suspect : 0, Failure : 4

Status	Signature	Reason	Date	Remediated	Job name	Tags
●	Check Point - > GaiaOS -> 2.5.4 Ensure Radius or TACACS+ server is configured - Exported	CIS 2.5.4 Radius or TACACS+ server is not configured : Fail	03-12-2023 14:01:00	N/A	All CIS CheckPoint	CIS, Level 1
●	Check Point -> GaiaOS -> 1.1 Ensure Minimum Password Length is set to 14 or higher - Exported	CIS 1.1 password length is correct	03-12-2023 13:59:28	N/A	All CIS CheckPoint	CIS, Level 1
●	Check Point -> GaiaOS -> 1.10 Ensure Force users to change password at first login after password was changed from Users page is selected - Exported	CIS 1.10 Force users to change password at first login after password was changed from Users page is selected: PASS	03-12-2023 13:59:49	N/A	All CIS CheckPoint	CIS, Level 1
●	Check Point -> GaiaOS -> 1.11 Ensure Deny access after failed login attempts is selected - Exported	CIS 1.11 Deny access after failed login attempts is selected : PASS	03-12-2023 14:00:50	N/A	All CIS CheckPoint	CIS, Level 1
●	Check Point -> GaiaOS -> 1.12 Ensure Maximum number of failed attempts allowed is set to 5 or fewer - Exported	CIS 1.12 Maximum number of failed attempts allowed is set to 5 or fewer : PASS	03-12-2023 14:03:52	N/A	All CIS CheckPoint	CIS, Level 1
●	Check Point -> GaiaOS -> 1.13 Ensure Allow access again after time is set to 300 or more seconds - Exported	CIS 1.13 Allow access again after time is set to 300 or more seconds is PASS	03-12-2023 14:00:01	N/A	All CIS CheckPoint	CIS, Level 1
●	Check Point -> GaiaOS -> 1.2 Ensure Disallow Palindromes is selected - Exported	CIS 1.2 palindrome is not allowed	03-12-2023 13:58:56	N/A	All CIS CheckPoint	CIS, Level 1
●	Check Point -> GaiaOS -> 1.3 Ensure Password Complexity is set to 3 - Exported	CIS 1.3 password complexity is 3	03-12-2023 13:57:49	N/A	All CIS CheckPoint	CIS, Level 1
●	Check Point -> GaiaOS -> 1.4 Ensure Check for Password Reuse is selected and History Length is set to 12 or more - Exported	CIS 1.4 Check for Password Reuse is selected and History Length is set to 12 or more : pass	03-12-2023 14:00:25	N/A	All CIS CheckPoint	CIS, Level 1
●	Check Point -> GaiaOS -> 1.5 Ensure Password Expiration is set to 90 days - Exported	password expiry is correct	03-12-2023 14:02:32	N/A	All CIS CheckPoint	CIS, Level 1
●	Check Point -> GaiaOS -> 1.7 Ensure Lockout users after password expiration is set to 1 - Exported	CIS 1.7 password expiration lockout days is 1	03-12-2023 13:59:06	N/A	All CIS CheckPoint	CIS, Level 1

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 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 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. It’s likely the network engineer is not in the loop and now 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. And for organizations considering building their own automations, BackBox offers a sustainable, scalable, and trusted alternative by automating all aspects of compliance – not just checks, but also remediation, comprehensive reporting, BACKBOX

About BackBox

Backbox is a Network and Security Device Automation Platform that supports over 180 vendors, with thousands of pre-built automations and a scripting-free way to build new ones. Enterprises and service providers worldwide trust BackBox to automate and audit anything an admin could do manually, with reliable automations that are flexible, scalable, and contextually aware. From backups and OS updates to configuration compliance, BackBox gives you confidence that your automations will deliver the expected outcome every time.

Find out more at www.backbox.com