BACKBOX
SOLUTION BRIEF

Automate Compliance with BackBox

Automatic configuration audit and drift remediation align your devices with your compliance regime.

Overview

Compliance is a big topic that means different things to different people. For some, it means being compliant with regulatory regimes or industry standards – like CIS Benchmarks, PCI DSS, NIST, DORA, HIPAA, or DISA STIGs. For others, it means staying compliant with a golden config that represents your organization's best practices.

The challenges of compliance projects are three-fold:

1. **How to start?** It can be overwhelming for network administrators with hundreds of network and security devices, across vendors to comb through configurations to check and see if they meet your standards.
2. **How to keep compliant over time?** When configuration changes are made in complex networks, sometimes the result is falling out of compliance. Many companies do a bi-annual audit to check for configuration drift because it's simply too time-consuming to manually check compliance regularly across the device population. However, six months is a long time to be out of compliance.
3. **How to groom configurations into compliance when non-compliance is discovered?** Eventually, when you discover non-compliance, grooming the configuration back into compliance requires multiple manual steps, an engineer's expertise, and hours of time.

92%

of network teams say more network updates are needed than they can keep up with

Compliance is an ongoing process, which makes it a suitable start for an automation project. Manual compliance tracking adds too much overhead to teams that are unable to keep up with demands and exposes organizations to risk.

THE AUTOMATION ADVANTAGE

- Teams can accelerate compliance by creating automation templates that define their compliance requirements. For compliance standards like HIPAA, STIGs, PCI DSS, CIS Benchmarks, and others, BackBox has many automations prebuilt in the Automation Library ready to be used.
- Teams can maintain compliance and avoid configuration drift with automated checks against the compliance requirements. Non-compliant devices can be automatically remediated, or trouble tickets can be opened in an ITSM like ServiceNow for manual investigation and remediation.
- Compliance audits are performed regularly, often nightly, without burdening your teams, and compliance reporting can be shared with other parts of the organization as needed.

Automate the Complete Compliance Lifecycle Across Your Hybrid Network with BackBox

Configuration compliance cannot be managed with most device vendor software. So, organizations often rely on a manual process for device onboarding combined with infrequent audits of the configurations to ensure that compliance is maintained over time.

Unfortunately, we know that this doesn't work. Configuration drift is a given, and in any complex hybrid network, configurations are likely to drift due to changes to software that are made ad hoc and are not recorded or tracked comprehensively and systematically.

Manual tracking of configuration changes is error-prone. And, irregular compliance checks are inefficient. As such, the way compliance is done today is fundamentally broken and outdated, considering the opportunity provided by automation.

Let's take a look at how the end-to-end compliance process can be improved with automation.

Get Started

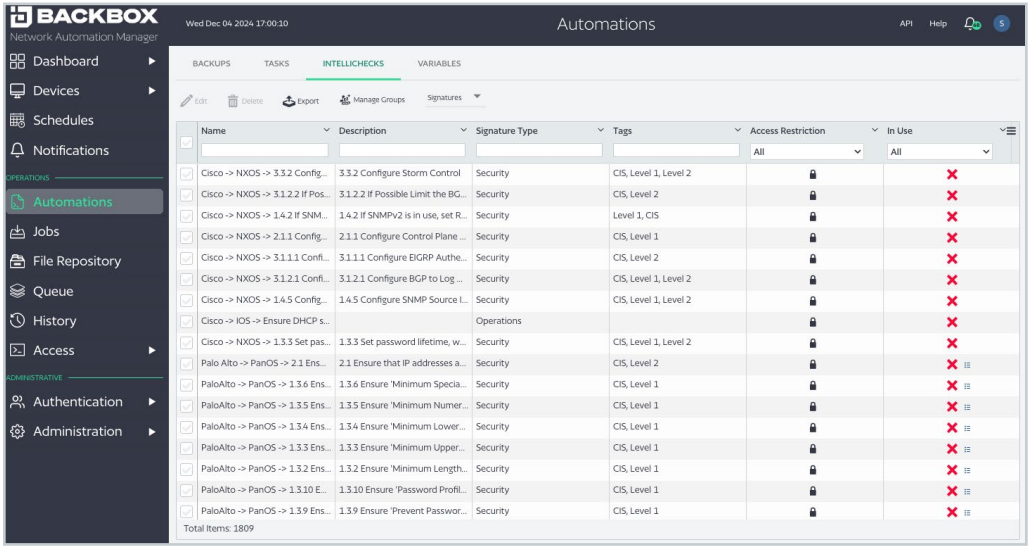
There are two questions that kick-off every compliance project:

1. What rules do we want each device to comply with?
2. What is the current state of devices and their configurations?

AUTOMATED VALIDATION REMEDIATION WITH INTELLICHECKS

Deciding the compliance rules is an organization's responsibility. Once these rules are chosen, IntelliChecks automations are created to check and enforce these rules.

BackBox contains prebuilt IntelliChecks that express the rules defined by CIS Benchmarks, DORA, NIST, STIGs, and others. These rules are a good starting point for organizations to build out custom rules based on their internal standards.

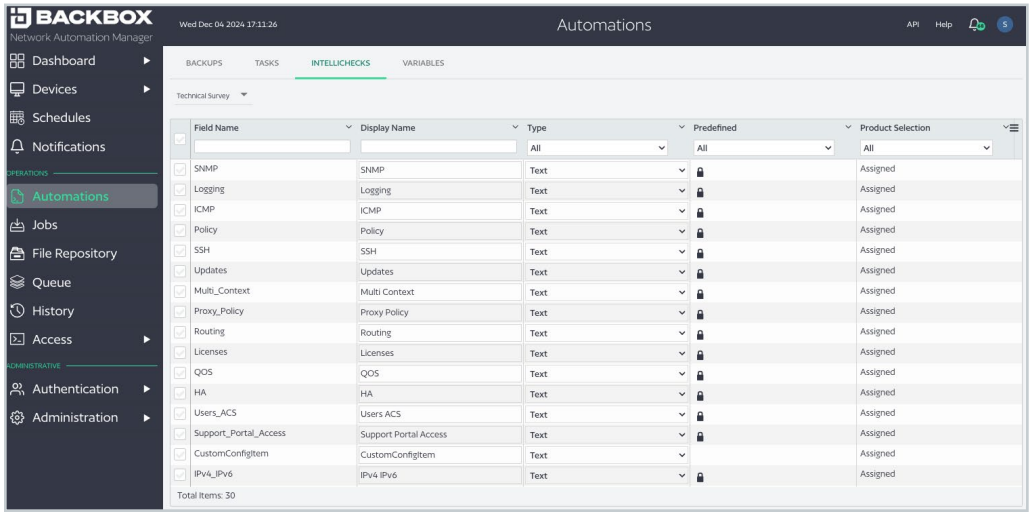


TECHNICAL SURVEY

During the process of building out compliant standards, it's useful to be able to "ask the network questions." For example, to find out which machines are not running SNMP or which have password requirements shorter than 10 characters.

Investigating network configuration parameters for both on-prem and cloud-managed devices, provides a baseline for building out compliance standards.

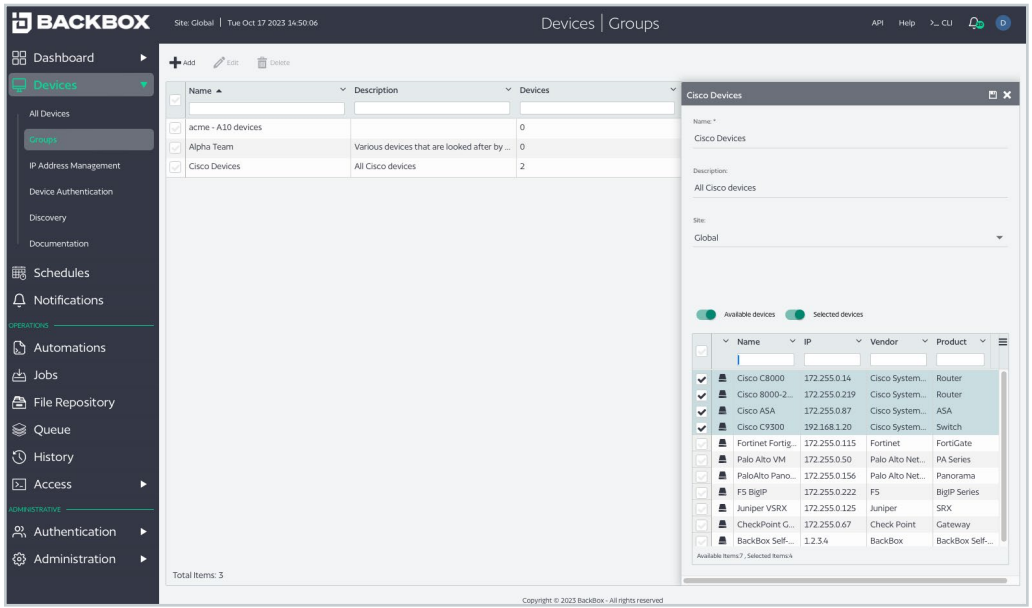
BackBox offers a Technical Survey capability that is easily accessible and lets network administrators quickly determine the current state of device configurations across vendors and environments.



Find Non-Compliance

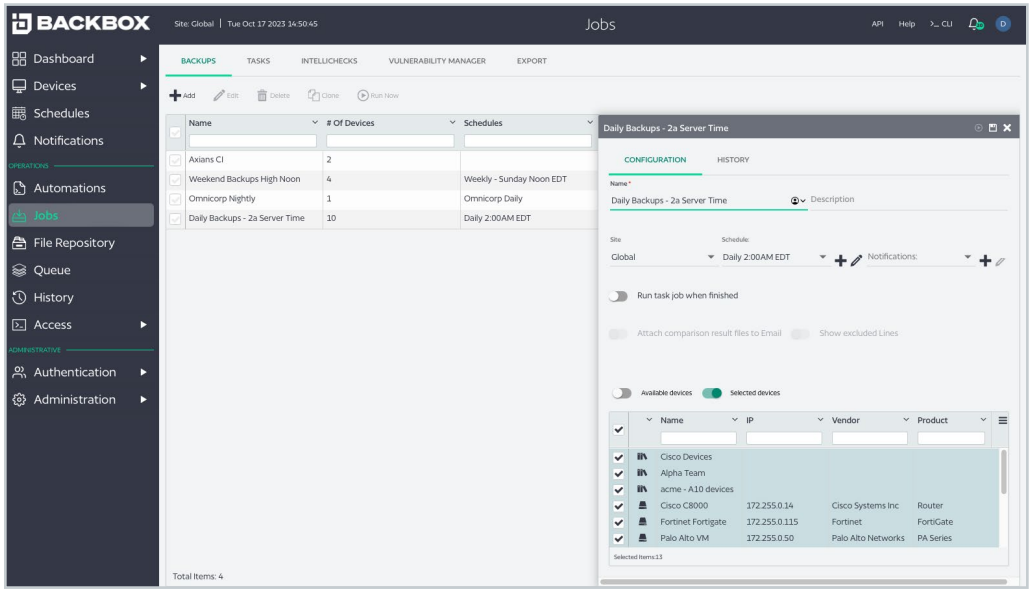
GROUPS

Once all the compliance automations are created, they're put into a Group to run collectively on whatever set of devices and combination of vendors you choose.



JOBS

With the Group setup, a Job is created and applied to the devices you wish to be compliant. The Job can be run manually or automatically, and typically serves as a starting point report. The Job should also be run on a daily schedule so that every day BackBox can search for and report non-compliant devices.



Stay Compliant

Remediation is an important part of compliance. BackBox IntelliChecks can include remediation capabilities so that when non-compliant devices are found, they can be groomed back into compliance. Automatic remediation is, of course, optional.

With remediation optional, there are two other ways that organizations use BackBox to respond to compliance violations.

1. **Reports.** Reporting is an integrated part of compliance because reports are often shared with other teams to assure them that the hybrid network is configured how it should be. Reporting can be done by the Job, showing the complete state of compliance, or by IntelliChecks, showing the status of any individual compliance rule across all devices. Reports include a column showing whether any remediation has been taken and, if so, the status.

2. **Automate trouble tickets.** It's understandable if automatic remediation makes teams uncomfortable. It's often better to have a human hand at the configuration keyboard. That's where external integrations come into play. BackBox can set up notifications to notify external systems of compliance violations. For example, BackBox can connect to an ITSM like ServiceNow to open a trouble ticket and resolve a compliance violation. And, because we know the remediation steps, we can put information about the remediation steps into the trouble ticket to help speed up resolution.

Another important part of staying compliant is ensuring that new devices are compliant when added to the network. Customers often create a Job with all the compliance configuration tasks, so it becomes easier to onboard new devices in a compliant configuration than manually installing a golden configuration.

CUSTOMER EXAMPLE

A customer was implementing DISA STIGs for their Juniper switches. This entailed a 92-step manual configuration check every week or two, with the output being an XML-formatted report of the configurations.

With BackBox, they could automate all 92 steps, saving the equivalent of almost a full-time engineer's worth of time.

Conclusion

Non-compliant devices — on-prem and cloud-managed — are a risk to the organization. Yet, device compliance is complex. It usually involves infrequent audits and contentious interactions between the network team and the compliance organization. The infrequent nature of compliance audits means that devices that fall out of compliance often stay that way for some time. Tracking device configurations manually and frequently is often too much overhead for teams already saddled with more work than they can keep up with.

Automation is simply the only way to have a timely compliance regime that's enforced. It ensures that configuration drift is groomed back into compliance – manually or automatically – and that there's transparent daily reporting on compliance status, with reports that can be shared among teams to help build trust.

With the ability to complete a Technical Survey and understand how devices are configured, BackBox serves as an ideal on-ramp to automation at your next compliance audit, creating reports that serve as project plans for grooming the current state of the network into compliance.

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**