BACKBOX
SOLUTION BRIEF

Backup and Restore with BackBox

Overview

Backups are a critical part of disaster recovery. But it's really challenging to prioritize backups when what people really care about is the ability to restore in a crisis. The backup itself is an administrative task, while the restore process gets all the glory.

The thing is, without a good backup process, restoring after a failure is going to be painful, slow, and risky.

We can't tell you how many stories we've heard of people who go to restore a backup only to find that the backup is corrupt. Or the backup process hadn't been running properly.

With BackBox, the focus is on easy-to-implement, reliable backups, that are consistent across all vendors and can be confidently restored with a single-click. Gone is the confusion that arises when a device fails and people need to remember how that particular device gets restored. BackBox saves time in a crisis with its single-click validated restore for all 180 vendors supported.

Before we get ahead of ourselves, there are less obvious but equally urgent considerations for network and security device backups. Backups are required precursors for cybersecurity insurance and even for some new regulatory regimes such as the EU-wide NIS2 Directive .

In this solution brief, we're going to consider two important aspects of backups:

1. The backups themselves
2. The backup process

Both the backup and the backup process are important to consider in the context of alternatives. Using a vendor tool for backing devices up might mean a rigid process, and a different process for each vendor. While writing custom scripts to get just the backup you need might offer flexibility, it will not have any process management around it (unless more scripts are written).

BackBox Backup Highlights

THE BACKUP

- Single-click restore
- Easy to implement
- 5-step verification of each backup
- Exception-driven alerting
- Collects all files needed to restore

THE BACKUP PROCESS

- Supports 180+ vendors with the same backup and restore processes
- Initiated on device discovery to ensure no device is left behind
- Backups can be triggered by an API for integration with other systems
- Backup automations can be embedded in other automations for easy roll-back if an operation fails, and immediate backup when an operation is successful
- Backup dashboard widgets are available to embed in network monitoring solutions like Paessler PRTG or LogicMonitor for seamless access within existing workflows

Without BackBox

The two most common ways to backup network or security devices without BackBox are to use a vendor tool or to write backup scripts on your own. Both have drawbacks.

Using a Vendor Tool

Vendor tools have limited flexibility when it comes to integrating the backup into your own process. Specifically, backup files can't easily be stored wherever you like, backup comparison tools are limited, and backups aren't always easy to restore.

Additionally, you're dependent on each vendor's tool for each product. This means that the backup process varies by vendor which hampers troubleshooting and the restore process in the event of a failure.

With BackBox the backup process becomes consistent across vendors – including ensuring each backup is valid and can be restored.

Additionally, vendor tools tend to focus on the specifics of performing a backup, whereas BackBox addresses the entire end-to-end backup and disaster recovery process.

Writing Your Own Backup Scripts

Writing scripts to backup is like writing your own email server. Sure, you can do it.
But should you?

Scripts need to be maintained. The people with knowledge of how the scripts are written can leave the company. And, it's more than just the backup the matters... it's the whole process.

- **How do you validate that the backup was successful?**
- **How do alerts on suspect backups work?**
- **Is the restore process as simple as a click, so that when you're under the gun with a failure you are up-and-running as quickly as possible?**

With BackBox you get an entire backup process infrastructure including scheduling, validating backups, notifications, and automated or manual comparison tools. You get a consistent way to do backups across all network and security device vendors in your network, and you don't have to maintain any code to accomplish your ultimate goal – having rock-solid backups that can be simply restored.

BackBox Backup and Restore

BackBox provides a framework for a rock-solid backup and restore process, enabling administrators to backup network and security devices from over 180 vendors consistently while minimizing errors and time-to-repair.

Earlier we mentioned the distinction between the backup and the backup process. Let's explore this distinction and the benefits of using BackBox to backup and restore network and security devices.

THE BACKUP

Backup and restore are the discrete building blocks of a successful backup strategy. BackBox's backup and restore solution is different in five important ways, even before considering the end-to-end process of backup management.

1 Single-click Restore

We always like to start with the outcome... the ability to restore a device in the event of a disaster. The restore might simply be to roll-back a configuration after a failed change or might be the result of failed hardware.In any case, BackBox's restore process is a single click. We take all the files needed and can restore the device even if it's a new piece of hardware being rebuilt from bare metal.

Prior to restoring files we validate the SHA256 checksum to ensure that the files being restored match the backup and that they've not been modified or corrupted. This prevents mishaps and ensures a speedy restoration.

2 Easy to Implement

Beginning with the device discovery process, administrators have the opportunity to tell BackBox to backup the device. This makes it easy to develop a discipline around device backups and ensures that every device discovered by BackBox is automatically secured by a reliable backup.

There are also out-of-the-box reports to know which devices don't have a backup scheduled, to compare backups for changes, and for backups which are suspect. These reports are useful for compliance and can be delivered on an exception-basis. Meaning that if there's nothing to tell, no report is sent. Only when something an administrator needs to take action on is noticed, is a report (or notification) sent.

3 Reliable Backups

BackBox backups are reliable. To deliver the industry's most reliable backups, we perform a 5-step verification process on each backup, including:

1. Backup errors
2. Size mismatch errors
3. Zero byte files
4. Looking for EOF (End-of-file)
5. Startup and running configuration mismatches

4 Exception-driven Alerting

We compare each backup to previous backups, and also give administrators powerful tools to compare backups across any time period. Flexibility is provided to save the backup history over time, which then allows backups to be used as a tool to answer the number one troubleshooting question: “What changed?”.

Rich notifications, including alerting or integration with external systems (like Slack, ServiceNow, or any ITSM) can be used to inform administrators to the possibility of an unsuccessful backup and that an investigation might be needed.

It’s always better to find out about a failed backup before trying to restore it in a crisis.

5 Collects All the Files You Might Need

BackBox gives the option to backup all files, including license files, running configuration files, and even the actual device software. Having all these files in one place when trying to restore a device is invaluable. Time is saved because everything needed to rebuild a device is handy.

Additionally, this allows administrators to rebuild failed devices with replacements. BackBox can restore to bare metal once a new device is reachable via an IP address. This makes BackBox ideal for restoring both to devices that need to be reconfigured and to devices that are being replaced.

THE BACKUP PROCESS

The NIS2 Directive in the European Union refers not to "backups" but to "backup management". This, in our opinion, implies that it's not just about the discrete backups that are needed. Responsible companies need a robust way to manage backups to ensure that their devices are kept safe from human errors, disaster, or cyberattack.

Let's take a look at the bigger picture backup process and how backups can be integrated into the enterprise workflow to ensure that devices are protected across the day-to-day operations of the network.

Multivendor

Every network has more than one vendor's equipment. And, this is especially true for service providers who support multiple customers.

The opportunity to use a single tool for backups presents the benefits of having one process for backing up devices, whether they're security devices or network devices, and regardless of the vendor.

BackBox supports automated backup for devices from over 180 vendors.

Backups are Initiated on Discovery

Backups become part of the onboarding process. This way, any device onboarded to BackBox automatically has a backup available for the worst-case scenario. This simple step provides a higher baseline for survivability from disaster because we know a working backup exists.

API Access to Backup Process

The BackBox API can be used to kick-off a device backup. This allows backups to be integrated into external processes that affect the network. It also allows other systems to control what happens to network devices which can be useful in environments where NetOps maturity is increasing.

Backups can be Embedded into Other Automations

Anytime a potentially destructive operation is done, you want to have a recent backup. However, backups can be cumbersome and so shortcuts are taken. "We'll use yesterday's backups" is a common refrain, never mind that yesterday's backup might not have completed successfully, or might not include changes from earlier in the day.

With backup being an automation, it can be easily chained into other automations as part of a workflow. It's easiest explained with an example.

Let's say you want to update a device's software. You can create a chain that first does a backup, then runs some pre-checks, does the update, runs some post-checks, and then after the update is verified as successful, run another backup so that you have a successful backup of the updated device.

When the above can be automatically chained together there's less potential for error or shortcuts that mistakenly avoid proper backups.

Dashboard Widgets

BackBox includes dashboard widgets for the BackBox console that summarizes backup status across the network. This gives administrators a visual representation of systems at risk.

Even more powerful, these widgets can be embedded in other systems (like Paessler PRTG or LogicMonitor) so that backups can be tracked from the monitoring system of your choice.

Conclusion

> **Do you sleep well knowing with confidence that you can restore your backups, or is there a small part of you that hopes you never have to find out?**

It's very easy to think that "backups" is a solved problem. After all, there are many different ways to accomplish backing up devices.

With However, it's all too common for teams to go to restore a backup only to find that the restore file is corrupt, or the backup process has been failing for weeks.

Teams need a best-in-class, reliable, multivendor backup solution that ensures the ability to restore devices in a crisis, even if restoring means to a new, replacement device. They need a backup management solution that not only focuses on the features of backing up a device, but the end-to-end process of managing the backup process.
BackBox is that solution.

BACKBOX

About BackBox

BackBox powers The BackBox Automation Platform for Network Teams, which supports network and security device automation of over 180 vendors, with thousands of security-centric pre-built automations and a scripting-free way to build new ones. Enterprises and managed 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 and vulnerability management, BackBox gives administrators the confidence that automations will deliver the expected outcome every time.

To learn more, visit backbox.com