BACKBOX
SOLUTION BRIEF

OS Updates and Patching with BackBox

Keep your network secure with the latest OS updates, simply and automatically.

> **The UK's National Cyber Security Center says, "Patching remains the single most important thing you can do to secure your technology." Yet often it's months before device updates are deployed. Why?**

OS Updates as Administrative Tasks vs Security Posture Management

OS Updates are repetitive, disruptive, and time consuming. They're mundane, manual administrative tasks and are prioritized as such rather than being prioritized as a security activity.

In the past, updates were driven by an undefined sentiment that "it's better to be on a more recent version", or occasionally to add features needed by applications. In short, updates were considered an administrative task that didn't really have a measurable impact on the business (other than the disruption which updates cause).

Today, updates are tightly related to the security posture of your network, ensuring that known vulnerabilities are mitigated or fixed so that networks are immune to malicious activity.

Thinking of updates as a security tool rather than an administrative task turns them from a nice-to-have to a must-have. But many organizations still haven't shifted their thinking or internal procedures to recognize and address updates as security priorities.

Update Urgency; It's in the Numbers

Everywhere you look there are statistics and anecdotes about the importance of OS Updates, and how automation can help.

> **Nearly 60% of cyber attack victims said installing an available patch would have prevented their breach,"** according to research by Ponemon / ServiceNow

And in a separate study by Ponemon / BMS , **"61% of respondents say their organizations are at a disadvantage in responding to vulnerabilities because they use manual processes and 55%agree that IT security spends more time navigating manual processes than responding to vulnerabilities."**

If that last quote wasn't enough, Gartner clearly says in their August '23 Market Guide for Vulnerability Assessment, **"Automation plays an important role in achieving timely remediation."**

THESE RESEARCH STATISTICS TELL US:

- OS Updates are the most important thing network administrators can do to keep their networks safe.
- In one study, patching would have prevented 60% of breaches that occurred (which means patching is not being done).
- Organizations are at a disadvantage when responding to vulnerabilities because of heavily manual processes.
- Gartner states the solution to timely remediation clearly: **Automation.**

Without BackBox, Updates are Complex

Many organizations haven't yet made updates a security priority, and haven't fine-tuned their internal processes to make them easier. However, vendors also haven't addressed the challenge:

1. They failed to make updates simpler.
2. They fail to realize that for many customers, updates include a multi-step process to update from an earlier version to the latest.
3. They fail to look at the context of the update in the environment, e.g. updating a high-availability pair.
4. They all have their own way of doing updates, and assume customers will align their internal processes to the vendor, rather than the other way around.
5. Their update processes are closed and hard to customize
6. They only look at the actual update steps, not the whole process, leaving customers to handle important supporting activities (like backups, or pre- and post-checks) manually as part of the update process.

OS Updates with BackBox

With BackBox, updates are easier, faster and can even be performed during regular business hours. BackBox considers five important elements of the OS Update process to make this happen:

1. **Process Integration.** We consider the entire update process when helping administrators complete patches. This means it's easy to incorporate automated backups at the start and end of the process. You can also include pre- and post-checks in the process, with decision making. – For example, you can automate roll-backs if your post-checks fail. We can move files during regular business hours, so that after-hours work in minimized. (This is especially useful in Check Point implementations because of the way they do updates.) We can even do call-outs in the middle of the process to update an ITSM or publish updates to Slack. The flexibility to make the process your own enables BackBox to solve OS Updates exactly the way your environment demands, rather than having to compromise your environment to shoehorn in a vendor's rigid process.

2. **Consistent Across Vendors.** As a multivendor solution, the BackBox Update process remains consistent across vendors. While each update is tuned to the specific vendor, the flexibility to make the process your own ensures that you have a consistent process for performing upgrades. For example, no matter what vendor, you can be certain that a backup is performed before the update and after a successful update.
3. **Reporting.** Reporting is customizable and in the event of exceptions to the update process reports can be sent automatically when further investigation is required.
4. **Firewalls and Routers.** Unlike other solutions, BackBox is custom-built for both security and network devices. This is especially useful since firewall updates can be more complex than router updates.
5. **Context Aware.** BackBox automations are aware of the environment being updated. Automations are high-availability aware, and can update the pair without downtime while ensuring that one device can handle the load of the pair. Similarly, BackBox can automate multi-step updates for devices that need multiple updates applied in order to get to a recent version.

In addition to these rich update process capabilities, BackBox will notify administrators when devices are end-of-life and updates will no longer be available, helping with hardware lifecycle management.

TWO CUSTOMER SUCCESS DATA POINTS

A global telecom provider with a large network has told us that Backbox saves them 45 minutes per device each time they upgrade.

And service provider, Edafio, says their old process that would take 35 hours on nights and weekends has been reduced to a single hour during business hours. The Edafio customer success story is available on the BackBox website.

These are powerful statements about the benefits and cost savings of automating OS Updates with BackBox.

Conclusion

Too many people still view OS Updates as an administrative task that takes a back seat to important business. Yet, in today's world, OS Updates are a front-line protection against vulnerabilities that expose organizations to costly cyber attacks.

As important as they are, OS Updates are still too complex and require a lot of manual administrative work, much of it often after-hours or on weekends. However, it doesn't have to be this way.

With BackBox, network administrators like Ryan Demay at Edafio have automated updates to eliminate errors, reduced the time it takes to update devices from many different vendors, and eliminated weekend work for their teams.

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