BACKBOX
SOLUTION BRIEF

Vulnerability Remediation with Kilter

Using dynamic inventory with risk data and scoring to help administrators prioritize and perform device OS updates with the greatest impact on network security.

Overview

As cyber-attacks leveraging unpatched devices become a common practice, an effort-saving comprehensive network security management platform is a must, empowering businesses to proactively identify vulnerabilities and strengthen their defenses against cyber threats.

> **More than 48,000 vulnerabilities were reported in 2025, an increase of around 20% from 2024."** NIST 2026

This presents a challenge for network and security device administrators.

Vulnerability patching for endpoints and compute systems is easier than patching network and security devices. Updating devices — on-prem and cloud-managed — like firewalls, IDSs, IPSs, routers, switches, and WAPs to patch CVEs is much more complicated, as each device impacts the entire network operations and security infrastructure. The BackBox network cyber resilience platform, working together with vulnerability intelligence can optimize the work invested in OS Updates in a way that maximizes the security impact on diverse, hybrid networks.

© 2026 BackBox. All rights reserved.

NIST lists over 2,500 CVEs per month. That's a lot of "out-of-context security information" for network administrators to consume. CVEs also serve, in part, as a roadmap for attackers to target network vulnerabilities. It's important to understand how CVEs pertain to your specific network inventory, taking the risk to your organization from the abstract to the specific.

The challenge is that permanently addressing the vulnerabilities disclosed in the CVEs requires an OS update or patch to the network devices. These updates are often complicated and time consuming, requiring after-hours work, sometimes with impacting the business.

This results in OS updates and vulnerability patches being delayed and deprioritized even though unpatched software is a top three access route for hackers, and patching remains the most important thing you can do to secure your technology.

Fortunately, there's now a better way for network operations teams and service providers of all sizes to protect their modern networks while reducing the intensity of manual work these software updates entail.

VULNERABILITY REMEDIATION

- **Dynamic Inventory.** With Kilter by BackBox, there's no guessing about your inventory. You want to ensure you have a complete and current view of your modern network and security devices. Collecting inventory information is an error-prone, manual process completed as part of provisioning new devices or updating existing ones. Kilter models your network's configuration inventory, which is mapped against an AI-enabled threat and vulnerability intelligence feed that uses CVEs and other security information to determine the threat level against your specific inventory.
- **Risk Scoring and Analytics.** Kilter vulnerability intelligence risk scoring engine reviews vulnerabilities impacting the organization and provides attack surface score and risk metrics for every connected device on the network. It understands and presents contextual risk across all devices and networks for a complete view of network vulnerabilities and risk exposure. The risk score integrates CVSS scores along with the number of CVEs on the device, whether or not a CVE is under active exploit, and if the device being scored is internet-facing.
- **CVE Mitigation.** Administrators can search device configuration files for specific vulnerable configurations to determine the relevance of any given CVE. If a vulnerability is found, using automation, it can be mitigated, and once mitigated, it's removed from the risk score. However, some CVEs will be determined to be irrelevant to the device. In that case, administrators can make the CVE non-applicable to the device, causing the risk score to recalculate and present an accurate view of the vulnerability state of the device. These non-applicable CVEs, called "mitigated" in the product, can be managed in their interface so that if they become relevant later in the future, they can be re-added.
- **Remediation Prioritized by Risk Analysis.** Kilter takes the complexity from the patching process while giving administrators risk analysis data to prioritize updates. This data helps create consensus and provides a complete picture of the priority of vulnerability patching, while the pre-built automations make deploying updates easier than ever before. Kilter even provides insight into step upgrades, enabling organizations to easily understand how their security posture improves by updating, but not to the most recent version.

© 2026 BackBox. All rights reserved.

Most network engineers would agree that updating an OS for its own sake is an administrative exercise, but patching vulnerabilities is critical. Should CVEs expose vulnerabilities, there are important steps to take immediately, followed by the software update, which is a permanent fix.

Let's explore the process of vulnerability patching in a little more detail.

Without Kilter

There are five elements to patching vulnerabilities:

1. Understand your inventory — on-prem and cloud-based — and exposures
2. Determine the update priorities
3. Remediate with temporary configuration fixes
4. Remediate permanently with OS updates
5. Remove temporary configuration fixes

We hear from many of our customers that this end-to-end update cycle is manual. Even when inventory is kept in a central system, there's a lack of confidence that it is complete and up-to-date for an important task like vulnerability patching due to shortcomings in the discovery process.

Similarly, the inventory system is not a "working system." Inventory needs to be exported somewhere (like a spreadsheet or database) to verify and perhaps manipulate it, for example, ordering vulnerability patches by priority relative to business need. Additionally, once the inventory is out of the inventory system, it should be assumed to be out of date with any adds, moves, or changes that occur after the export.

Once visibility into inventory is available, a similar exercise needs to happen with CVEs.

CVEs, if they're tracked at all, are tracked manually in a spreadsheet or a database, with some limited ordering based on priority and associated with the equipment in the inventory. Additional information can be correlated manually from other sources to enrich that presented in the CVE. It's a lot of manual effort.

This can result in ambiguity and blind spots. For example, how does my security posture improve if I update to a newer version, but not the latest, a common practice? Or, of the critical vulnerabilities my network is exposed to, which ones are currently being exploited in the wild? You might prioritize those vulnerabilities with known exploits if that exploit information were presented in the context of the rest of the security scoring.

© 2026 BackBox. All rights reserved.

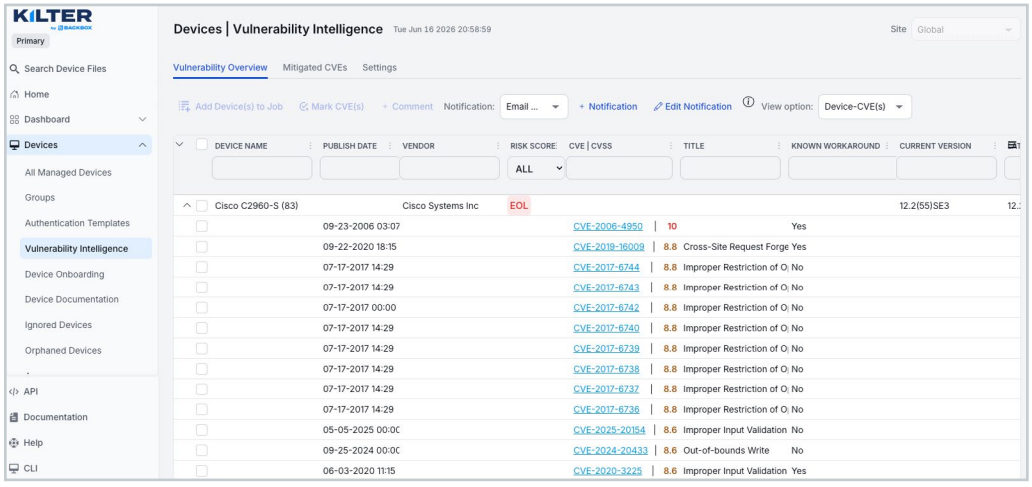
Temporary configuration changes are easy enough to make with the usual processes at the organization, but software updates remain highly disruptive. Additionally, temporary configuration changes have a nasty habit of becoming permanent simply due to a lack of systems to track which devices have been temporarily patched and then updated.

Lacking a security score and hard data on the impact of potential protection updates, they're moved to after-hours administrative work driven by a vague notion that being on the latest version is better. And, without automation closing the loop between inventory and the vulnerability patch, the effort is time consuming, error-prone, and leaves a big time gap between known vulnerability and patched vulnerability that can be maliciously exploited.

With Kilter Vulnerability Intelligence

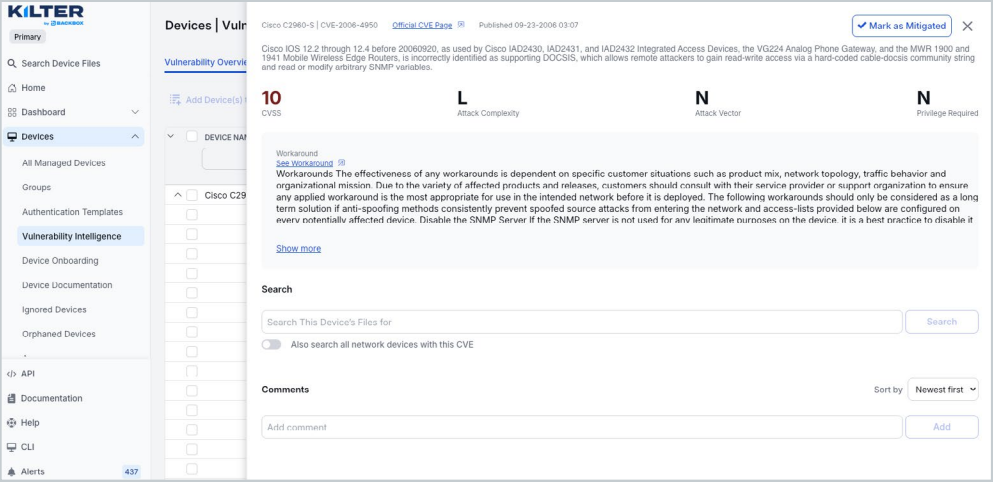
Kilter has closed the loop between dynamic inventory and OS update prioritization by integrating a continuously updating operational security database of CVE information, risk scoring, and other security metadata.

Kilter provides details about a vulnerability and the device, such as make, model, firmware, configuration, etc. CVE scores are based on industry-standard CVE scoring. Kilter informs you if a CVE is currently being exploited in the wild. Kilter provides a level of context that you won't get if you're handling this manually. Like the network inventory, the CVE, vulnerability, and risk data that informs the analysis are also updated daily. The result is that both inventory and vulnerability/risk information is updated and correlated daily, giving administrators a current view of their network exposure to cyber threats.

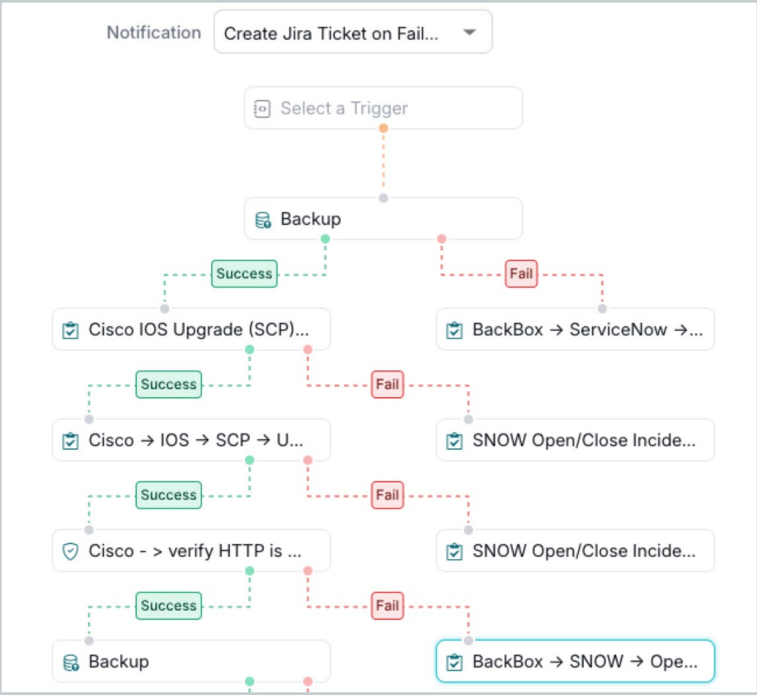


© 2026 BackBox. All rights reserved.

Kilter leverages AI to normalize disorganizaed data sources and ensures traceability of AI-process data. You can drill down into each CVE to get more details and visit the vendor website. If there is a workaround or remediation available, Kilter will recommend the best upgrade paths based on current device versions. With Kilter, you can also search managed devices to identify other devices or configs affected by a vulnerability. It's all available in one place.



Kilter can automate CVE remediation by converting cleaned workaround data into logical, executable steps. This simplifies the vulnerability review and and prioritzation process, reducing the effort from weeks to hours.



© 2026 BackBox. All rights reserved.

Conclusion

Vulnerability patching is hard. It's time-consuming, manual work often done after hours. While Kilter has always made it easier and faster to complete updates, they were still done without insight into vulnerability severity or the actual risk to the organization, until now.

With Kilter, modern networks can be kept more secure, with OS updates prioritized by risk and vulnerability data. Administrators can act on known inventory and be certain they have complete network visibility. Inventory is correlated with up-to-date data on CVEs and known risks, giving administrators a current view of their network exposure to the latest cyber threats. As always, updates are done in the most efficient way possible with support for over 180 vendors in the built-in Automation Library.

About BackBox

More than 500 enterprises worldwide trust Kilter by BackBox as their preferred network cyber resilience platform. Kilter supports network devices from over 180 vendors, offering thousands of pre-built automations and a no-code way to create new ones. Kilter 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, Kilter ensures that automations deliver consistent, reliable outcomes.

To learn more, visit backbox.com