BACKBOX
SOLUTION BRIEF

Top 5 Things to Know About Cyber Resilience for Network Devices

Overview

Cyber resilience is a hot topic as more and more organizations realize that it is not a matter of if, but when they will be attacked. In fact, 94% of cloud users were targeted at some point during every month of 2023, and of those 62% were successfully compromised.

However, one of the areas that gets lost in cyber resilience discussions are network devices, even though they are essential to keeping your business up and running. In these five questions we'll get to the bottom of why cyber resilience for network devices is lagging, and what to do about it.

1 What is cyber resilience for network devices?

The ability to **persistently** prevent, withstand, and recover from disruptions to network devices due to cyberattacks, or natural or man-made disasters.

2 Why are network devices hard to keep resilient?

There are two primary reasons. First, unlike endpoints, there are hundreds of different manufacturers that make up your network device topology in your environment. Having people manually maintain and manage a diverse environment is hard enough. But even the largest and most well-resourced organizations find it difficult to manage that complexity **all the time** to keep network devices resilient. Despite best efforts, 58% of breaches are surfaced by third parties or the attackers themselves, not the organization's security teams and tools.

Cyber resilience for network devices is a time, resource, and priority problem that should be automated.

This leads to the second reason why it's hard to keep network devices resilient. People don't automate because many automation systems shift the burden to the user to write automations. Most organizations don't have people sitting on the bench with the skillset to take on the coding required. Others that have gone down the path of packaged automations have been burned because they don't get alerted when something fails so it can be fixed.

For your network devices to be resilient you need to automate, and it must be done responsibly.

3 Why is it important for network devices to be cyber resilient?

The world depends on networks, so network devices need to be up and running, even in the face of disruptions that threaten downtime. At the same time, while AI initiatives can be a boon to businesses, in the hands of threat actors the technology increases the success rate of cyberattacks. Threat actors are using AI to help discover the latest exploits and exploit vulnerabilities faster. In 2023, the average time to exploit vulnerabilities was 44 days, but in 25% of cases, exploits were available on the same day, and 75% were exploited within 19 days.

The odds of your network being disrupted are increasing. Cybersecurity technology that only monitors and tells you about your risk posture or threats is not enough. You need cyber resilience, not just monitoring, to stay ahead of today's threats. Cyber resilience of your network devices will give you confidence that your business can keep moving forward.

4 What are the key components of cyber resilience for network devices?

Network devices that are cyber resilient are in a known and trusted state – all the time. This requires the following capabilities to maintain resilience:

- Reliable backups. As a baseline, you need backups for all your devices from all your vendors that have been validated, **and the ability to restore** with a single click so that you have a fast and reliable way to recover in the event of a service disruption.
- Configuration compliance. You must be able to run compliance checks of all your devices quickly and easily to see if you're still resilient or what has changed. Any configuration drift should be able to be automatically groomed back into compliance with your organization's standards or industry best practices.
- Vulnerability management and remediation. You should be able to quickly know what active exploits you are vulnerable to, and then have the option to automatically mitigate the vulnerability with a configuration change or remediate the vulnerability by updating the device software.

5 What are the benefits of cyber resilience for network devices?

Keeping your network devices resilient means that:

- Your network availability remains high because you face fewer disruptions
- You reduce the risk of a breach and the financial and reputational fallout from a disruption
- You are able to remain compliant with policies and regulations, reducing the potential for fines and other penalties

When you lean into automation, you can achieve all of this and realize a strong ROI.

Why BackBox

More than 500 enterprises worldwide trust BackBox as their cyber resilience platform of choice for network devices. BackBox includes support for network devices from over 180 vendors and thousands of pre-built automations and a no-code way to create new ones. Teams have confidence in automation and in their ability to withstand disruptions while maintaining business as usual and recover quickly.

Request a Demo