BACKBOX

SOLUTION BRIEF

7 Essential Priorities for Implementing a Network Cyber Resilience Solution

A well-designed network cyber resilience solution can save resources and boost productivity while minimizing downtime and risk to the organization. Here are some priorities in shaping the network cyber resilience solution.

1 Integration is Key

Systems don't operate in a vacuum. That means the network cyber resilience platform must be tightly integrated with network monitoring systems, the security operations stack, and the IT Service Management framework. It's critically important to integrate real-time, ongoing threat intelligence and vulnerability management – whether from proprietary, open source, government-supplied, or other sources – that can be automatically fed into the system.

2 Gain a Proactive Understanding of the Project Scope and How it May Change Over Time

Network cyber resilience needs to address more than just a snapshot in time. Instead, the solution must automatically scale and adapt to how the network evolves and grows over time – up to and including radical shifts that may come with a merger or acquisition. That's why capabilities like automated discovery of new systems and scalable security that grows with the size of the network are essential.

3 Availability and Redundancy are Critical

Network cyber resilience combines scheduled activity and management of unforeseen events. Especially in the latter case, it's essential to have adequate availability and redundancy to ensure that that clock never stops on security. System visibility and adaptive security measures should continue, even during downtimes and system outages. Otherwise, security teams remain dark while cyber risks multiply every momentile cyber risks multiply with every passing moment.

4 Ensure Robust and Automated Reporting

The network cyber resilience capabilities portfolio must include automated reporting to optimize the company's compliance and security posture continuously. This can be done by leveraging asset and device communication protocols to collect information and generate highly detailed yet easy-to-read reports on previous and current device status. Specific remediation actions and performance testing must also be documented to demonstrate compliance.

5 Match the Network Automation Solution to a Realistic Understanding of Team Availability and Skill Sets

Some organizations have plentiful IT budgets and staffing resources, which allows them to set up in-house network cyber resilience. Others are hoping for out-of-the-box solutions and partnerships to make the network more secure without becoming a Full-time job for the company. Both are viable options, provided the chosen solution is realistically matched with the staffing realities.

6 Use the Highest Level Protocol Available as the Basis for Automation

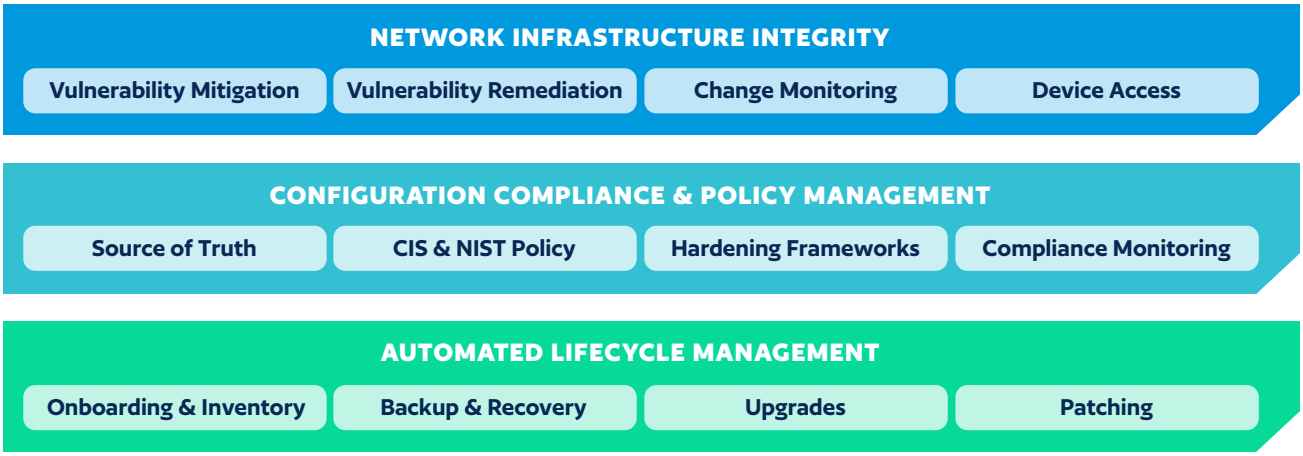
Automate at the highest and most modern level in the stack. For instance, when integrating a network cyber resilience tool with other systems, do so at the API level rather than through user interfaces. This reduces the chance of getting stuck with data structures and configuration parameters that may change over time.

7 Don't Automate Anything Without an Underlying Grasp of How to do it Manually

Automation should be rooted in understanding how to perform a function manually. This is necessary for quality assurance and troubleshooting. Document and understand all workflows, assets, and dependencies; pilot and validate processes; and then scale with automation.

Fulfilling the Promise of Network Security Automation

The right network cyber resilience solution can deliver a wide range of out-of-the-box, predefined applications of network security automation use cases. Modern enterprises need a solution that can address potentially thousands of automation use cases and support the roughly 300-plus vendors in the market today. Organizations must also future-proof their networks by allowing business users to create custom automations via self-serve platforms that don't require advanced programming language or expertise.



BackBox delivers all these benefits and more as the leading provider of Network Cyber Resilience solutions for automated lifecycle management, compliance and policy management, and network infrastructure integrity. We help companies worldwide automate and streamline complex tasks, ensure network health and performance, achieve business continuity, and do more with fewer resources.

BackBox supports customers with industry-leading experience and a passion for improving enterprise network operations. It's the driving force behind award-winning solutions that constantly exceed our customers' expectations.

BACKBOX

SOLUTION BRIEF

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