

7 Key Recommendations for MSPs in Shaping Network Cyber Resilience Partnerships



A well-designed network cyber resilience partnership can help MSPs save resources and boost productivity while minimizing downtime and risk to their client organizations. Here are some priorities in crafting a cyber resilience partnership that's ideally suited to the world of MSPs:

1 **Ensure the MSP's network cyber resilience partner has a centralized console for managing access and configurations across multiple IT estates**

Managing customer networks requires specialized features for multi-tenancy and reachability. Choose a partner whose platform supports these ecosystems' unique requirements.

2 **Ensure the network automation system is smart enough to manage overlapping or duplicated IP address spaces or identical device names across multiple client networks**

One challenge MSPs face is that their customers are likely using the same or overlapping private IP address spaces. Standard device names like "internet gateway" may also be used by multiple customers. The partner's network security automation platform should support these scenarios out of the box.

3 **Be sure to select partnerships that have an accessible and user-friendly learning curve**

Most MSPs won't have the luxury of dedicating two or three staff members' time to maintaining the network cyber resilience platform. Select a partner that allows your team to focus on your customers versus their platform.

4 **Ensure the network security automation partner has an advanced approach to client workflows and processes**

Workflows are the unsung heroes of modern automation approaches. Pre-checks, post-checks, and recursive workflows are table stakes. Even a relatively basic automation to patch a firewall may require rerouting traffic, validating connectivity and performance, and then rerouting the traffic as a part of the procedure. Be sure that your prospective partners are up to these challenges.

5 **Ensure the network automation partner can handle both greenfield and brownfield deployments**

Some technology service providers deploy new greenfield hardware when onboarding customers, while others modify the customers' existing brownfield equipment. Make sure that any partner you choose has solutions for each.

6 **Be sure to select a vendor that offers rich support for customizing network automation use cases**

Even if your staff includes a healthy number of automation experts, getting help straight from your automation partner will be the shortest path to success in many scenarios. Choose a partner willing and able to operate seamlessly as an extension of your team.

7 **Be sure to select a network cyber resilience partner that has a proven track record with MSPs and their unique needs**

Nobody wants to be the first guinea pig for an emerging network automation platform. Choose a partner with an established history of success with other partners that are at least as large as your organization.

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.

NETWORK INFRASTRUCTURE INTEGRITY

Vulnerability Mitigation

Vulnerability Remediation

Change Monitoring

Device Access

CONFIGURATION COMPLIANCE & POLICY MANAGEMENT

Source of Truth

CIS & NIST Policy

Hardening Frameworks

Compliance Monitoring

AUTOMATED LIFECYCLE MANAGEMENT

Onboarding & Inventory

Backup & Recovery

Upgrades

Patching

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.

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