BACKBOX

7 STEPS TO ENHANCE NETWORK CYBER RESILIENCE THROUGH AUTOMATION

When it comes to network cyber resilience, we often think about vulnerabilities or exploits. About internal threats, and password compromises. **We don't often think about automation.** Automation is the foundation on which networks are kept secure and resilient.

HERE ARE 7 STEPS TO ENHANCE NETWORK CYBER RESILIENCE THROUGH AUTOMATION:

01 ASSESS YOUR ENVIRONMENT, SET YOUR STRATEGY, & SELECT A PLATFORM

Not all automation is the same. Evaluate your network's demands and your team's skills in scripting and automation before making commitments. Also, consider your budget and ROI for automation.

02 IMPLEMENT WELL-ARCHITECTED, AUTOMATED BACKUPS

Backups can be a hassle. You need to ensure they work, manage files, and practice restoration. It's also crucial to confirm they correctly run every evening and before and after any significant changes. If your network goes down, quick restoration is essential, but it's not always easy.

03 AUTOMATE COMPLIANCE AUDITS & REMEDIATION

Compliance can take various forms, from best practices as a golden configuration to formal standards like CIS Benchmarks, HIPAA, or NIST. The goal is to use automation to achieve compliance, monitor drift, and auto-remediate any issues to maintain compliance.

04 AUTOMATE ONBOARDING & DISCOVERY

Whether you're just starting to add devices or tracking their movements and changes, you want automation with templates to ensure that new devices are integrated into the network and configured securely to protect the company.

05 INTEGRATE VULNERABILITY & RISK INTELLIGENCE DATA

Automation enables a comprehensive device inventory, serving as a foundation for security audits against an AI-enabled threat intelligence feed, integrating data from CISA, NVD, NIST, and vendor websites. This risk analysis informs software updates and configuration changes to mitigate exploits before deployment.

06 AUTOMATE OS UPGRADES & PATCHES

OS updates are challenging, often requiring off-hours work and significant manual effort. They can fail and may take multiple attempts to succeed. In large networks, updates involve complex workflows, including backups, validation, and high-availability considerations. Automation allows for more frequent updates that patch vulnerabilities faster and enhance network security.

07 FUNNEL CHANGES THROUGH THE AUTOMATION PLATFORM (EVEN MANUAL ONES)

Automate as many changes as possible, then secure them so only the automation platform can adjust. The platform can audit device changes and provide recorded sessions for training and compliance. Reviewing logs can reveal more automation opportunities, increasing the value brought to the organization.

Contact us to request a demo and learn the value the BackBox cyber resilience platform can deliver.

REQUEST A DEMO // CONTACT US

www.**backbox**.com