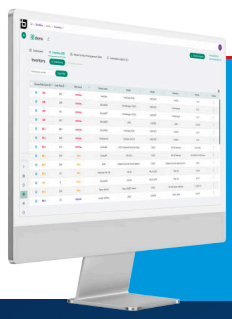
BACKBOX

SUPERCHARGE SECURITY:

10 Automation Use Cases for Network Cyber Resilience

Managing and securing complex networks is a constant struggle for Network and Security teams. Network automation empowers you to **streamline network device security**, **compliance**, and **lifecycle management**, ensuring business continuity during disruptions, and enabling swift recovery.

ON YOUR OWN	WITH BACKBOX
Manual onboarding delays new services rollouts and equipment replacements, leading to inventory backlog and old devices remaining in production.	**DEVICE DISCOVERY & ONBOARDING** BackBox cuts onboarding time with automated discovery, compliance enforcement, and instant backups.
Manual backup management is unreliable, creating constant anxiety about data loss and slow recovery times when disaster strikes.	**BACKUP & RECOVERY** BackBox simplifies backup and recovery with data validation, one-click restores, customizable schedules, and vast vendor support.
Slow and inconsistent software patching leaves organizations vulnerable to cyberattacks.	**DEVICE OS UPDATES** BackBox offers secure, automated patching with seamless rollbacks, high-availability awareness, and pre-built multi-step updates for optimal network security and uptime.
Organizations struggle to balance urgent vulnerability mitigation with complex patching processes and messy rollbacks.	**VULNERABILITY INTELLIGENCE** Smart automation prioritizes critical security fixes on essential devices, keeping your network safe with an always-updated risk score and assessment.
Manual network security processes result in errors, inefficiencies, and a lack of real-time visibility.	**NETWORK SOURCE OF TRUTH** BackBox auto-discovers your network, keeping inventory current with real-time data. No more manual work, just a complete and accurate Network Source of Truth.
Manual compliance remediation is slow, error-prone, lacks oversight, and bottlenecks risk management, never mind that compliance violations often go unnoticed (and unfixed).	**COMPLIANCE REMEDIATION** BackBox streamlines compliance with flexible scheduling, efficient resource usage, exception-based alerts for proactive risk management, rich reporting, and optional auto-remediation of compliance violations.
Urgent troubleshooting in production networks leaves behind "temporary" changes, creating security vulnerabilities needing regular, systematic cleanup.	**CONFIGURATION DRIFT REPORTING & REMEDIATION** BackBox cuts through compliance complexity, surfacing critical exceptions, automating fixes, and seamlessly linking with external systems for complete issue management and resolution.
Spreadsheet fatigue leads to expired certificates—a significant cause of network failures.	**SSL CERTIFICATE EXPIRATION TRACKING** BackBox simplifies network certificate management with automated tracking, targeted alerts, and helpdesk integration for expiring certificates.
Missed license renewals lead to a scramble for vendor updates, costing time and money.	**LICENSE EXPIRATION TRACKING** BackBox automates license tracking, supports all your vendors, and gives you complete control and visibility with exception-based management.
Manual ticket enrichment creates a bottleneck in the service desk, impacting the speed and accuracy of problem resolution.	**IT SERVICE DESK TICKET ENRICHMENT** BackBox empowers help desks with rich data and automated insights to accelerate problem-solving and improve IT service efficiency.



BackBox enables network and security teams to reclaim time, reduce errors, and proactively manage network security by automating repetitive tasks, effortlessly scaling, and providing a centralized view for faster threat detection and improved compliance.

www.backbox.com