BACKBOX

WHITE PAPER

Network Security Automation: Securing the Dynamic Enterprise at Scale

Introduction

Network automation is becoming ubiquitous across many industry sectors as a key driver of digital transformation (DX) and scaling of the enterprise. From connectivity and monitoring, to load balancing, data center provisioning and beyond, a growing number of network functions are being automated every day to create more powerful, efficient and scalable enterprise operations.

Paradoxically, the rise in network automation to solve challenges of scale and complexity is creating its own set of new challenges, specifically around network security. That's because, as automation helps expand the size and reach of network systems, enterprise risk has also expanded via growing attack surfaces, gaps in systems integration and in an increased number of potential attack vectors. The resulting rise in risk from breaches, data exfiltration and everyday instances of unintentional human error can compromise operations and compliance and, in many cases, may be catastrophic to the organization.

To secure operations and minimize risk, the task of securing these vast automated networks must itself be addressed by automation – network security automation, to be precise. In other words, newly expanded enterprise IT systems require a newly expanded level of network security – one that can only be maintained by automating the process of continuously validating and improving the network security posture.

Without automation to drive constant visibility and a continuous improvement loop of evaluating and strengthening network security, organizations suffer the alternative scenario of a constantly weakening security posture. This happens as new vulnerabilities, exploits and malicious actors continue to add up over time and outpace the network's ability to keep up in monitoring and mitigating these threats, as the pace of change required by modern network operations causes configuration drift.

> **A growing number of network functions are being automated every day to create more powerful, efficient and scalable enterprise operations.**

IN THESE PAGES, WE'LL DEFINE EXACTLY WHAT NETWORK SECURITY AUTOMATION IS, IT'S BENEFITS AND IMPLEMENTATION BEST PRACTICES.

What is Network Security Automation?

Network security automation, most simply, is a portion of network automation that is focused on continuously enhancing network security posture. When executed properly, network security automation creates an environment where, at the end of every day, your network should be more secure than it was when the day began.

Network security automation can help transform the entire IT estate to become more reliable, agile and resilient in the face of shifting technological and business conditions. This is because you've built a system of automation that is continuously improving the security posture over time as you get data from threat intel sources, from vendors on known exploits, and from users on configuration changes that are needed.

Well-implemented network security automation incorporates insights from all these data sources to continuously refine configurations to harden the perimeter around your network to improve security. Without network security automation, networks are inherently getting less secure with every passing day – as the number of new exploits, vulnerabilities and attackers continues to grow and chips away at the security and integrity of network systems.

CRITICAL ELEMENTS OF NETWORK SECURITY AUTOMATION INCLUDE:

Disaster Recovery; Backup and Restore

Highly available and well-orchestrated network infrastructure backup and recovery systems can reduce downtime and cut the risk of lost or compromised data from outages. Imagine a critical path firewall that has experienced a hardware failure. How quickly can you failover to a secondary route, replace the equipment with a new, fully configured firewall and reroute the traffic without automation?

OS Upgrade, Patch, and Vulnerability Management

Network security automation tools and processes benefit from integration with your vulnerability and risk management solutions. Combining their capabilities allows you to strategically plan your infrastructure upgrades and rapidly accelerate implementation. Organizations with a large number of remote offices without local IT staff, like retail and restaurant chains, as well as Managed Security Services Providers (MSSPs), see an especially high Return on Investment (ROI) for automation efforts of this type.

Managing Privileged Access

While most changes should be made via the network automation tool, at times engineers may need to make changes by hand. In these instances, it's incredibly important that: a) automated device backups occur before and after each critical step of the change and b) this "privileged activity" be done from the automation server using access management capabilities. This ensures that you can lock down where changes can originate from and maintain a detailed, immutable log of all activity.

Compliance Validation and Automated Remediation

Most organizations use compliance standards, such as those from NIST and CIS, to provide a baseline for data security and privacy protection. Network automation tools can audit device configurations, in real-time, to ensure that they adhere to compliance standards; industry best practices as they relate to security policy endorsement; and firewall rule maintenance. One way to leverage this technology is to orchestrate an "intelligent check", where the automation platform searches your configurations for misconfigurations that would drive you out of compliance, recommends remediations and gives you the option to activate those changes in real-time or at a determined schedule of all activity.

Cybersecurity Asset and Attack Surface Management (CAASM)

Especially as other forms of automation swell the size of the IT estate and the range of assets involved, network security automation is the key to maintaining visibility and control over these expanded asset ecosystems. For example, in hybrid-cloud environments where CI/CD processes dynamically reconfigure and provision new computing assets daily, connecting your CAASM system with both your ITSM platform and your network security automation platform can help ensure that as new resources are added to the network, they're added in secure and managed ways.

IT Service Management (ITSM)

Network security automation can bring consistency and standardization to the ITSM framework an organization uses to design, build, deliver, operate and control information technology services offered to customers. As one example, as new server VLANs are assigned, the network automation tool can deploy configuration changes to data center switches and apply rule updates to upstream firewalls. It's imperative that network security automation tools integrate with the organization's ITSM and service desk tools to enable closed-loop automation.

> **Network Security automation creates an environment where, at the end of every day, your network should be more secure than it was when the day began.**

Key Pitfalls to Avoid in Establishing Network Security Automation

Unfortunately, not all automation approaches are alike when it comes to addressing the challenge of securing network architectures. There can be huge variations around cost, performance, accessibility and scalability depending on how the network security automation initiative is designed and implemented.

Some automation solutions are not powerful, adaptable or comprehensive enough to securely handle the range of what might be literally thousands of different tasks and enterprise functions that lend themselves to automation. Other approaches fail to support the variety of vendors and range of network automation use cases required to suit the specific needs of an enterprise. In addition, they fail to adequately integrate these applications together within what might be very large, multi-cloud environments.

There's also the accessibility factor: Even network security solutions that address a business need are of limited use if they're not accessible to the business user. They may be overly complex and lack out-of-the-box convenience that would allow business users to tailor a pre-defined automation to a new use case through self-serve customization tools like no code and low code interfaces. This leads to an over-reliance on vendor support, as business users looking to automate a new use case must go back to the vendor to design it.

The good news is that with a proactive strategy that avoids these pitfalls, organizations can transform their IT operation into one that's more responsive, reliable and resilient. The right network security automation approach can be the foundation for a continuous improvement ecosystem as the organization grows – optimizing technology and talent utilization, continually updating and validating a company's security posture and reducing overall risk to the organization.

7 Essential Priorities for Implementation

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

1 Integration is Key

Systems don't operate in a vacuum. And that means the network security automation platform must be tightly integrated with network monitoring systems, the security operations stack and the entire IT Service Management framework. As part of this, 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 security automation 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 security is a combination of 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 in the dark while cyber risks multiply with every passing moment.

4 Ensure Robust and Automated Reporting

The network security automation capabilities portfolio must include automated reporting to ensure the company's compliance and security posture is optimized at all times. 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, as well as documentation of specific remediation actions and performance testing 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 that allow them to stand up network security automation completely in house. Others are hoping for out-of-the box solutions and partnerships to make the network more secure without it 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 security automation 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 an understanding of how to do a function by hand. This is necessary for quality assurance and troubleshooting. Make sure to document and understand all workflows, assets and dependencies; pilot and validate processes; and then scale with automation.

About BackBox: Fulfilling the Promise of Network Security Automation

The right network security automation solution can deliver a wide range of out-of-the-box, predefined applications of network security automation use cases. Modern enterprises today need a solution that can address potentially thousands of automation use cases and support the roughly 200 vendors that exist in the market today. Organizations also need the ability to future-proof their networks by allowing business users to create their own 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 Intelligent Network Automation solutions for disaster recovery, asset management, configuration orchestration and intelligent checks for the security and network infrastructure. 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 fundamentally improving enterprise network operations. It's the driving force behind award-winning solutions that constantly exceed our customers' expectations.

The BackBox solution simplifies the way you maintain your diverse network with:

- Automated Backup and Single-click Recovery
- Dynamic Inventory Management (with Network Visualization)
- Custom Task Orchestration

With additional add-on capabilities such as:

- Compliance Audit and Remediation
- Performance Checks
- Operations Checks
- Security Checks
- Access Auditing

BACKBOX

About BackBox

BackBox powers The BackBox Automation Platform for Network Teams, which supports network and security device automation of over 180 vendors, with thousands of security-centric pre-built automations and a scripting-free way to build new ones. Enterprises and managed service providers worldwide trust BackBox to automate and audit anything an admin could do manually, with reliable automations that are flexible, scalable, and contextually aware. From backups and OS updates to configuration compliance and vulnerability management, BackBox gives administrators the confidence that automations will deliver the expected outcome every time.

To learn more, visit backbox.com