BACKBOX

WHITE PAPER

Using Automation to Drive Revenue Growth and Cost Reduction for MSSPs

Introduction

Managed Security Service Providers (MSSPs) play an essential role for enterprises that don't have a dedicated network engineer or access to the talent needed to automate network security capabilities. Small and medium businesses (SMBs) have few options when it comes to network security and therefore outsource network security to MSSPs.

However, the increasingly critical role of the MSSP as an enterprise security provider creates some unique pain points for MSSP companies themselves as they seek to reliably access, manage and continually secure what may be dozens, or even hundreds, of customer networks. From configuration and access management, to network visibility, compliance and more, MSSPs must deal with unprecedented levels of complexity and scale as they protect the various IT estates of their many client organizations.

In the face of these challenges, MSSPs must establish the right protocols and industry partnerships to thoroughly automate network security for agile management and continuous improvement of the security posture across the many networks they are paid to protect. In these pages, we'll explore how MSSPs can best achieve this for enhanced revenue generation and service margins as they serve their enterprise clients.

MSSPs Face a Tough Proving Ground for Network Security Automation

The IT landscape for Managed Security Service Providers is among the most demanding in cybersecurity. A typical MSSP today must be able to navigate a diverse range of multi-vendor ecosystems and manage a wide variety of configurations that are already deployed and running in their clients' production environments. MSSP engineers routinely must juggle access and authentication methods and protocols that vary contextually across many different domains and network environments – with policies, rules enforcement, data standards, and workflows that all vary wildly from client to client and network to network.

These technological challenges become more daunting as MSSPs increasingly include managed firewall services as part of their solution to remain competitive in securing business – either directly from enterprise customers or through white label sales via Managed Service Providers (MSPs) that don't specialize in security.

The irony is that such clients are turning to the MSSP for its seasoned security and firewall engineers, but these engineers can quickly run out of hours in the day if forced to manage network security by hand.

Against this backdrop, MSSP network engineering teams are increasingly turning to automation as a way to handle the various configuration changes, backups, restores, patching and related network security management tasks that need to happen across their many client networks. However, not all automation solutions are created equally. For instance, insufficiently robust automation may allow for the streamlining of some routine tasks, but may have trouble handling multi-cloud environments; remain too costly to scale; or may not be able to handle the more advanced aspects of managed firewall services.

The quality of the network automation partnership is therefore critical to the MSSP's business continuity and mastery of configuration management across multiple vendor and enterprise ecosystems. (Keep in mind that, according to research by EMA, 80% of all network security issues can be tied back to problems with configuration management.) The stakes are such that MSSPs must do their homework on how to select and structure the partnerships for automating and scaling network security on behalf of their many diverse clients.

© 2024 BackBox. All right reserved.

Key Pitfalls to Avoid in Shaping the MSSP Network Automation Approach

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. All these variations are amplified for MSSPs as they seek to serve what may be dozens or hundreds of different customers.

To begin with, some network automation partners offer solutions that are not powerful, adaptable or comprehensive enough to securely handle the wide range of what might be literally thousands of different tasks and enterprise functions that lend themselves to automation. Especially critical for MSSPs are the shortcomings some automation partners have when it comes to supporting the variety of vendors required for MSSPs to serve the needs of the many different enterprises that make up their client base.

Accessibility can be a challenge as well. Even if a network security solution addresses the business needs that MSSPs must solve for clients, those solutions will be of limited use if they're not accessible to the business user. Tools that require software development skills or dedicated resources to operate are a poor choice for these environments. They may be overly complex and lack out-of-the-box convenience that would allow the MSSP to tailor a pre-defined automation to a novel use case, through self-serve customization tools like no-code and low-code interfaces. This leads to an over-reliance by the MSSP on vendor support from its network automation partner, sapping time and cutting into the MSSP's bottom line.

The good news is that with a proactive strategy that avoids these pitfalls, MSSPs can transform their operation into one that's more responsive, reliable and resilient on behalf of their clients. The right network security automation approach can be the foundation for MSSPs to differentiate themselves to customers by providing a continuous improvement security ecosystem that optimizes technology and talent utilization, continually updates and validates their clients' security posture and reduces overall risk to the MSSP and its portfolio of enterprise customers.

> **A well-designed network security automation partnership can help MSSPs save resources and boost productivity, while minimizing downtime and risk to their client organizations.**

80%

of all network security issues can be tied back to problems with configuration management, according to research by EMA.

© 2024 BackBox. All right reserved.

CRITICAL ELEMENTS OF NETWORK SECURITY AUTOMATION

MSSPs market themselves for their advanced capabilities in network security and firewall management. Here are six non-negotiable areas where MSSPs must deploy automation to provide that level of exemplary service and security to clients:

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 MSSPs, see an especially high 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.

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.

© 2024 BackBox. All right reserved.

7 Key Recommendations for MSSPs in Shaping Network Security Automation Partnerships

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

1 Ensure the MSSP's network automation 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 the unique requirements of these ecosystems.

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 of the challenges that MSSPs and MSPs face is that their customers are likely using the same or overlapping private IP address spaces. Additionally, common device names like "internet gateway" may occur amongst 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 MSSPs won't have the luxury of dedicating two or three staff members' time to maintaining the network automation 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 tables 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 simply 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 automaton partner will be the shortest path to success in many scenarios. Choose a partner who is willing and able to operate seamlessly as an extension of your team.

7 Be sure to select a network security automation partner that has a proven track record with MSSPs 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 own organization.

© 2024 BackBox. All right reserved.

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

© 2024 BackBox. All right reserved.

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