BACKBOX

WHITE PAPER

2023 Network Operations and Network Security Survey: What's Ahead for Automation

Executive Summary

This independent survey of 250 network operations and network security professionals in companies with 500 or more employees explores the current state of network automation, the challenges teams face, and opportunities for organizations to gain more benefit from network automation moving forward. Key findings and recommendations include:

NETWORK AUTOMATION: CRUCIAL BUT CAPABILITIES ARE LACKING

Nearly all respondents say more automated network operations is crucial to allow them to focus on more impactful work (98%) and help scale the business (96%). However, almost half (48%) report their company has not implemented or deeply invested in network automation.

> Start with simple outcomes: reliable backups, simple software updates and configuration updates. Then move to more advanced automations like inventory management, compliance validation and automated remediation.

THE TECH SPRAWL PARADOX

Despite averaging four network automation tools, with 45% having five or more, 92% of respondents can't keep up with network update velocity and 53% (rising to 68% for larger companies) only upgrade network and security devices quarterly or less frequently.

> Reduce the number of tools in the NOC stack, starting with legacy tools. Then integrate remaining tools in an overarching network automation strategy that supports multi-cloud and on-prem environments, and automates upgrades in line with compliance and security standards.

TRUST ISSUES ARE RAMPANT

Respondents cite skepticism of leadership 33% of the time, but their own negative experiences and distrust are equally to blame for lack of confidence and trust in automation. Only 20% say they can restore from backup within a few minutes.

> Automate to enable best practices and build confidence with capabilities that include reliable daily backups, storage of changes, verification and validation of backups, notification and retry of unsuccessful backups, and accurate reporting.

PROACTIVE GOALS, REACTIVE PROCESSES

Although 62% of respondents say their leadership prioritizes cybersecurity spending on prevention over response, 93% are dissatisfied with their company's current approach to automation which hampers proactive measures. Case in point: 56% say the last time they were breached it was due to a known vulnerability being exploited.

> Equip teams to be more proactive with capabilities that automate discovery of new systems, prioritize and patch vulnerabilities and upgrades based on risk profiles, and validate and even manage compliance.

For more detailed findings and additional recommendations, keep reading.

Introduction

In today's multi-cloud era, modern enterprise-class networks are incredibly complex, and every network equipment manufacturer and network security device company has their own specific way that their tools must be monitored, managed and protected. Network operations and network security professionals struggle to address these requirements and keep pace with the speed of network updates. The simplest configuration change or even a typo can sometimes have a ripple effect that results in downtime or disruption. In just the first month of 2023, a multinational technology and collaboration company, a top blockchain platform, and a large Canadian health organization all experienced publicly reported network outages that disrupted critical services for their customers.

Network outages like these are both common and costly. Uptime Institute's 2022 Outage Analysis report points to network-related issues as the single biggest cause of all IT service downtime incidents with costs ranging from at least $100,000 in total losses to upwards of $1 million, and nearly 30% last more than 24 hours, up from 8% in 2017. Yet, many organizations are woefully underprepared for them, revealing the importance of not just automating improvements to network operations and security, but recovering quickly and minimizing downtime when disaster strikes. As of 2022, Gartner found that less than 35% of network activities were automated.

Why are so many organizations suffering from outages that take hours and even days to recover from? What barriers exist to network automation and where can they focus to make their network infrastructure more reliable, agile and resilient?

To understand how network operations and security professionals on the front lines view and are navigating automation, we decided to undertake a survey focused on:

- The current state of network automation adoption
- The challenges network operations and security professionals face doing their jobs
- Confidence and trust in automation
- Opportunities for network automation moving forward

Methodology

Leading network automation provider, BackBox, commissioned a survey undertaken by independent research organization, Wakefield Research, between January 26 and February 2, 2023. The survey included responses from 250 network operations and network security professionals in companies with 500 or more employees.

Key Findings

1 The Importance of Network Automation and Benefits

Network automation is important to network operations and network security professionals, with 98% saying that having more automated network operations will allow their team to focus on more impactful work. Respondents also see tremendous value to the organization itself, with 96% saying that scaling the business is impossible without automating network operations. However, despite widespread awareness and appreciation for the value network automation provides, almost half (48%) report their company has not implemented or deeply invested in network automation.

RECOMMENDATIONS:

Network operations and network security professionals see the benefits of automation, but many lack the tools and technologies to implement network automation within their organization. Every organization is at a different point in their journey to network automation and the ultimate destination and definition of being "deeply invested in network automation" will vary based on the scope of the network infrastructure, resource availability and team skill sets.

As a rule of thumb, to begin to deal with network and security device complexity, organizations often start with simple outcomes: reliable backups, simple software updates and configuration updates. As their adoption of network automation matures, they find value in more advanced automations like inventory management, compliance validation and automated remediation.

Automating day-to-day, time-consuming administrative work frees up teams to focus on more strategic tasks and decision points that move the business forward and require their expertise and experience. Such activities include R&D and growth-related initiatives like evaluating and deploying additional network infrastructure to support evolving business models, honing processes to drive efficiencies, establishing additional compliance policies, and aligning measurement and reporting with the needs of the organization.

As multi-vendor networks proliferate, so does the complexity of network and security device management tasks. Network automation helps businesses scale operations if the solution is designed to include capabilities like:

- Integration with a broad ecosystem of devices from a variety of vendors across multi-cloud and on-premises environments to support a variety of use cases.
- Flexibility to adapt to how the network evolves over time, for instance enabling automated discovery of new devices and systems, and providing low code/no code methods that allow business users to add or customize automation tasks.
- Task automation to push common configurations seamlessly across numerous devices at one time, with options to build custom chains of automation to simplify entire processes.
- Centralized device management that is comprehensive enough to handle a range of thousands of different tasks and enterprise functions that lend themselves to automation and maintain real-time inventory information.
- Availability and redundancy by providing system visibility, management, and security even during downtimes and system outages.

Network automation puts network operations and security professionals in the driver's seat, able to transform the entire IT estate to become more reliable, agile and resilient in the face of shifting technological and business conditions and rapid growth.

96%

Say scaling the business is impossible without automation.

2 Network Operations and Security Professionals Struggle to Keep Pace

Digging deeper into the environments they operate in, on average network operations and security professionals make use of four tools for network automation, including nearly half (45%) who use five or more. Yet for all the technology, 42% report that network operations issues often arise that require manual work and can't be addressed automatically.

As tech stacks grow, it becomes more difficult to keep networks up to date, and larger companies are less likely to maintain updates than their smaller-sized colleagues. In fact, more than half (53%) of all companies surveyed only update their network and security devices quarterly or less, and that number jumps to 68% for companies with more than 1,000 employees.

It's not surprising then that the vast majority of network security and operations pros (92%) agree there are more network updates needed than they can keep up with.

RECOMMENDATIONS:

The reason organizations invest in network automation is to stay efficient, secure, and agile in the face of rising network complexity and changing business circumstances. Reducing the number of tools in the NOC stack is an important step in that direction. This includes legacy tools that were bought to automate network changes but have fallen out of use, and home-grown automation tools that require major updates to handle new requirements.

Integrating remaining tools like service desk tools and network monitoring tools within an overarching network automation strategy is also essential to reduce fragmentation and drive successful automation. A network automation platform should work in multi-cloud and on-premises environments, be vendor-agnostic, and support a best-of-breed ecosystem comprised of devices from multiple vendors.

The final component to a successful network automation strategy is to ensure the network automation platform stands up to the scrutiny of industry standards and methodologies for security and compliance, and reduces the need for human intervention in infrastructure management. For example, a record 26,448 software security flaws were reported in 2022, with the number of critical vulnerabilities up 59% from 2021 to 4,135, according to an analysis by The Stack of data on Common Vulnerabilities and Exposures (CVEs). These numbers are the equivalent of a new CVE being identified every 20 minutes and illustrate the pressure to regularly update device operating systems to patch vulnerabilities.

92%

Say more network updates are needed than they can keep up with.

53%

Update their network and security devices quarterly or less.

A network automation solution can help companies automate the deployment of patches and upgrades for firewalls and other network devices on a weekly schedule, with the ability to inject high priority upgrades in near real-time, as a part of their network automation, compliance and cybersecurity strategies.

3 Confidence and Trust Issues Are Prevalent

Automation is becoming increasingly necessary for network operations and network security professionals, yet 80% cite distrust and skepticism as top barriers to increasing their use of network automation, due to factors including previous negative experiences (35%), distrust of more automated solutions (38%) and skepticism by leadership (33%).

When asked if they completely trust their current approach to automating network changes, only 24% of network operations and security professionals say they do. And only 20% are completely confident in their ability to rapidly restore their network from backup within a few minutes of an outage or misconfiguration.

While 93% of respondents who haven't invested deeply in automation say they often address network issues by fixing the immediate problem without addressing the root cause, the fact that 60% of respondents who have invested deeply in automation say the same underscores a lack of confidence and trust in automation.

RECOMMENDATIONS:

While outages can be caused by a small configuration change or typos, the greater concern is how long it can take to restore service. Downtime is costly in terms of real dollars but also reputational damage, which is nearly incalculable. Network teams also feel the pain. Many have targets of five or six nines of availability – which equates to five minutes of downtime or less per year – and are often at least partially bonused based on network reliability. When only 20% say they can restore their network within a few minutes, the pain is real for teams, organizations and customers.

Network automation solutions offer a range of capabilities and support best practices that help teams and leadership gain confidence and trust in network automation and ensure business continuity. For instance, network automation solutions can enable automated backups of all devices on the network – even discovering and backing up new devices as they are added, schedule and store any number of configuration backups for as long as needed, and automatically verify backup processes and validate the quality of backups. At a minimum an automation platform should create backups daily as well as before and after changes. Pre- and post-checks with automated reporting of device backups that failed, and the ability to automatically retry unsuccessful backups, ensure all devices are covered and enable teams to minimize manual work by quickly ferreting out devices that truly need human attention.

In many cases outages don't occur immediately after a configuration change so getting to the root cause is challenging. The ability to store a long history of backups within an autoscaling, fault-tolerant data store enables teams to access the data they need to go back in time to correlate past configuration changes during root cause analysis. Successful troubleshooting instills confidence that the problem has been fully remediated and service has been fully restored.

80%

Cite distrust and skepticism as top barriers to network automation.

62%

Say their leadership prioritizes spending on prevention over response.

20%

Are "completely confident" in their ability to restore from backup within a few minutes of an outage.

4 The Management Disconnect

A majority (62%) of respondents say their leadership prioritizes cybersecurity spending on prevention over response. Having a leadership team that values proactive approaches to cybersecurity should be good news for network engineers responsible for security.

However, 92% feel overlooked compared to IT teams in their contributions to ensuring company security, and 93% are dissatisfied with their company's current approach to automation which doesn't enable them to be as proactive as they could be. Top reasons cited include difficulty adding new automations, only partial network coverage, compliance concerns, poor integration, piecemeal approaches, and too much manual interaction required.

More than half (56%) of respondents report that the last time their company experienced a cybersecurity breach it was due to a known vulnerability being exploited and 61% of companies only upgrade network and security devices quarterly or less frequently. This further points to a disconnect between management's focus on prevention and the capabilities of NetOps teams focused on security to do so.

93%

Are dissatisfied with their company's current approach to automation.

56%

Report that the last time their company experienced a cybersecurity breach it was due to a known vulnerability being exploited.

RECOMMENDATIONS:

There are several best practices and automation capabilities that can help teams be more proactive and align network operations and device security with the goals of the business. Here are just a few to consider:

- Being proactive starts with having a full understanding of the network and how it changes over time. That's why capabilities like automated discovery of new devices and integration with ITSM tools and CMDBs are essential.
- Unpatched software is a top access route for hackers and, according to the UK's National Cyber Security Centre (NCSC), patching remains the single most important thing organizations can do to secure their technology. As discussed earlier, more effective approaches to automation enable proactive patching of vulnerabilities and more timely upgrades without the need for manual intervention.
- As automation adoption matures, more advanced applications include enabling proactive compliance validation and management. Capabilities include comparing collected configurations with corporate standards and any regulatory compliance requirements that the organization is subject to, notifying when gaps are detected and, ideally, automating the remediation process.
- Integrating vulnerability intelligence and risk data into the mitigation strategy enables network teams to accurately and systematically prioritize upgrades based on the organization's risk profile, decreasing risk while doing updates more rapidly.
- Finally, detailed reporting and metrics go a long way to elevating conversations with leadership and help drive a more strategic approach to investment in network automation. This is also an effective means for network teams to raise awareness for the value they deliver to the organization. For example, automation of operational and security audits with preemptive network health checks provide measurable data to help prevent problems and verify proper operations before an issue affects the network.

Conclusion

Network automation is a key enabler of digital transformation and critical to scaling the enterprise while enhancing security. As the survey revealed, network operations and network security professionals see the benefits of automation, but many lack the tools and technologies to implement network automation in a way that will allow them to be more proactive, trust the outcomes, and demonstrate value to the organization. Fortunately, leadership teams prioritize prevention over response and network automation is a critical enabler.

Every organization is at a different point in their journey to network automation and the ultimate destination will vary based on the scope of the network infrastructure, resource availability, and team skill sets. Modern network automation platforms can accelerate that journey with a range of capabilities and support for best practices that help teams and leadership gain confidence in automation, be more proactive, and enable business continuity. At BackBox we see that organizations are on the right track, automating a number of functions in today's multi-cloud networks — from connectivity, monitoring and management, to strengthening security posture and risk mitigation — to drive efficiency, availability and security at scale.

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**