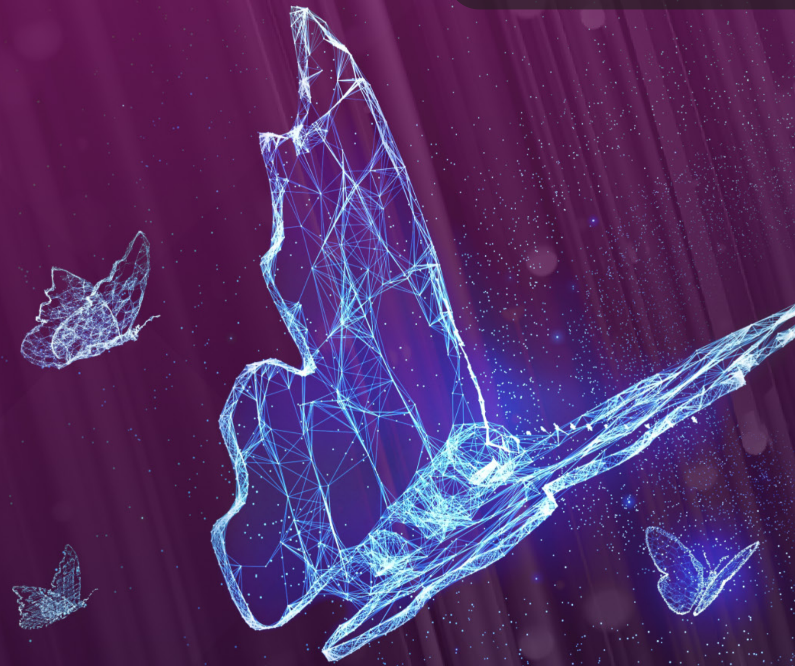
REPORT



SKYBOX® SECURITY

The Network Butterfly Effect: The Hidden Cost of Network Security Policy Management

Executive Summary

In high-stakes and highly regulated critical industries, network complexity is not just a challenge – it's a looming threat.

Large organizations operate vast networks with thousands of interconnected endpoints and devices, governed by thousands of firewall rules, each representing a potential risk.

But a single misconfiguration, like the proverbial butterfly's wings, triggers a cascade of unintended consequences, impacting security, compliance, and operational uptime. This "Butterfly Effect" creates a constant undercurrent of risk, stifling innovation and agility.

Based on the feedback of 500 networking professionals working in critical national infrastructure industries such as financial services, energy, healthcare, and manufacturing, this report reveals the magnitude of challenges network professionals face in the age of digital transformation:

Manual tasks consume nearly half (40%) of their workweek, rising to over 50% in larger organizations.

Pernicious misconfigurations add to this burden, with professionals spending an additional 10% of their working week correcting these errors.

Compliance concerns also pose a major issue for network teams, with 91% of professionals worried about internal audit failures and 89% concerned about external audits.

The looming risk of non-compliance and the potential for severe penalties and reputational damage highlights the need for stronger network management and regulatory strategies.

The answer to these issues lies in automation. Network professionals view automation as the most impactful technology for transforming their work to reduce the time spent on manual processes, reclaim 40% of network teams' workweek, minimize the need to work out of hours, maintain compliance and enhance overall performance.

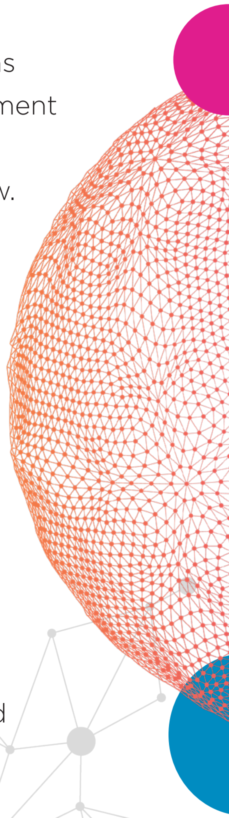
This report highlights the urgent need for organizations to embrace automation to mitigate risks, improve compliance, and empower network teams to shift their focus from routine tasks to higher-value initiatives. It also offers practical insights that will empower network teams to scale to meet the demands of agile organizations, ensuring stability and business resilience and keep up with the demands of digital transformation without fearing the consequences.

The cost of managing complex networks

Critical industries - such as financial services, energy, healthcare, and manufacturing - rely heavily on seamless network performance to maintain operations. For these sectors, network compromise is not an option. It results in significant financial losses, safety risks, and regulatory breaches. As these sectors continue to undergo rapid digital transformation, network teams face increasing pressure to ensure uninterrupted connectivity, security, and performance.

The expectation is that businesses deploy applications and services quickly, often leveraging technologies such as cloud services and payment gateways. However, in large corporations, these new services must integrate with an already vast and complex network of firewalls and devices. The challenge is not only the increasing number of demands for agile innovation but also the accelerating complexity of managing this growing infrastructure. The interplay between on-premise and cloud technologies and their interdependencies makes this task even more challenging.

Managing these complex networks is time-consuming, costly and error-prone. Network teams must navigate an increasing amount of data, held in separate silos, making efficient management even more difficult. The need for streamlined, unified approaches to network management is urgent as digital transformation accelerates and the demands on network infrastructure grow.



A manual burden on network teams

Despite automation in many areas of an organization, many network managers still lack the tools they need to automate their tasks and improve efficiency.

Network professionals lose
of their week to manual tasks **40%**

The networking professionals we surveyed spend on average 40% of their weekly workload performing manual tasks, such as the firewall change process, firewall rule recertification, and network provisioning. This figure rises to over 50% in organizations with more than 10,000 employees.

The challenge is exacerbated by the complex, multi-disciplinary processes required to implement firewall changes. Large organizations, on average, must complete eight separate manual stages - from initial requests to multiple verifications and approvals.

Network teams face a bureaucratic bottleneck with an average of eight manual stages of verification to process firewall changes.

While these steps may not be technically challenging, they are administratively challenging and introduce the risk of mistakes and delays due to miscommunication. Two-thirds of network professionals attributed these mistakes to differing priorities and objectives (63%) and insufficient collaboration (62%) across teams. Interestingly, in financial services, inadequate documentation of changes was cited as the main cause of miscommunication.

62% attribute these mistakes to differing priorities and insufficient collaboration across teams.

Intensifying regulatory compliance

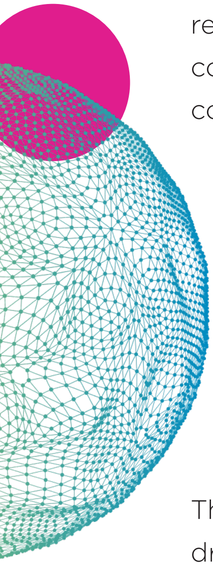
Network teams are not only grappling with the demands of digital transformation within their organizations but also with an increasingly complex regulatory landscape. As networks grow in scale and complexity, ensuring compliance with industry guidelines and legislative frameworks becomes more challenging.

Firewall rules, access, and certifications must be continuously monitored to maintain compliance with regulations such as NIST 800-41 and PCI DSS. Network devices, including firewalls, must be properly configured and patched to protect against emerging vulnerabilities. Failure to adhere to these requirements may result in severe penalties, particularly in highly regulated industries, such as financial services and healthcare.

Recent legislative changes add further pressure to respond to cyberattacks. For example, the U.S. President's Executive Order on Improving the Nation's Cybersecurity has set new requirements for critical infrastructure sectors, emphasizing the need for enhanced cyber defenses. Similarly, in Europe, the Digital Operational Resilience Act (DORA) is set to impact financial services organizations by January 2025, while the NIS 2 directive will extend cybersecurity obligations to seven additional sectors, including energy, financial services, and banking. These new frameworks are wide-reaching in their remit but place more weight on these organizations to comply with the firewall compliance frameworks.

The high cost of compliance

Maintaining compliance is a continuous process that requires frequent reassessments. Among the large organizations surveyed, the majority assessed their network security compliance with relevant standards and frameworks every four weeks. However, over half of these organizations conducted assessments at least once per week, highlighting the significant resources dedicated to compliance efforts.



50% of large organizations conduct network security compliance assessments at least once per week

The scale of manual updates, firewall rule changes, and compliance checks has become a major drain on productivity for network teams. Skilled networking professionals spend significant portions of their time on tasks that could be automated, resulting in high costs for businesses. As organizations continue to expand their networks and regulatory requirements become more stringent, the cost of managing these complex infrastructures will only increase unless more effective, automated solutions are adopted.

> "In 2022, the UK's top five banks had a combined number of 2,146,314 firewall rules. That's no small number when you consider how each needs to be regularly reviewed and maintained. Take, for example, that it was 500,000 rules per bank, each taking a fairly conservative average of two minutes to review, allowing for lunch and coffee breaks, that's going to take almost 15 man-years to review. That takes one big team to maintain compliance."
>
> \- **Skybox**

The Butterfly Effect for Networks

The interconnectedness of these vast networks and the siloed data required to manage them results in hidden dependencies, making it difficult for network and security managers to make changes without catalyzing undesired consequences.

This situation creates a “Butterfly Effect” in network management, where a single network misconfiguration or errant rule triggers a ripple of unintended consequences. Such an error often generates a ripple effect, impacting security, compliance, and overall operational uptime.

The Butterfly Effect carries potentially serious implications for organizations:

1. **Cyber risks** - One of the most significant concerns expressed by network and security teams is the potential for network misconfigurations to introduce vulnerabilities that could be exploited by cybercriminals, with over half (51%) of respondents citing this as their primary technical concern. As network estates grow larger and more complex, so does their attack surface, making them increasingly attractive targets for threat actors.
2. **Network downtime** – In today’s always-on world, network downtime is one of the greatest risks of misconfigurations. In fact, 45% of network and security professionals view downtime as a major risk associated with network misconfigurations, with downtime resulting in potential financial loss. IT teams are measured on the availability of the network and networked assets, with disruptions having serious business consequences.
3. **Loss of customer trust and reputational damage** - The ripple effects of network issues often extend beyond technical disruptions. Over half of network and security professionals recognize that misconfigurations, whether disrupting the availability of services or risking the exposure of sensitive customer data, extend beyond immediate disruption to impact customer relationships and business success.

90% of network managers fear failing compliance audits due to preventable misconfigurations

An additional consequence of the Butterfly Effect is unnecessary friction with ensuring regulatory compliance. Maintaining compliance with various legislative regulations, such as PCI DSS and NIST 800-41, is a top priority for organizations. However, network misconfigurations, firewall rule violations, and access weaknesses expose organizations to violations, triggering costly penalties and reputational damage.

89% of network and security professionals expressed concern about failing an external audit due to misconfigurations, while 91% are concerned about failing an internal audit. And with good reason, less than 3% of network and security managers could confidently say their organization hasn't identified any failings in their internal or external network security audits that could have resulted in a security breach over the past five years. Instead, the majority (73%) reported identifying two or more failings as part of an external audit during this period.

Non-compliance presents a huge risk to organizations. For example, organizations failing to meet PCI DSS compliance, risk facing fines ranging from $5,000 to $100,000 per month until the violations are resolved. Indeed, the scale of these risks was demonstrated by high-profile cases such as the $229 million fine British Airways received following a data breach that compromised the personal data of 500,000 customers.

73% of network teams identify multiple failures in external audits over the past five years

Beyond the immediate risks to security and compliance, network misconfigurations carry a substantial operational cost. Overall, the top concern amongst networking professionals was the time-consuming process of identifying and correcting errors and the burden of remediation which significantly adds to their workloads. Network teams spend, on average, an additional 10% of their time remediating misconfigurations each month. This increases in line with organization size, rising to 12% of their time every month in companies with a headcount of over 10,000 employees.

This heavy workload not only hinders efficiency, but also contributes to high turnover among networking professionals as the highly manual and unfulfilling tasks dominating their roles lead many to seek more interesting and fulfilling roles.

The time-consuming process of identifying and remediating misconfigurations on their workload is the biggest concern networking professionals have about the Butterfly Effect of network management

Understanding every ripple

As organizations continue to scale, the challenge of managing network configurations has grown exponentially. The best way to reduce the amount of time spent remediating misconfigurations is to reduce the rate at which they are introduced.

However, traditional approaches to network management fall short of providing the visibility or scale required to securely manage modern, complex networks. The lack of real-time visibility, the intricate interdependencies, and the potential for human error make it difficult to ensure network security and performance.

To enhance resiliency and security, and reduce the operational costs of network management, network teams must embrace new ways of working. The focus must shift to understanding and pre-empting the full scope of every ripple across the network—anticipating how each change, no matter how small, affects the organization.

Network and security experts have identified the most impactful capabilities that help them pre-empt the unintended consequences of network management and manage the Butterfly Effect, including:

Live Network Models

A dynamic visual model of your entire hybrid network, this "digital twin" of the real environment allows both security and network teams to visualize and interact with the network topology, assets, security controls, and access paths without directly impacting the live network.

This approach offers two primary advantages, recognized by over half of network and security professionals:

1. **Test network changes before committing** - By testing changes in a live digital twin of the network, organizations identify and address potential issues before they impact the production network. Assessing the change prevents the exposure of a known vulnerability, opening up an access route to an attacker, breaking a compliance directive, negatively affecting firewall hygiene, or causing un-scheduled downtime. Validating changes in this live sandbox before deployment not only increases confidence in network updates and reduces the risk of downtime, but enables faster innovation and deployment of new technologies and services.
2. **Check compliance continuously** - In critical industries with stringent regulatory requirements, maintaining regulatory compliance across a large number of firewalls and network devices requires active and constant management. Whether an organization has a small or large amount of firewalls, auditing each to ensure compliance before making network changes or providing an aggregated view for an auditor is a time-consuming task. With a live model of the network, this process runs automatically to generate reports to inform decisions that both prevent new exposure and continuously remediate existing risks.

Integrated threat intelligence

Another crucial capability is integrating live threat intelligence into network management. Live threat intelligence feeds provide real-time information about emerging threats and vulnerabilities, helping teams stay ahead of evolving risks. In fact, two-thirds of network and security professionals want to see this integrated into their network security policy.

This integration offers two key benefits:

1. **Keep up to date with live vulnerabilities** - Network managers must adhere to regulatory requirements, which often include tight timelines for patching known vulnerabilities. By incorporating live threat intelligence into their workflows, teams ensure that vulnerabilities are patched proactively, even if the affected device isn't currently under review. This helps prevent gaps in security and maintains compliance across the entire network.
2. **Prevent new risky network routes for malicious actors** - When making a network or access change, understanding whether any of the devices through which traffic will be routed has a vulnerability enables better collaboration between network and security teams to secure that new access route. Patching the application before implementing the network change is critical to inadvertently opening a new door into the network to malicious actors.

Combining live threat intelligence data with network security policy management enables network teams to assess the risk of potential changes before they are implemented, limiting the impact of unintended consequences.

While **90%** of organizations stated they have formal processes in place for network and security teams to collaborate on vulnerability and exposure management, communication and coordination between these two teams is a challenge.

Our research found that **45%** of organizations experienced miscommunications that resulted in delays in reporting or addressing security incidents in the past 12 months. This led **75%** of IT and security decision-makers to believe their organization's security posture was negatively impacted by miscommunication between network and security teams.

When network teams operate without a clear understanding of the security implications of the changes they make, unnecessary risks or vulnerabilities are introduced.

That's why **61%** are likely to implement an integrated vulnerability and network security management solution to improve collaboration between the two teams.

Read our article to learn more about how to converge security and network operations for a strategic advantage:

Breaking Down Exposure Management Silos: Confronting the Network-Security Disconnect ›

Amongst networking professionals at every level, automation is perceived to have the greatest impact on network management - from the Head of IT Operations (78%) through to NOC Managers and Network Engineering Managers (88% and 78% respectively). Network teams recognize the transformative potential for automation to reduce time spent on manual processes, allowing them to focus on more strategic tasks and reducing the risk of human error.

But how can networking teams automate with confidence?

Automation to reduce manual processes topped the list of impactful capabilities by network managers in finance, energy & utilities, and manufacturing

Automating with clarity and confidence

As the complexity of modern networks continues to increase, network automation has emerged as a critical tool for minimizing the Butterfly Effect.

The primary use cases for network automation that help mitigate the Butterfly Effect include:

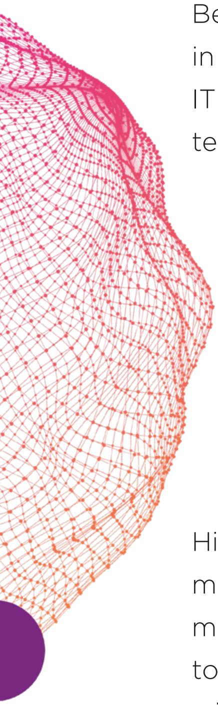
1. **Identify misconfigurations** - Automation is used to analyze and enforce rules, access, and configuration policies for firewalls and network devices enabling networking professionals to foresee all the possible implications of a network change and anticipate misconfigurations quickly, reducing the risk of introducing errors.
2. **Optimize workflows** - By automating tasks like security posture assessments and rule recertification, businesses optimize their workflows and achieve greater precision in change control, ultimately enhancing their overall resilience.
3. **Replace manual tasks** - Automation significantly reduces the time spent on repetitive tasks like firewall rule management and device provisioning. These time-consuming tasks are prone to human error, especially in large, complex networks. Automating them not only reduces the risk of mistakes, but also allows network teams to focus on more valuable tasks.

The implementation of network automation drives significant business value across multiple areas. Firstly, it significantly reduces the cost of complexity for organizations. Automation provides enhanced visibility and control over network operations, a benefit cited by 60% of network and security professionals. With better visibility, network teams quickly identify and address potential issues before they escalate, preventing costly downtime and outages. Automation also helps organizations optimize their deployment of specialist networking talent by reducing manual tasks and the need to roll back up to 30% of changes that network professionals anecdotally indicated include misconfigurations.

60% of network professionals find automation provides enhanced visibility and control over network operations

Secondly, it improves the overall professional experience. Networking professionals bear the cost of manual processes, often working long hours to keep up with the growing number of demands for network changes as they accelerate with the increased pace of the modern enterprise. Automation alleviates this burden, with 57% of networking professionals anticipating it would reduce the need to work outside of contracted hours.

Beyond individual benefits, automation also has the potential to improve cohesion between teams in the IT office. More than half (55%) believe automation would enhance collaboration with other IT and network teams, thanks to its potential to break down information silos and free up time for teams to collaborate on higher-level projects and initiatives.



Automating manual processes tops the network transformation wish list, with **57%** of networking professionals anticipating it will reduce the need to work overtime

Highly skilled networking professionals currently spend a large portion of their time performing manual, repetitive tasks. While once a necessary evil to support digital transformation and maintain security and compliance, this allocation of time and resources detracts from their ability to contribute to more strategic initiatives. As we've touched on, automation changes this dynamic, with 62% of professionals expecting it will provide more time to focus on higher-value tasks, such as designing and implementing innovative network solutions and optimizing network performance.

Automation also opens new doors for skills development and career growth within network teams. By reducing time spent on routine tasks, automation frees up the capacity for networking professionals to pursue additional training and gain expertise in emerging technologies and cybersecurity. In fact, 65% believe that automation leads to increased opportunities for training and skills development, helping them directly support their business's future success.

Overcome the Butterfly Effect using smart automation

In large organizations, automation is the only way to keep up with the complexity, compliance, and cost of network management.

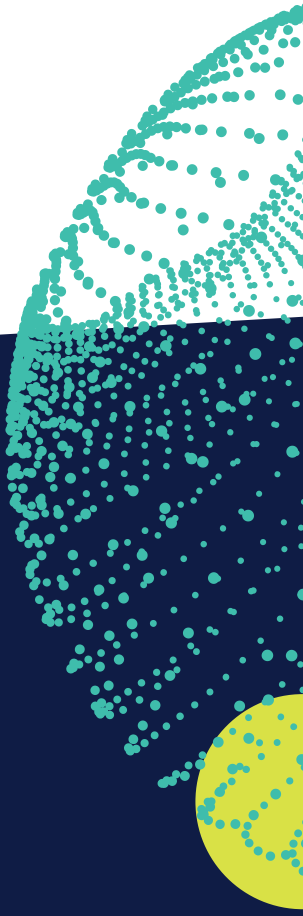
It not only fortifies business resilience by minimizing security and compliance risks at scale, but also empowers networking teams by eliminating repetitive manual tasks, reducing the risk of making errors, and freeing them up to focus on higher-value activities that align with the company's strategic goals.

This transformation overcomes the Butterfly Effect of network management, releasing professionals from the burden of managing the constantly cascading and unpredictable effects of misconfigurations. Ultimately, ensuring stability and control in an increasingly complex digital landscape.

Learn how Skybox enables organizations to reduce the risks and costs associated with managing firewall and network security policies across large, complex networks.

Want to learn more? Get a demo or talk to an expert:

skyboxsecurity.com/request-demo



METHODOLGY

This report is based on research conducted by Censuswide of 500 Network Operations Managers, Network Security Architects, Head of Infrastructure, and comparable roles. Respondents were working in organizations of over 1,000 employees in the CNI industries and manufacturing based in the U.S. and UK.

ABOUT SKYBOX

Over 500 of the largest and most security-conscious enterprises in the world rely on Skybox for the insights and assurance required to stay ahead of their dynamically changing attack surface. Our Continuous Exposure Management Platform delivers complete visibility, analytics, and automation to quickly map, prioritize, and remediate vulnerabilities across your organization.