DARKREADING
RESEARCH

DECEMBER 2024

The State of Firewall Security

Commissioned by Tufin

tufin

Executive Summary

The challenges of firewall security are as pressing as ever. Many organizations remain bogged down by manual processes, with change management often turning into a cumbersome bottleneck. IT teams are grappling not only with outdated and redundant firewall policies, but also with frequent errors and misconfigurations caused by manual operations that threaten network security. For over a third of organizations, gaining the foundational network visibility and control necessary for automating and orchestrating these tasks feels like an uphill battle.

The rise of cloud computing is further complicating matters. It is creating a shift in responsibility for security policy beyond simple firewall rule management out to the computing edge, and hence adding layers of complexity, management, and cross-functional collaboration to already strained teams and systems. Hybrid environments have become the norm; organizations must navigate new security challenges without losing control of their on-prem and cloud infrastructure.

Against this backdrop, the demand for smarter security automation and orchestration is more urgent than ever. With cybersecurity talent shortages growing, threat actors enabled by AI moving faster than ever, and economic pressures limiting budget increases, organizations can no longer rely on manual methods. Business leaders and regulators alike are demanding more transparency and efficiency, pushing for security orchestration, automated remediation, AI-driven policy management, faster and more accurate audit response, and enhanced compliance documentation.

Yet, the data we collected paints a sobering picture. In September 2024, Dark Reading conducted a survey on behalf of Tufin resulting in data from 105 IT and cybersecurity management professionals at companies with 20 or more firewalls. Even for core security functions like firewall management, many organizations are far from the maturity level to be able to automate and orchestrate network security tasks. The Dark Reading 2024 State of Firewall Security Survey reveals that despite the critical and fundamental importance of firewalls, a significant portion of organizations — large or small — still rely on manual processes to manage dozens, if not hundreds, of firewalls. Even at some of the largest enterprises, firewall changes and policy revisions are tracked manually, often in outdated spreadsheets, leaving organizations vulnerable to security gaps, unmanaged attack surfaces, risky security postures, and compliance risks.

This report draws data from respondents at all company sizes, but it also drills down to highlight some differences in our findings across the total respondent base compared to those at large companies with 2,500 or more employees. Even at the largest organizations, keeping a handle on all of the changes and policy revisions controlling firewall functionality is still largely done by hand in a spreadsheet.

The following are some of the highlights that will be examined further in the report:

- **Firewall management is a huge task:**
  Almost a third of organizations surveyed manage large complex networks protected by 100 or more firewalls from the likes of Cisco, Palo Alto, and Fortinet. Almost 1 in 3 of these organizations is inundated with more than 50 change requests per week, and staff at half of large organizations spend more than 10 hours per week managing these requests.

- **Firewall management takes a lot of collaboration and friction abounds:**
  The percentage of companies that put firewall management at the feet of IT infrastructure teams slightly outnumbers those that put security teams in charge — but a significant number of firms have multiple departmental stakeholders actively managing firewalls. This introduces points of friction that are only getting exacerbated by adding cloud teams to the mix. Half of large organizations say it is painful for their network and cloud teams to collaborate on firewall management.

- **Manual tasks persist:**
  Only half of organizations today use some form of automation to manage firewall policies, which leads to redundant, shadowed, and outdated firewall policies at nearly the same percentage of firms. Many firms are also challenged by errors and misconfigurations, due to the persistence of manual work and a strong reliance on spreadsheets to track and orchestrate network changes.

- **These issues result in more risk and poor business outcomes:**
  The collaboration challenges and manual work are resulting in more risk and poor business outcomes, with around a third of organizations saying they experience more than 10 service disruptions per year due to firewall configuration changes. Firewall management issues are also causing a delay in many organizations in implementing zero trust initiatives.

- **Situational blindness:**
  Few enterprises engage in ongoing or continuous assessment of their cloud and SaaS environments. The rest do security assessments at intervals that range largely from once a quarter (18% for cloud, 11% for SaaS) to once a year (25% cloud, 26% SaaS), and in some cases not at all.

- **Difficulty patching:**
  Enterprises are also concerned about adversaries exploiting un-patched vulnerabilities in web applications (39%) and cloud environments (23%). Almost 1 in 5 say they have difficulty applying security updates and patches, creating a situation where organizations are exposed to attack as a result of exploitable vulnerabilities.

- **Sluggish response:**
  Topping the list of IR concerns are a lack of skilled workers (49%), limited visibility into cloud and hosted environments (46%), and the inherent com-plexity of cloud-centric incidents (46%).

Firewall Management Scope

The Dark Reading 2024 State of Firewall Security Survey found that respondents are charged with managing dozens to hundreds of firewalls at a time. Over half manage more than 50 and nearly a third manage 100 or more firewalls. Digging into the types of firewalls under management, we discovered there's no technological monolith across survey participants. The most common firewall vendors in place are fairly evenly distributed, with Cisco (55%), Palo Alto (44%), and Fortinet occupying the top three, followed relatively closely by Azure and Juniper (**Figure 1**). At organizations with 2,500 or more employees, the top five remains the same with a slight shakeup in order: Cisco, Palo Alto, Azure, Juniper, Fortinet.

With complex networks in place, organizations must move on numerous network change requests each week. Twenty-eight percent of organizations of all sizes field over 50 change requests a week, and 8% tackle more than 350 (**Figure 2**). Meanwhile, at larger enterprises those request volumes increase significantly. Almost half of organizations with more than 2,500 employees are called to handle more than 50 requests per week. Twelve percent of these enterprises field over 1,300 change requests per week.

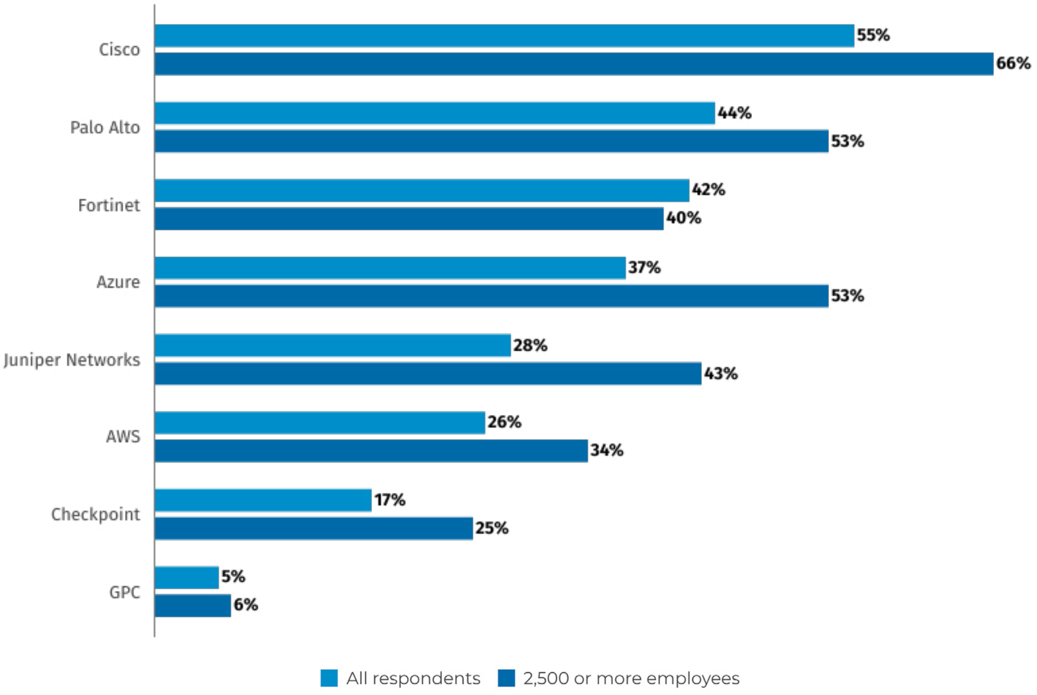
The scope of work around these change requests takes a lot of people hours to carry out across multiple departments. A third of those in charge of firewall management personnel say they or their teammates spend more than 10 hours a week dealing with change requests (**Figure 3**). At larger organizations, this burden is even heavier with half of firewall management staff spending the same amount of time each week dealing with change requests.

These findings highlight the substantial burden of firewall management, especially at larger organizations, where the volume and complexity of change requests are particularly high. As firewall infrastructures grow more intricate and diverse, with a variety of vendors in use, organizations face significant challenges in maintaining their

Figure 1

FIREWALL VENDORS IN USE

Which firewall vendors and/or cloud providers are currently in use in our organization?



Base: 105 respondents with 100 or more employees and 53 respondents at companies with 2,500 or more employees
Note: Multiple responses allowed
Data: Dark Reading survey of 105 IT management pros at companies with 20 or more firewalls, September 2024

security posture while responding to frequent network changes.

This ongoing demand for resources not only increases operational strain but also underscores the need for automation and streamlined processes to improve efficiency. Without such measures, managing firewall configurations and network changes can quickly overwhelm IT teams, leading to potential delays in addressing security issues and a higher risk of configuration errors.

Roles and Responsibilities

It's typically either the IT infrastructure team of someone in security who is, ultimately, responsible for managing firewalls. Some 43% of organizations say their IT team executes these duties, while 39% say either network security or InfoSec leads these activities. In most instances, though, there are a lot of cooks in the proverbial kitchen when it comes to tending the firewall. Some 43% of respondents stated that other teams beyond those ultimately responsible for the state of the firewall have a hand in actively managing them.

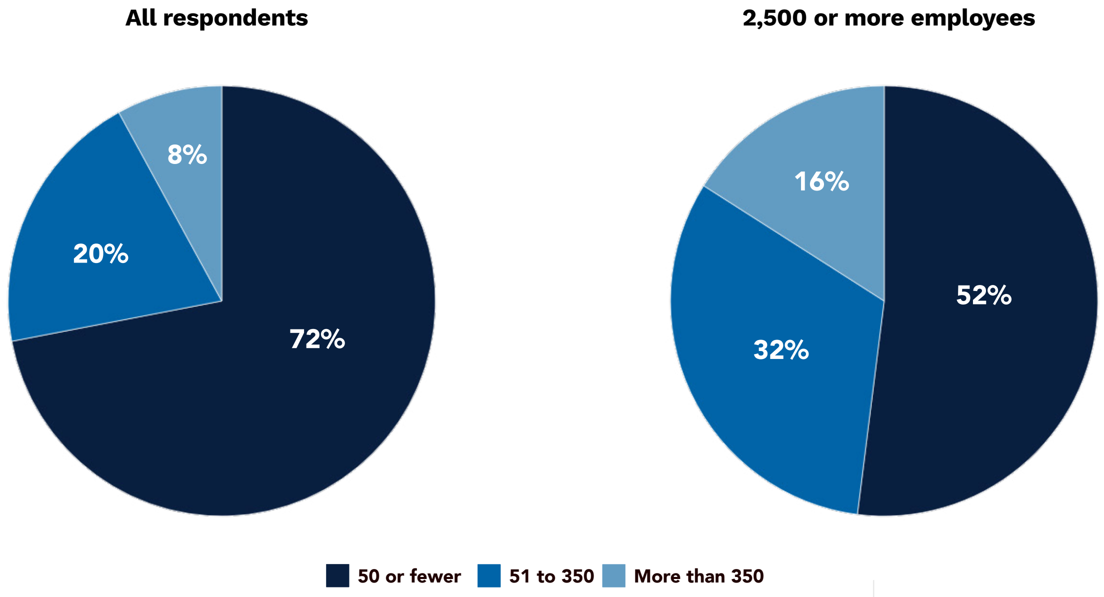
In addition to the IT infrastructure and security stakeholders, those most likely to influence firewall policies include risk management teams (31%), MSPs (24%), and DevOps and cloud teams (20%). This will inevitably introduce more points of friction and conflicts between teams that have different objectives. Even within just the IT networking team, the 2024 State of Networking Report released by Network Computing in April 2024, showed that network security may be the top challenge the team is focused on, but only by a hair (cited by 27%) — they've also got to contend with reducing cost (23%), improving network performance/efficiency (20%), network monitoring/observability (18%), and staff training issues (15%).

It only follows that collaboration challenges will mount as more teams — including DevOps, cloud, and even third-party vendors — contribute to firewall management efforts. These frictions often stem from differing priorities, workflows, and levels of expertise, which can hinder effective coordination. Addressing these challenges requires not just technological solutions but also a strategic

Figure 2

NUMBER OF NETWORK CHANGE REQUESTS

How many network change requests do you field on a weekly basis?



Base: 105 respondents with 100 or more employees and 53 respondents at companies with 2,500 or more employees
Data: Dark Reading survey of 105 IT management pros at companies with 20 or more firewalls, September 2024

focus on fostering communication and aligning objectives across teams. Without careful work on this front, it becomes a battle of wills and egos to decide who gets the final say between an IT team that wants to open ports for a new project and risk managers who say it will threaten crucial assets or between an MSP needs certain ports open for remote administration and compliance teams who say it will put the company afoul of regulatory demands.

This need for more collaborative policymaking is a common one in security today.According to another survey, the just-completed Dark Reading's 2024 Strategic Security Survey, 66% of respondents said the CISO sets security policies in their organization, while 63% say CIO or IT directors set policies. Another 44% say security managers and administrators set policies, while 42% say IT managers. Firewall management is not alone — security policy work is a team sport, and if sound collaboration and well-defined decision-making processes aren't employed, then conflict and complexity will prevail.

The transition to the cloud is only going to heighten the need for effective collaborative policy management. The firewall survey showed that the shift to the cloud has impacted roles and responsibilities for firewall management at many organizations, especially larger ones. Approximately 45% of large organizations and 30% of the broader respondent pool say that they've seen impacts in who is responsible for managing firewalls due to cloud implementations (**Figure 4**). Unsurprisingly, these shifts in responsibilities have caused friction as teams navigate the political, cultural, and logistic challenges of collaborating across teams, departments, and outside vendors. The majority (51%) of larger organizations say that it's somewhat to very painful for their network and cloud teams to collaborate on firewall change management.

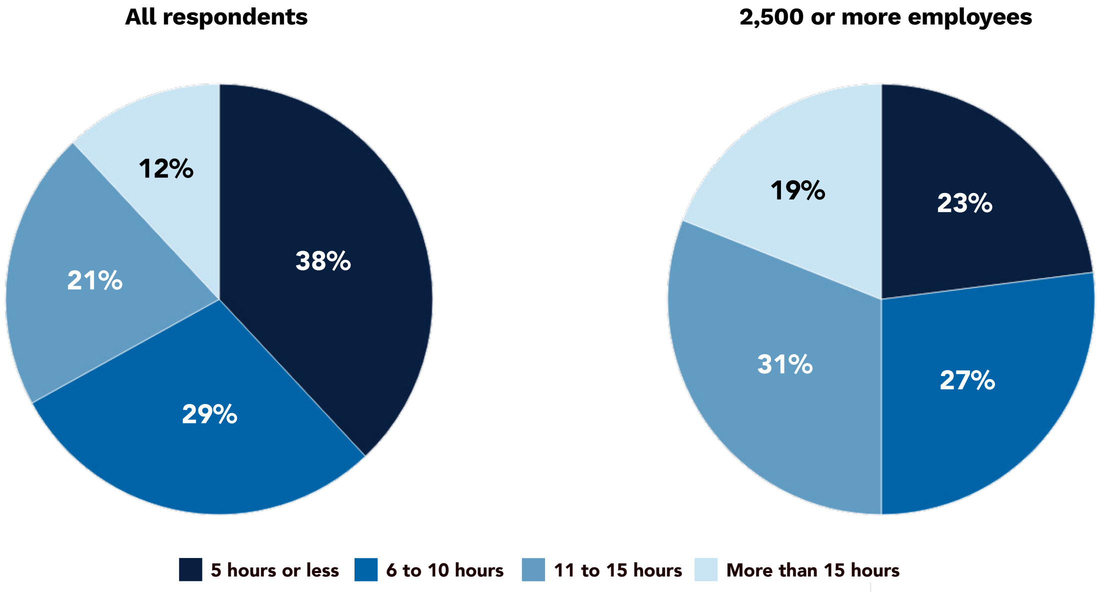
45% of large organizations

have seen firewall responsibilities shift due to transitioning to cloud.

Figure 3

HOURS PER WEEK DEVOTED TO CHANGE REQUESTS

How many hours each week do you and your team field firewall change requests?

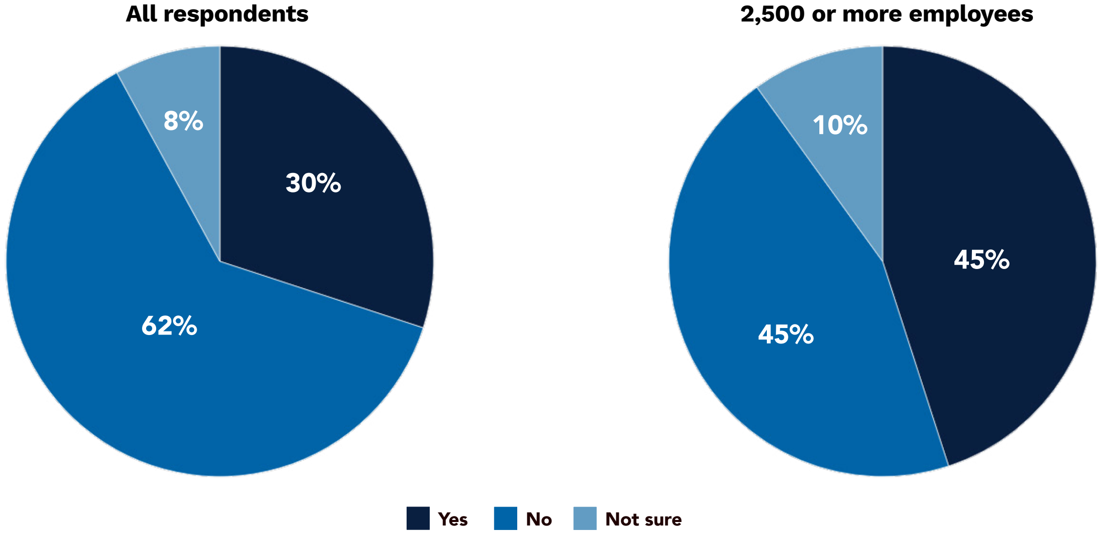


Base: 105 respondents with 100 or more employees and 53 respondents at companies with 2,500 or more employees
Data: Dark Reading survey of 105 IT management pros at companies with 20 or more firewalls, September 2024

Figure 4

IMPACT OF CLOUD ON FIREWALL MANAGEMENT

Has the transition to the cloud impacted who is responsible for managing firewalls?



Base: 105 respondents with 100 or more employees and 53 respondents at companies with 2,500 or more employees
Data: Dark Reading survey of 105 IT management pros at companies with 20 or more firewalls, September 2024

Managing firewall rules is very different in the cloud than in the on-premises firewall world, which will continue to challenge the collaborative framework for IT teams. Additionally, the shift in roles, driven by the increasing integration of cloud technologies, has reshaped the traditional boundaries between IT, security, and other stakeholders, leading to growing pains in managing change requests and policies. This is likely why larger companies with a higher reliance on cloud are especially struggling — they're spending more time navigating these collaboration logistics, which is likely why a third of them take more than 10 hours a week to manage these change requests.

Lack of Automation Lingers

Some of the biggest challenges standing in the way of effective firewall management today stem from a lack of automation in how policies are tracked, managed, enforced, changed, audited, and reported on. A solid half of organizations admitted that manual change management processes are their biggest challenge in managing firewall policies (**Figure 5**). Additionally, 47% say they struggle with redundant, shadowed, and outdated firewall policies and rules, and 42% say they're challenged by errors and misconfiguration. In the meantime, over a third of organizations say they're struggling with the basic prerequisites for solid firewall management automation, namely establishing network visibility and control.

Only half of organizations report that they use some form of automation to manage their firewall security policies and fielding of network change requests. Surprisingly, that number does not significantly rise for large organizations — only 59% of organizations with over 2,500 employees utilize automation for this task. This means that even among the largest enterprises that are ostensibly under significant pressure from the SEC, the board, and customers to maintain high security standards, over 4 in 10 of them are manually managing the daily work around keeping firewall policies updated.

This tracks with other industry data that shows that automation may be lagging in many facets of security today. For example, in the recent report The State of Vulnerability Management in the Enterprise, 74% of security leaders reported they're planning to automate vulnerability management processes in the next year, indicating a need to eliminate manual processes on this front. In that case, the report found leaders were focusing automation on detection and remediation and to streamline workflows for security and operations teams. That striving toward the brass ring of automation was echoed in another Dark Reading study, the Strategic Security Survey, in which one respondent stated that if they could change or improve one thing about their organization's approach to cybersecurity, it would be to "implement automation as far as possible and use proper and adequate governance mechanisms for alerts and mitigation."

50% of organizations say they rely on Excel or other manual technology.

For now, though, automation eludes many and in firewall management this is best illustrated by the heavy reliance on spreadsheets to operationalize and orchestrate network change management processes. An even 50% of organizations say they rely on Excel or other manual technology. That number is just a couple ticks higher for large enterprises, with 54% stating they rely on Excel. In fact, 1 in 10 of these large organizations admit that they rely "a great deal" on Microsoft Excel to execute their network change management processes. Again, this mirrors similar reliance on spreadsheets in other facets of security operations. A 2021 CyCognito/ESG report found that 73% of cybersecurity and IT pros still use spreadsheets to manage security hygiene and posture. While some improvements have been made since then, the spreadsheet is still highly prevalent and firewall management's dependence on Excel remains especially acute. The vulnerability management survey showed 27% of companies still use spreadsheets to remediate vulnerabilities and 19% use "other manual processes."

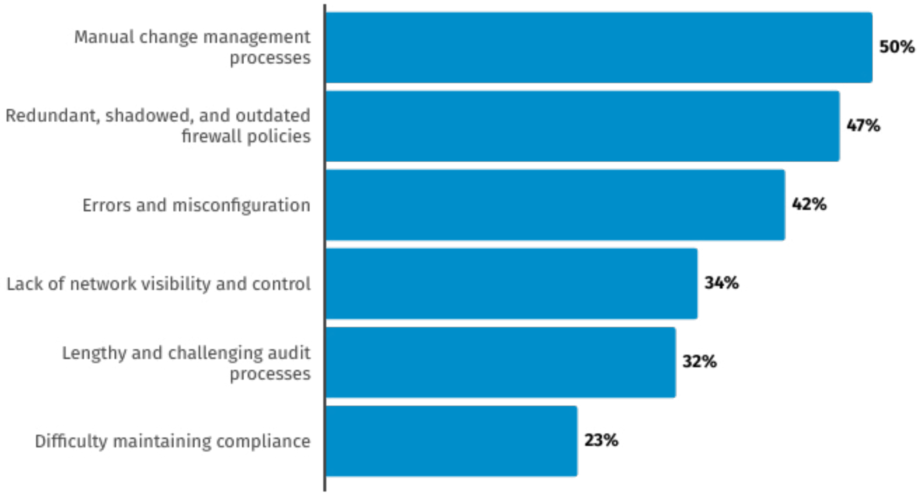
According to Network Computing's State of Networking survey of 196 IT and networking pro-fessionals, network security is the number one network management priority for the next 12 to 24 months, cited by 43%. That study showed that 44% of organizations have increased network security spending in the last year by 5% or more. What's more, more than 1 in 10 organizations say they will increase their network security spending by more than 10% in the coming year. However, the fact that the most basic aspects of network management and network security are still run in the spreadsheet attests to the fact that there's a lot more work to do and that the increased spending will need to be properly targeted.

As things stand, the Dark Reading Firewall Security Survey showed that a significant chunk of organizations that do have automation in place don't always get the most out of it. Just over one-third

Figure 5

CHALLENGES WITH MANAGING FIREWALL POLICIES

What challenges do you currently face when it comes to managing firewall policies?



Note: Maximum of three responses allowed
Data: Dark Reading survey of 105 IT management pros at companies with 20 or more firewalls, September 20244

(34%) of those with automation said that their current automated workflow for change management is not very easily repeatable. These findings suggest that enhancing automation capabilities and ensuring consistent, repeatable processes could be critical steps toward overcoming the current challenges in firewall management.

The data underscores a clear need for organizations to invest in more advanced automation capabilities to address the persistent challenges in firewall management. The reliance on manual processes and tools like spreadsheets not only hampers efficiency but also increases the likelihood of human error, misconfigurations, and outdated policies.

As networks grow in complexity, the limitations of manual tracking become more pronounced, leaving IT teams struggling to maintain security and respond to changes swiftly. For those with existing automation, optimizing workflows to ensure they are repeatable and scalable is essential to fully realize the benefits. Improving automation and streamlining network policy enforcement will be crucial for organizations to achieve robust firewall management, reduce risk, and enhance overall security posture.

Manual Processes Results in Increased Risk and Poor Business Outcomes

The lingering reliance on manual processes is resulting in poor security and business outcomes for many organizations, especially those that run large, heterogenous digital environments. And the transition to the cloud is making things more complicated.

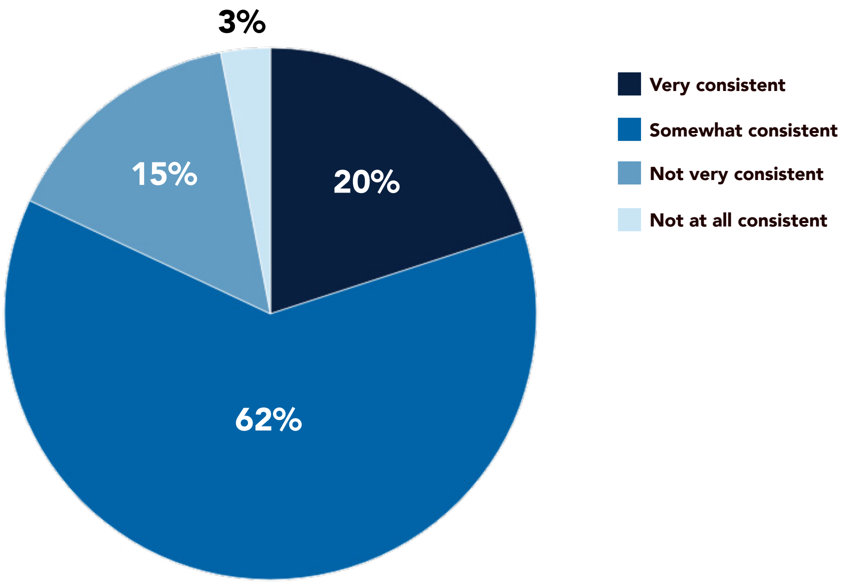
The reliance on manual processes is undermining security and operational outcomes for many organizations, especially those with large and complex digital environments. Only 20% of organizations today say that they're consistently able to execute on firewall management duties across on-premises and cloud network assets (**Figure 6**). While the vast majority of organizations — 71% — report that firewalls and associated security policies are very important to their security posture, their current performance in firewall management leaves something to be desired. Half of the organizations surveyed say they consider their current process somewhat to very risky to their security posture (**Figure 7**).

The consequences of these challenges are significant. One in 3 organizations report that they experience more than 10 application service disruptions per year as a result of firewall

Figure 6

EXECUTION OF FIREWALL MANAGEMENT ACROSS CLOUD ASSETS

How consistent is your execution of firewall management across on-premises and cloud network assets?

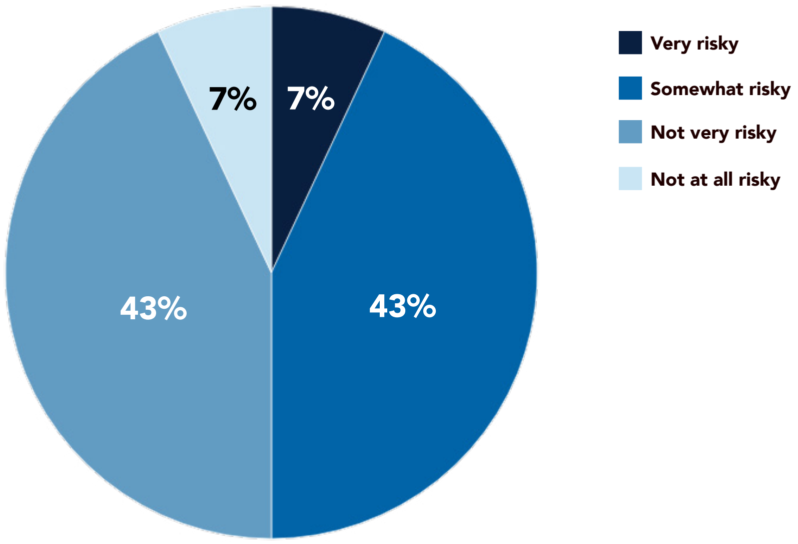


Data: Dark Reading survey of 105 IT management pros at companies with 20 or more firewalls, September 2024

Figure 7

SECURITY RISK OF FIREWALL MANAGEMENT PROCESSES

How risky do you consider your current firewall management processes to the security posture of your business?



Data: Dark Reading survey of 105 IT management pros at companies with 20 or more firewalls, September 2024

configuration changes. When outages do occur, it can take many organizations a significant amount of time to detect and respond to firewall-related outages. Thirteen percent of all respondents and 21% of those at large organizations reported it takes four or more hours to detect outages (**Figure 8**). Roughly, the same percentage say it also takes four or more hours to respond to these outages (**Figure 9**).

Additionally, 29% of organizations report that firewall change management and policy management work causes IT or security teams to miss SLAs for servicing business partners (**Figure 10**). This difficulty in keeping up with business requirements is even more severe at large organizations, 43% of whom report SLA problems as a result of firewall management. This is likely why 23% of organizations report that the relationship between firewall management staffers and software engineering is somewhat contentious.

69% of respondents are either currently implementing or planning to implement zero trust initiatives in the next 12 months.

The state of audit processes also exposes the impact of manual approaches. While almost all organizations today check up on the state of their firewalls with at least annual audits, only 12% of organizations are able to do audits on more than a monthly basis. The majority — 69% — do audits monthly or quarterly. While 90% depend on at least a decent level of reliability in their audit process, only 28% can honestly rate their firewall audit results as very reliable and the current audit processes are usually a significant time sink — likely stemming back to the prevalence of manual processes. Just 19% of organizations say it takes less than a day, and more than 1 in 10 organizations report that it takes a week or longer. Not only does this use up valuable resources on rote processes and deliverables, but it also keeps staff from completing mission-critical projects. Resources are improperly allocated to rote tasks rather than high impact tasks like zero trust initiatives, security posture improvement projects, etc. Slow audit response times also reduce auditor trust and extend their deadlines, causing more dissention in the organization.

46% of those implementing or planning to implement zero trust report that firewall menagement is causing moderate to significant delays and distruption.

Even more detrimental to business and security objectives, firewall management is causing security difficulty in executing on some of its most strategic initiatives. The study showed that 69% of respondents are either currently implementing or planning zero trust initiatives today. Among those, 46% report that firewall management is causing moderate to significant delays and disruption to those zero trust efforts. By delaying zero trust efforts organizations are putting themselves at risk. The core concept of zero trust is ensuring that tools, teams, and technologies who must have access have access. Firewalls rules and security policies are the basic foundation of successful zero trust initiatives.

The findings reveal that manual firewall management processes are not just inconvenient — they're hindering security and business outcomes, especially in large, complex environments. The gap between the critical role of firewalls and the effectiveness of current management practices is evident, with organizations facing frequent service disruptions, slow outage responses, and SLA issues. These challenges also extend to strategic initiatives like zero trust, where manual processes cause delays and undermine broader security goals. To address these issues, shifting to robust automation is crucial for enhancing firewall management, reducing risks, improving audits, and supporting key business and security objectives.

Conclusion

The results from this year's firewall security survey present both encouraging and challenging news about the state of automation in security today. The industry stands at a critical juncture, with organizations making strides toward more reliable, responsive, and transparent control over network policies. The good news is that half of organizations have managed to implement some level of automation and orchestration into their processes.

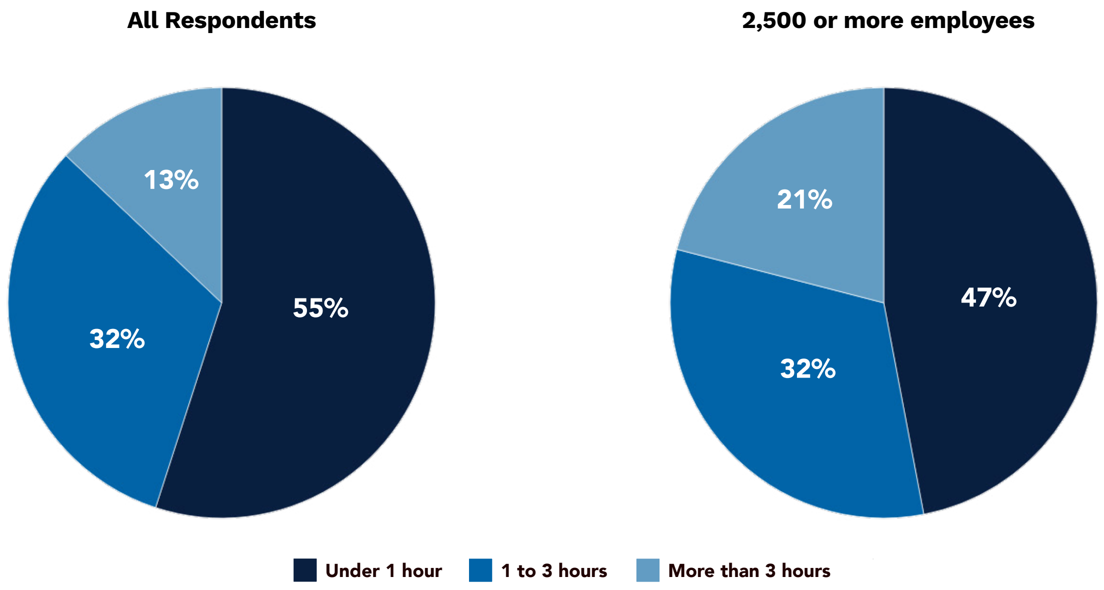
However, there's still significant progress to be made. For organizations still relying heavily on manual processes, it's crucial to begin automating tasks like firewall policy management and change request handling. Those already on the automation path must focus on improving consistency, reliability, and repeatability in their workflows.

Looking ahead, the integration of cloud environ-

Figure 8

TIME TO DETECT NETWORK OUTAGE

When there is a network outage, what is the timeframe for your team to detect it?

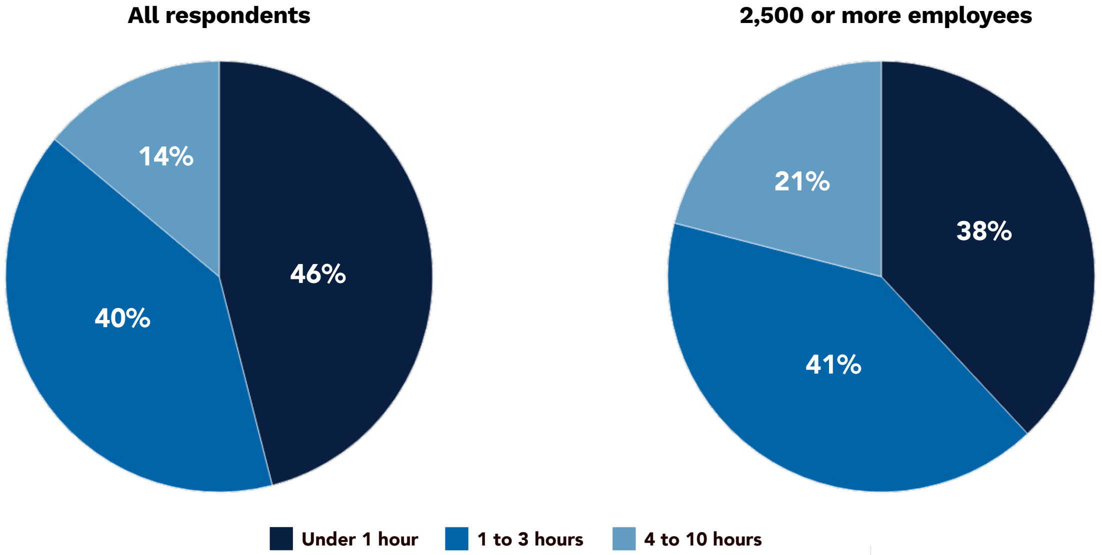


Base: 105 respondents with 100 or more employees and 53 respondents at companies with 2,500 or more employees
Data: Dark Reading survey of 105 IT management pros at companies with 20 or more firewalls, September 2024

Figure 9

TIME TO RESPOND TO OUTAGE

What is your team's average time to respond to a network outage?



All respondents

2,500 or more employees

Base: 105 respondents with 100 or more employees and 53 respondents at companies with 2,500 or more employees
Data: Dark Reading survey of 105 IT management pros at companies with 20 or more firewalls, September 2024

ments and the rise of AI-driven solutions will further shape this landscape. Cloud adoption is driving the need for scalable, hybrid solutions that seamlessly secure both on-prem and multi-cloud environments. AI, on the other hand, holds the potential to revolutionize firewall management, enhancing decision-making, predictive analytics, and policy optimization, while potentially automating mundane or rote tasks, and inviting IT professionals to complete network security tasks without the involvement of the cloud or network security teams. Organizations that embrace these technologies will be better positioned to stay ahead of evolving threats, reduce operational overhead, and ensure continuous compliance.

The following are a few recommendations on how to get started in these improvement initiatives:

Centralize Your Hybrid Network, Multi-Vendor Policy Management:
Organizations that manage firewalls in siloes will have a hard time establishing authoritative visibility and control over their network flows. And they'll have to put in a lot of work in the process. Centralizing policy management affords organizations greater control, reduces risk and improves efficiency.

Visualize and Map Your Network:
Getting a better handle on your network map or topology enables organizations to gain control and visibility across their entire network. Topologies can help security teams analyze attack paths, implement workflows to decommission rules and objects, and harden access to control their attack surface. Ideally, organizations should find ways to key automated reports to topology to help them identify unneeded, risky and misconfigured access control rules and detect points of failure.

Align Rules and Policies to Business Objectives:
Firewall management staff need to work with a wide range of IT and business stakeholders in departments like R&D, compliance, development, risk management, and legal to create a consensus on standardized firewall policy rules that line up with business objectives and expected SLAs.

Optimize and Secure Rule Management: Outdated, redundant or shadowed firewall rules keep doors open for attackers. Organizations that can automate and streamline the hunt for unused, shadowed or outdated rules can then start working on rule optimization to cut down on misconfigurations that expand attack surfaces and threaten business objectives.

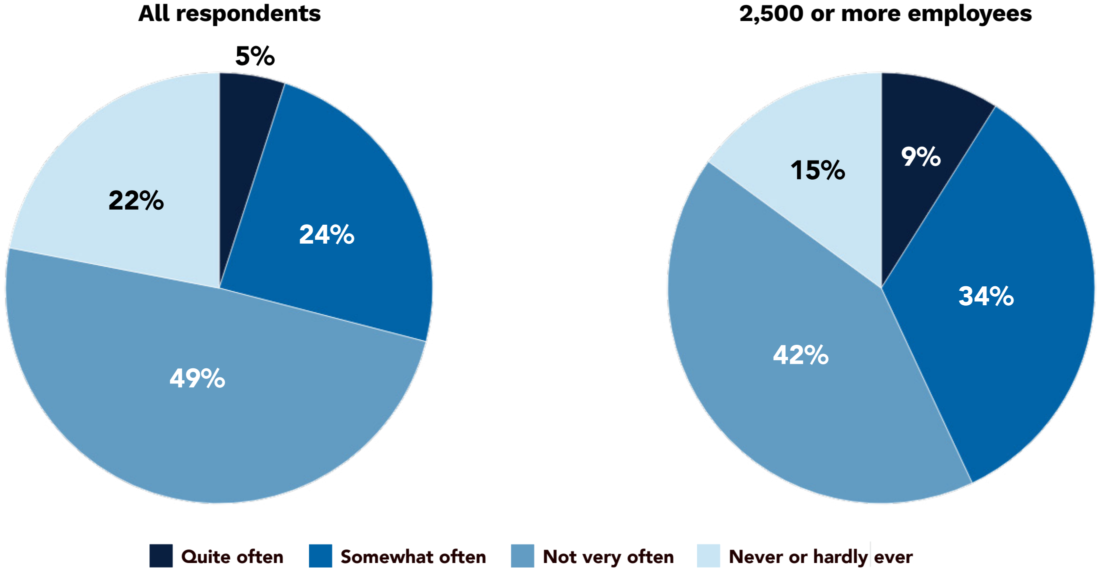
Drive Accurate Compliance and Security Policies Through Automation: There are too many firewalls, too many policies and too many change requests in modern IT environment to sanely do this manually anymore. Organizations can keep one step ahead of the regulators and improve the efficiency of their security teams by implementing automation to do the heavy lifting.

Limit Access to Reduce Attack Surface: The age-old rule of least privilege still reigns as one of the most effective security strategies an organization can lean on — this is why so many security programs are investing heavily in zero trust initiatives. Organizations should strive to tighten their firewall rules and align them to actual rule usage so that firewall rules aren't overly permissive or overly complex.

Figure 10

FIREWALL CHANGE MANAGEMENT AND MISSED SLAS

How often does firewall change management and policy management work cause your team to miss SLAs for servicing business partners?



Base: 105 respondents with 100 or more employees and 53 respondents at companies with 2,500 or more employees
Data: Dark Reading survey of 105 IT management pros at companies with 20 or more firewalls, September 2024

Survey Methodology

Tufin commissioned Dark Reading to conduct a survey to explore firewall management. The survey queried respondents about their processes for managing firewalls, change requests, the teams involved in managing firewalls, the use of automation, collaboration between network and cloud teams, and the implementation of zero trust.

The survey collected responses from 105 IT and cybersecurity high-level titles who are involved in the management of firewalls at companies with more than 20 firewalls. Thirty-percent are IT/cybersecurity executives such as CIO/CTO, CSO/CISO, VP of IT, or VP or cybersecurity. Twenty-three percent are the head, vice president, senior director, or director of divisions such as IT operations, cybersecurity, and networking. Thirty-four percent of respondents are senior management in these departments.

Respondents represent companies predominantly within North America. Thirty percent of respondents work at companies with 100 to 999 employees; 17% with 1,000 to 2,499 employees; and 53% work at companies with 2,500 or more employees. Some of the data citations within this report focus on respondents at the largest sector of 2,500 or more employees.

More than 21 vertical industries are represented in the final respondent base including technology manufacturer, consulting, communications carriers, banking/financial services, education, government, healthcare, other manufacturing, and solutions providers to name those cited by 6% or more of respondents.

The survey was conducted online in September 2024. The data cited in this report is based on 105 respondents unless otherwise noted. The sample base (N=105) yields a margin of error at a 95% confidence rate of +/- 9.5 percentage points. Respondents were recruited via email invitations containing an embedded link to the survey, with an incentive offering where respondents could enter a random drawing for five $50 Amazon gift cards. The emails were sent to a select group of Dark Reading's database that fit the desired respondent profile. Dark Reading was responsible for all survey design, administration, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing U.S. privacy laws.