SANS | Research Program

Survey

The Future of Network Security Technology: A SANS Survey

Written by **Matt Bromiley**

February 2024

paloalto NETWORKS

Introduction

A myriad of factors can influence the dynamics of an organization's security team and their respective spending patterns. What drives organizations to spend and allocate resources the way they do? Is it the looming shadow of various security risk factors, stringent requirements of compliance, or the ever-evolving landscape of threats? How does one even go about sorting their risks and priorities?

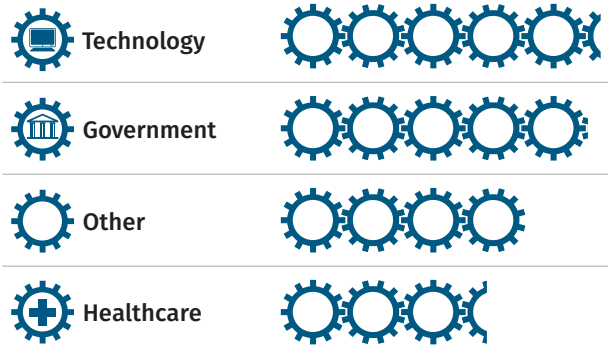
Another consideration when it comes to tooling and resource utilization is that although security teams often have significant purview, they are not the only teams requiring insight into an organization. Network engineers and IT operations are critical to uptime and business processes and often drive their own spend—if not spend that is integrated with security needs.

In this survey, we set out to understand how the various driving forces in the industry, ranging from organizational needs to insider threats to third-party access, can impact the confidence and acquisition of various security tools or approaches. Our topics ranged from network engineering to security detection and response to other complexities, such as hybrid environments and the use of AI. Figure 1 presents the demographic information from the survey.

Our key takeaways from the survey include:

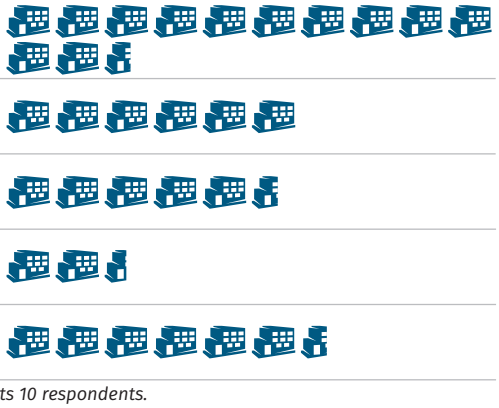
- **There's a healthy blend of enterprise IT tools. Approximately 76% of respondents see a convergence of tools across security, networking, and IT ops. We expected and celebrated this stat, showing that integrated tooling is the path forward.**
- **Environments are diverse; no tool can do everything. Nearly half of respondents (49%) indicated they use a hybrid security stack, relying on in-house and outsourced security tooling assistance.**
- **Zero trust methodology is growing. Our survey indicated that zero trust implementations are growing, with 67% working toward some level of zero trust integration.**
- **You don't know what you don't know. Approximately 95% of respondents indicated some level of concern about non-approved or unknown devices connecting to their networks.**

Top 4 Industries Represented



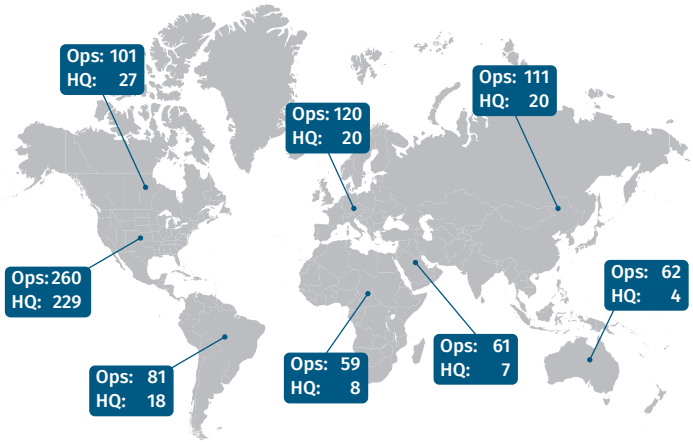
Each gear represents 10 respondents.

Organizational Size

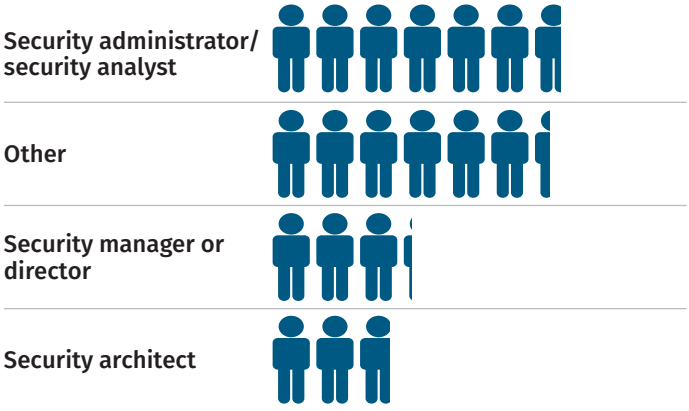


Each building represents 10 respondents.

Operations and Headquarters



Top 4 Roles Represented



Each person represents 10 respondents.

Figure 1. Demographics of Survey Respondents

This survey covers a vast landscape of questions and insight into organizations. Across the multiple topics covered, we encourage you to look for areas your own organization may be considering or implementing. Surveys often provide a useful barometer to determine where other organizations stand—an important metric that can be used to help guide your own budgeting and resource allocation.

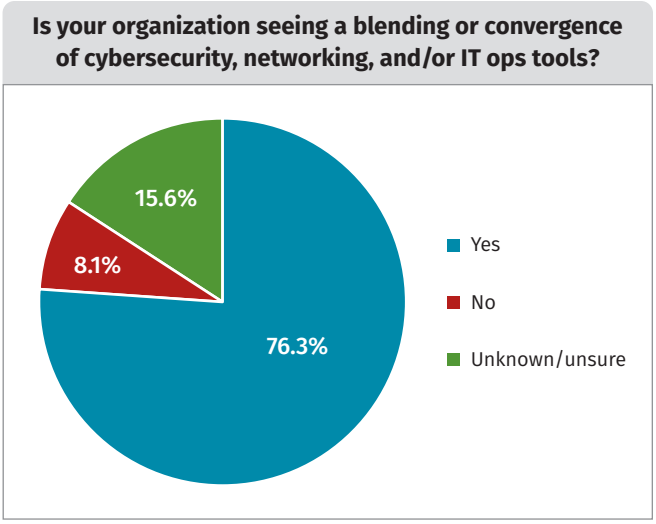


Figure 2. Blend/Convergence of Cybersecurity, Networking, and/or IT Ops Tools

Not Just Security

Our assessment began by understanding the convergence of tools across cybersecurity, networking, and IT ops. Tool convergence is not just a benefit—it's critical. Integrated toolsets foster a more cohesive and efficient approach to managing and securing IT infrastructures. Our survey began with this core topic, asking our respondents whether they see a convergence. See Figure 2.

A healthy majority, approximately 76%, of our respondents reported seeing a convergence in tools across these three disciplines. This did not come as a surprise. We have seen for years that organizations are blending tools and finding value. Only 8% reported they did not see a blend. We dug deeper, looking to understand *how* the blend is comprised. Figure 3 provides those answers.

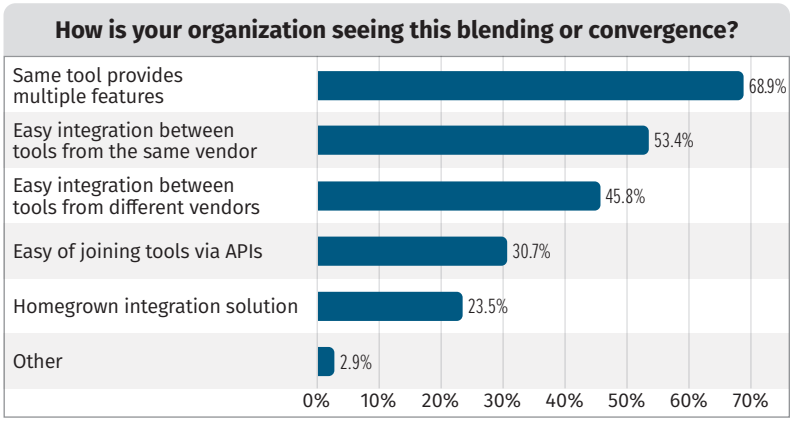


Figure 3. How Organizations View Blending or Convergence of Tools

Our largest response category, approximately 69% of respondents, indicated they utilize the same tool for multiple features across the disciplines mentioned in previous paragraphs. This speaks volumes to what organizations likely seek in today's market: simplicity and tool integration versus multiple specialized tools. Our second-highest answer, at approximately 53%, highlights the ease of integration between tools from the same vendor. Again, we see an element of tool streamlining and a movement away from tool-segmented environments.

The top four are rounded out by the ease of integration across tools from *different* vendors and joining tools via API, approximately 46% and 31%, respectively. While lower in representation, these answers reflect the necessity for interoperability and customization across *different* tool vendors. In situations where other vendors are present, the ability to make tools work *together* is a necessity.

We shifted gears slightly, asking respondents if they were consolidating their tools. If so, how far along are they in the process? See Figure 4 for the answer.

Approximately 44% of respondents indicated they were in the process of consolidating, while approximately 21% indicated they were planning to. Combined, 65% of customers are somewhere in the consolidation process, confirming that consolidation is the current state or way forward for many organizations.

We next looked at the progress these respondents were making to consolidate. Figure 5 shows that many are still in the middle of the process, with a third coming in at 41 to 60% completed.

In the aggregate, nearly 81% are between 21% and 80% completed, indicating that our focus on tool consolidation is familiar for many organizations and already an initiative in progress. For those organizations that are less than 20% completed (13% of our respondents), we offer some encouragement: Getting started is the hardest part. Keep working on those initiatives!

Approximately 17% of organizations, however, responded that they had no plans to consolidate (Figure 4). This response should not be interpreted in a negative way because it may indicate environmental constraints. For example, no consolidation plans might indicate specialized tooling for specific functions, a strategy toward highly specialized tools, or legacy systems. Of course, we also cannot overlook the possibility that, for some teams right now, consolidation is not a priority.

With every survey, we have an appreciable response size of "Unknown" or "Unsure." Although we often don't capture *why* a respondent replies to any given question this way (could be lack of visibility, transparency, etc.), we encourage organizations to seek to minimize unawareness of tooling and capabilities. It is better to recognize and seek to fix a gap than to be unsure whether it exists.

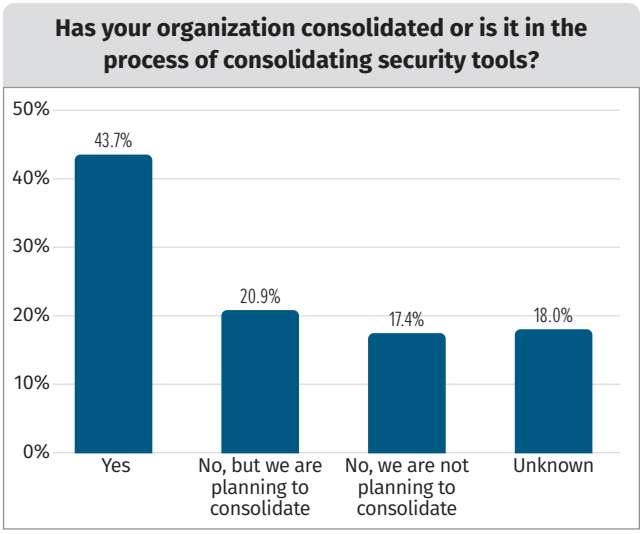


Figure 4. Consolidation of Security Tools

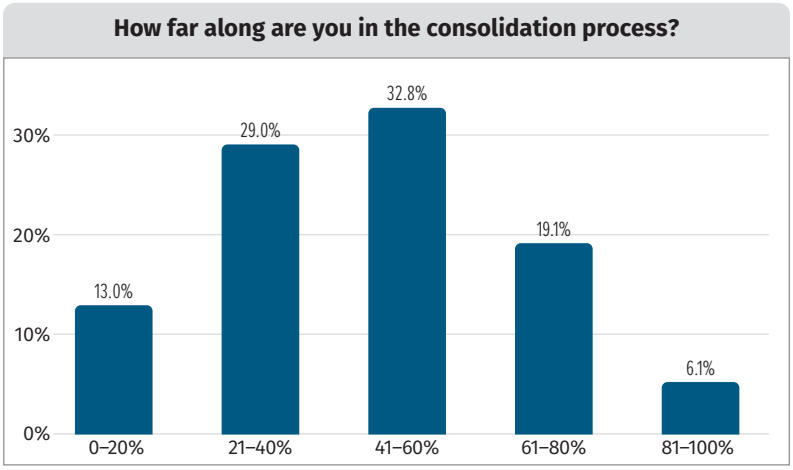


Figure 5. State of Consolidation Process

Security Detection and Response

The previous section looked at tool convergence and how organizations see, or expect to see, various teams utilizing the same technologies to achieve their objectives. However, an organization's need for continuous monitoring and incident response capabilities is another critical driver of network security technology. The survey continued to explore the topic of tool convergence, slightly more specialized in the security realm.

Cybersecurity Tooling

Cybersecurity technology integration, from continuous monitoring to incident response, bolsters a comprehensive approach to overall organization security and a robust security posture. Figure 6 is a snapshot in time of *how* organizations handle cybersecurity technology, monitoring, and incident response.

Our results were varied and painted a realistic image of how organizations build their security capabilities today. Approximately 43% of respondents rely on in-house teams, while 49% indicated they have a hybrid approach. Only 7% relied entirely on a vendor. Although not evenly split, these results align with our expectations.

A wide variety of security configurations exist throughout the industry and there are plenty of reasons to utilize either setup. We'd expect to see hybrid approaches grow in the future. A hybrid approach allows organizations to lean on the specialized expertise of external vendors while retaining critical control and customization of their posture with their in-house team. Internal cybersecurity handling also can help with data privacy concerns, limiting sensitive data access with internal personnel.

Visibility into threats is another driving force because security postures are often built around the confidence that an organization can observe threats and events within its environment. In our survey, we looked to capture that level of confidence. Figure 7 provides insight into our respondents' confidence.

How does your organization handle cybersecurity technology, monitoring, and incident response?

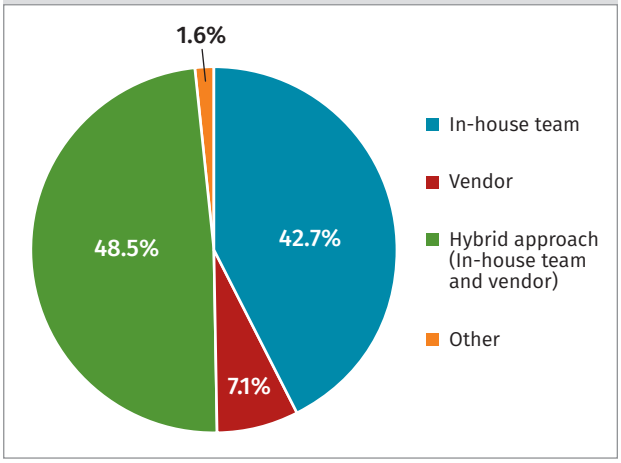


Figure 6. Handling of Cybersecurity Technology, Monitoring, and Incident Response

Do you feel confident that you have visibility into your network and the threats against it?

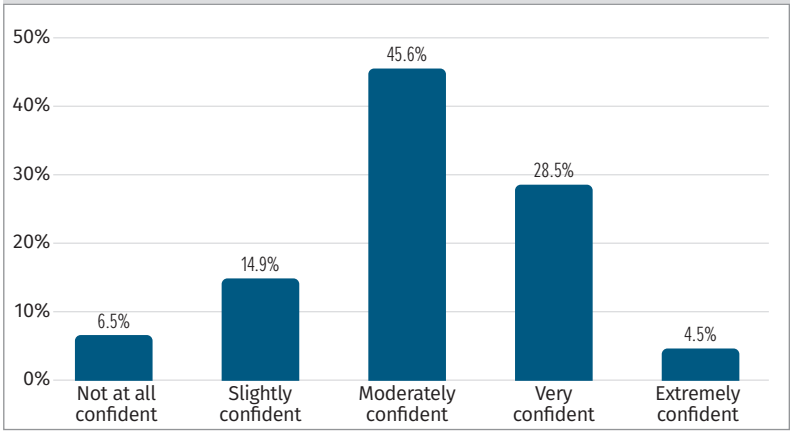


Figure 7. Confidence in Visibility and Knowledge of Threats Against Network

Approximately 46% of respondents indicated they are moderately confident, with 33% indicating they are *very* or *extremely confident*. We celebrate these results, which indicate that cybersecurity investments are paying off and instilling confidence. We would expect this response to shift to "more confident" year after year because organizations *should* be realizing the value in their security investments.

On the other hand, approximately 21% of respondents indicated they are slightly confident, at best. This statistic indicates room for growth and potential acquisition of new tooling or better integration. Confidence in visibility also may be attributed to a skilled workforce capable of wielding the tools. Although we did not differentiate between the two, tool and technology investments can only find success with people behind them.

Strong confidence can be an important asset for an organization, but it does not completely eradicate concerns. Playing on the idea of visibility and confidence, we also asked respondents about their concerns with who and what devices are accessing their network, and what applications they have access to. Figure 8 shows those responses.

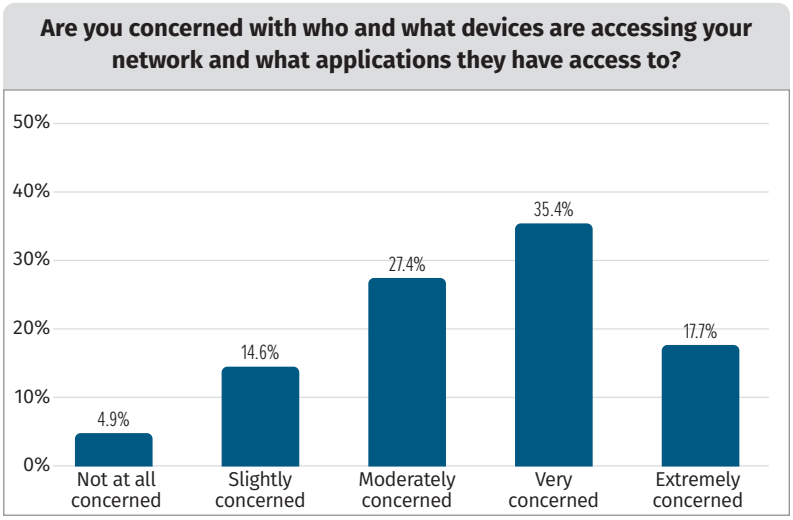


Figure 8. Concern About Who and What Devices Are Accessing the Network and What Applications They Can Access

As mentioned earlier, there is some level of concern expressed by at least 95% of our respondents—and rightfully so. Unauthorized access is an important concern, one that can lead to data breaches or theft of sensitive data. It also can be an easy gateway for threat actors to enter and gain a foothold into an organization. Far too often, however, security professionals focus on external threats. Internally, security teams should be concerned about what *internal* users are doing and what they have access to.

To expand on this further, we asked our respondents with some level of concern specifically what they were most concerned about. Figure 9 provides those answers.

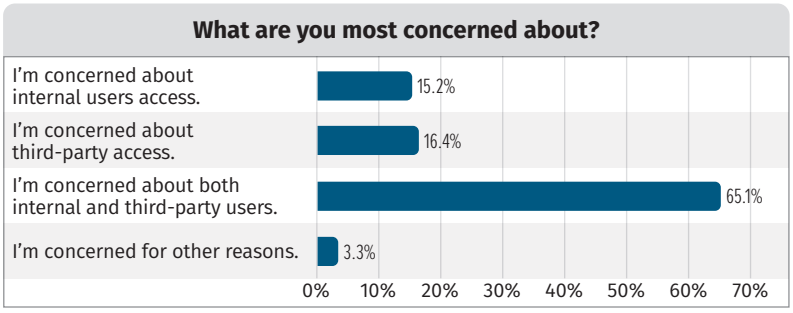


Figure 9. Areas of Most Concern

A little more than 65% of these respondents indicated that they are concerned about *both* internal and third-party users, not just specifically one or the other. These respondents understand that cybersecurity threats can originate from both inside and outside an organization. Internal users can pose a risk due to misuse of privileges or over-privileged accounts. On the other hand, third-party vendors have posed a significant risk to multiple industries lately, sometimes serving as an easier path for adversaries. Unfortunately, we hear far too often of data breaches that originated with a third-party vendor that had privileged access to a sensitive network that was the ultimate target.

Many solutions exist to help organizations mitigate the risks of unauthorized or misused access. Robust access controls and trust policies can help an organization:

- Maintain trust policies
- Minimize insider threat and adversary reach
- Streamline user access to resources
- Adapt to changes in the threat landscape

Access controls and trust policies likely never reach a "final" stage—they are always evolving and adapting. However, they can help bolster confidence when deployed and utilized correctly. Figure 10 looks at how our respondents felt about their current access controls and trust policies.

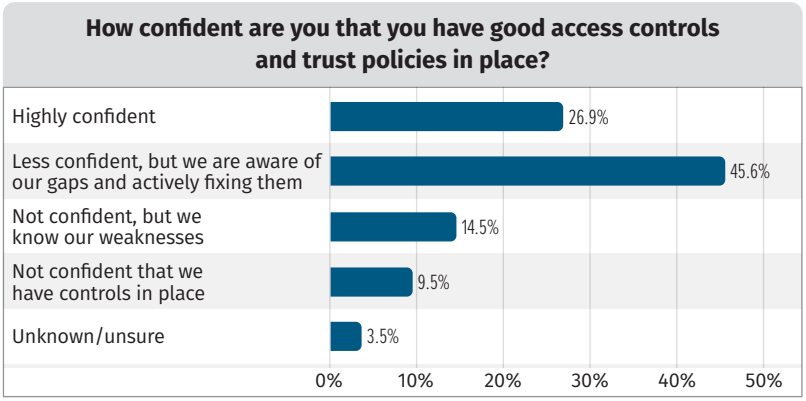


Figure 10. Confidence in Access Controls and Trust Policies in Place

Only 27% indicated that they are highly confident in their policies. In general, we find these results to reflect a common theme across various business, industry, and government sectors: knowledge of a gap but actively working to fix it. Approximately 46% indicated they could be more confident but are aware of their gaps and that fixes are underway. Perhaps more concerning is the combined 28% of respondents who lack confidence either because they know their weaknesses, are unaware of controls in place, are just plain unsure, or don't know.

If we had to pick one area for organizations to heighten their awareness or look for additional resource investment, it would be tightening their access controls. For many organizations, access controls are a rampant problem from legacy IT policies, employee churn, legacy and current technology usage, and lack of visibility. Weak access controls are where *many* adversaries find success.

To help mitigate access control concerns, one increasingly common methodology among public and private organizations is "zero trust." While treated as a buzzword by some, zero trust can be a constructive methodology to guide organizations toward safer access controls and policies and provide them the resources they need to understand how to best structure account capabilities within their network.

We included zero trust adoption in our survey, as seen in Figure 11.

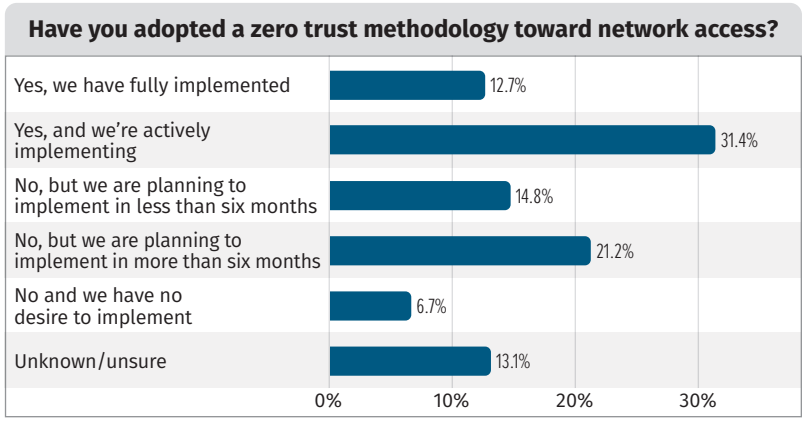


Figure 11. Adoption of Zero Trust Methodology

Our results were varied, from 13% indicating that they are fully implemented to 20% saying "No" with no desire to implement or "Unknown/unsure." The more interesting takeaway, however, is that approximately 67% of respondents indicated they are either actively implementing or will be in the future. This represents a trend in the right direction.

About Zero Trust

Zero trust is not a vendor-specific term, meaning it is not a move toward a product implementation. As a methodology, zero trust is an approach that helps enhance network security and lock down access controls. Zero trust helps to mitigate many of the concerns respondents called out in previous questions: confidence in visibility and access controls or other concerns about external threats. Taking a proactive stance is valuable, as is recognizing that perimeter-based security is insufficient.

Enterprise Complexities

Our survey continued beyond security methodologies and threats to find out how the modern, hybrid landscape affects organizations. It should come as no surprise to anyone that the past five years have seen a dramatic shift in the use of cloud environments and a significant increase in third-party integrations. Many organizations are still balancing hybrid implementations, while some are shifting in either direction based on their needs.

We asked our respondents whether their network has become increasingly complex. Figure 12 shows those results.

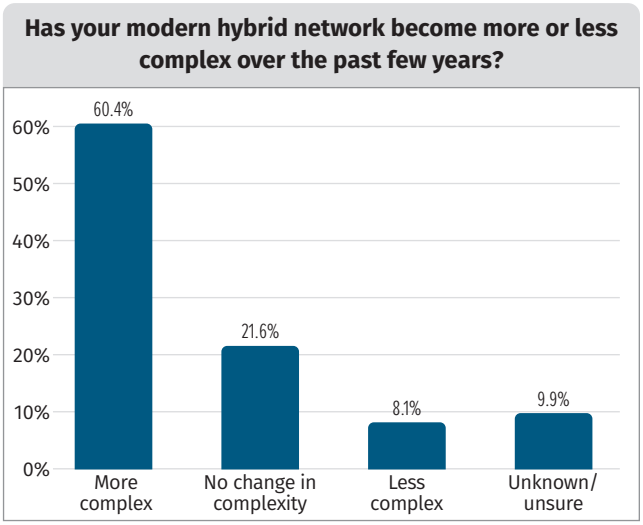


Figure 12. Complexity of Modern Hybrid Network Over the Past Few Years

As expected, approximately 60% indicated that their network has become more complex. This echoes the trend(s) observed in the industry for years, especially over the past half-decade. Growth in the use of public and private clouds, IoT devices, and demands for remote access create issues and concerns that must be addressed.

For those that said their network has become more complex, Figure 13 looks at the key contributors to that increase in complexity.

Most respondents (81%) indicated that more cloud and on-premises blending was a source of complexity. Again, following observed trends, additional leading complexity drivers were the increase in third-party applications (approximately 61%) and BYOD/user-driven devices (44%). This should come as no surprise—these two categories can introduce an array of unstandardized and unsecured devices and software into an organization's network. These factors can increase the complexity of environment makeup and management as well as the enforcement of security policies.

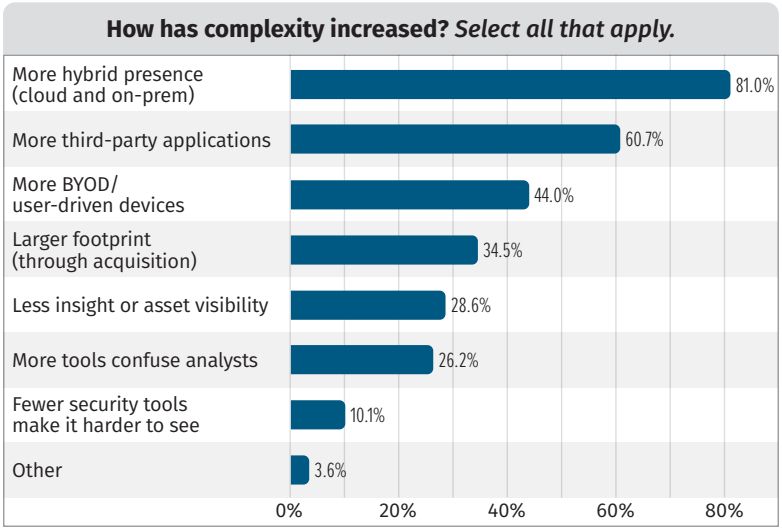


Figure 13. Reasons for Increase in Complexity

We also wanted to understand why, for some respondents, complexity had *decreased*. The results, shown in Figure 14, were insightful.

Approximately 87% of these respondents indicated that better security insight or tooling was the reason for less complexity. This trend—increased confidence and less complexity, all driven by better security insight or tooling—surfaces within this survey multiple times. The second and third responses, a smaller footprint and less on-premises presence, respectively, received equal attention at 39% each.

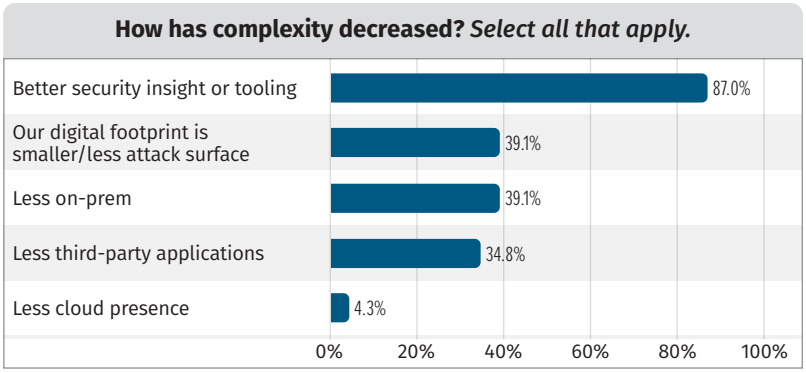


Figure 14. Reasons for Decrease in Complexity

Here, the top three results are an excellent indicator of where organizations are seeing efficiencies in enterprise security and a payoff in long-term investments. From a tooling perspective, increased insight is invaluable. Tools, however, are not "set it and forget it." They take time to implement and hone. Furthermore, shrinking one's digital footprint (either by smaller attack surface or less on-prem presence) is not an overnight activity. It costs valuable resources but pays off in dividends for years to come (for the right organizations).

Another implementation or capability that can greatly benefit organizations is the use of security automation tools. In addition to providing more visibility and insight, automation can help amplify security team capabilities by reducing the time spent on mundane tasks. Figure 15 looks at security automation in our respondents' environments.

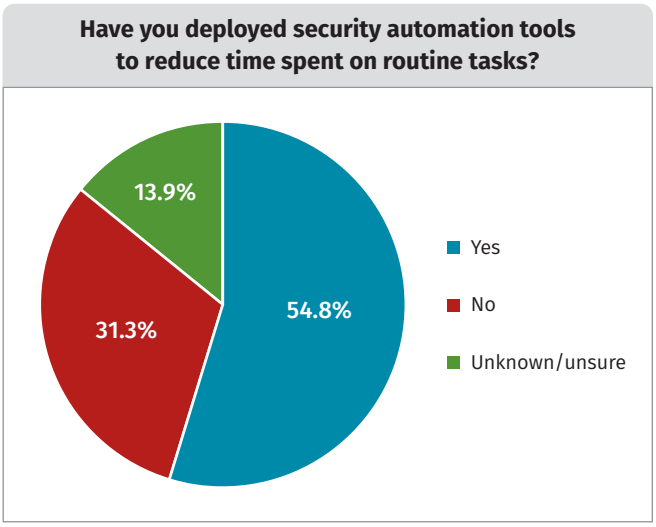


Figure 15. Deployment of Security Automation Tools as a Means of Reducing Time Spent on Routine Tasks

As expected, more than half (55%) of our respondents utilize security automation tooling. Conversely, approximately 31% are not utilizing security automation tools. Why, when so many others have found productive efficiencies? As we mentioned, automation can be a force multiplier for teams by removing the need to focus on tasks that could be easily automated. The use of automated tools frees analysts to focus on the problems for which humans are best suited. It also helps streamline operations between security and other enterprise teams.

In today's security landscape, there might be a need to move beyond "simple" automation. This move would mean that security teams might need more than just the ability to automate tasks—they'd need assistance in making decisions. Of course, we're moving toward AI capabilities integrated into almost *everything* we do, so why would enterprise tools be any different? Our next two questions look at AI-powered operational tools. See Figure 16.

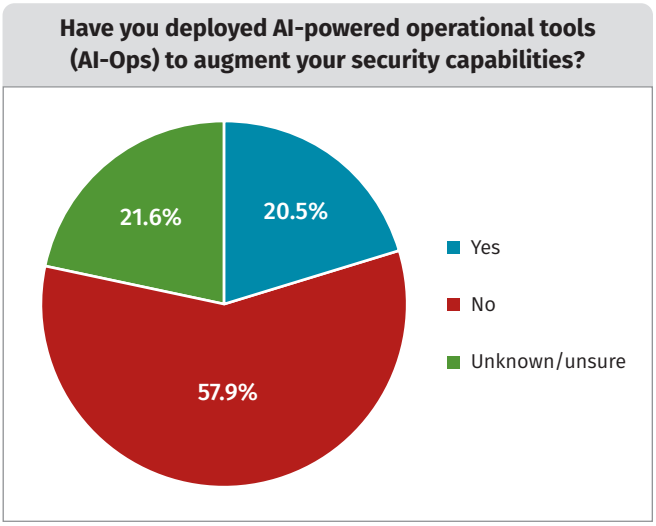


Figure 16. Deployment of AI-powered Operational Tools (AI-Ops) to Augment Security Capabilities

Nearly 58% of our respondents are *not* utilizing AI-Ops tools in their current security capabilities while 21% are. Given the year this survey was conducted, these results align with what we expected to see. Many are still testing AI-powered capabilities, unsure when to hand the reins over to artificial intelligence. However, despite initial hesitations, we expect the usage of AI-Ops tools to grow in the future.

Where do we expect organizations to benefit? Our respondents, as shown in Figure 17, identified several key areas.

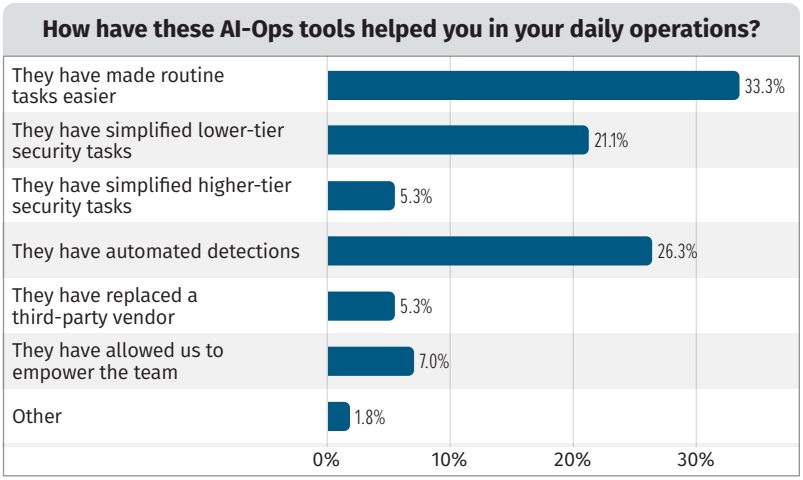


Figure 17. Benefits of AI-Ops Tools in Daily Operations

Results were split across multiple categories with no clear majority but instead several different capabilities. A third of respondents found that AI-Ops helped make routine tasks easier, while automated detections took an important second place at just above 26%. We agree with AI-Ops simplifying lower-tier security tasks. We most appreciated the fourth-place answer, however: that AI-Ops empowers the team.

AI-Ops not only can empower a security team by reducing the time spent on mundane tasks but also help the team focus on strategic decision making and response planning activities. AI's ability to learn and adapt can help move the team toward a proactive stance. Rather than waiting for threats to pop up, the team can focus on hardening the environment and bolstering the security posture.

Closing Thoughts

For several reasons, understanding the driving factors behind spending on network security technology is crucial. First, it enables organizations to understand where they find efficiencies and how best to allocate future investments. This understanding is necessary in the ever-changing landscape. Our survey showed that organizations want confidence in their visibility and are moving toward more secure states. Knowing where they came *from* helps determine where they are *going*.

Knowing what drives spending also helps organizations prioritize risk and anticipate future security requirements so they can stay ahead of internal and external threats. Anticipation can also help handle future regulatory and compliance requirements, which are also ever-evolving. Our respondents indicated they use many automated and manual tools to help them secure their environments. Knowing what comes next helps them assess whether their current implementation is the best option.

Lastly, the threat landscape will always be an essential driver. Threat actor objectives alone, such as ransomware, data destruction, or corporate espionage, can significantly impact an organization. But organizations want to have clarity about how they are detecting, be confident in their visibility, and secure their digital footprint. Now, more than ever, optimal enterprise security depends on many pieces working together—not siloed—toward a common goal.

Sponsor

SANS would like to thank this paper's sponsor: