IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Prepared for:

BROADCOM

NetSecOps:

Examining How Network and Security Teams Collaborate for a Better Digital Future

January 2024 EMA Research Report Summary

By **Shamus McGillicuddy**, Vice President of Research
Network Infrastructure and Operations

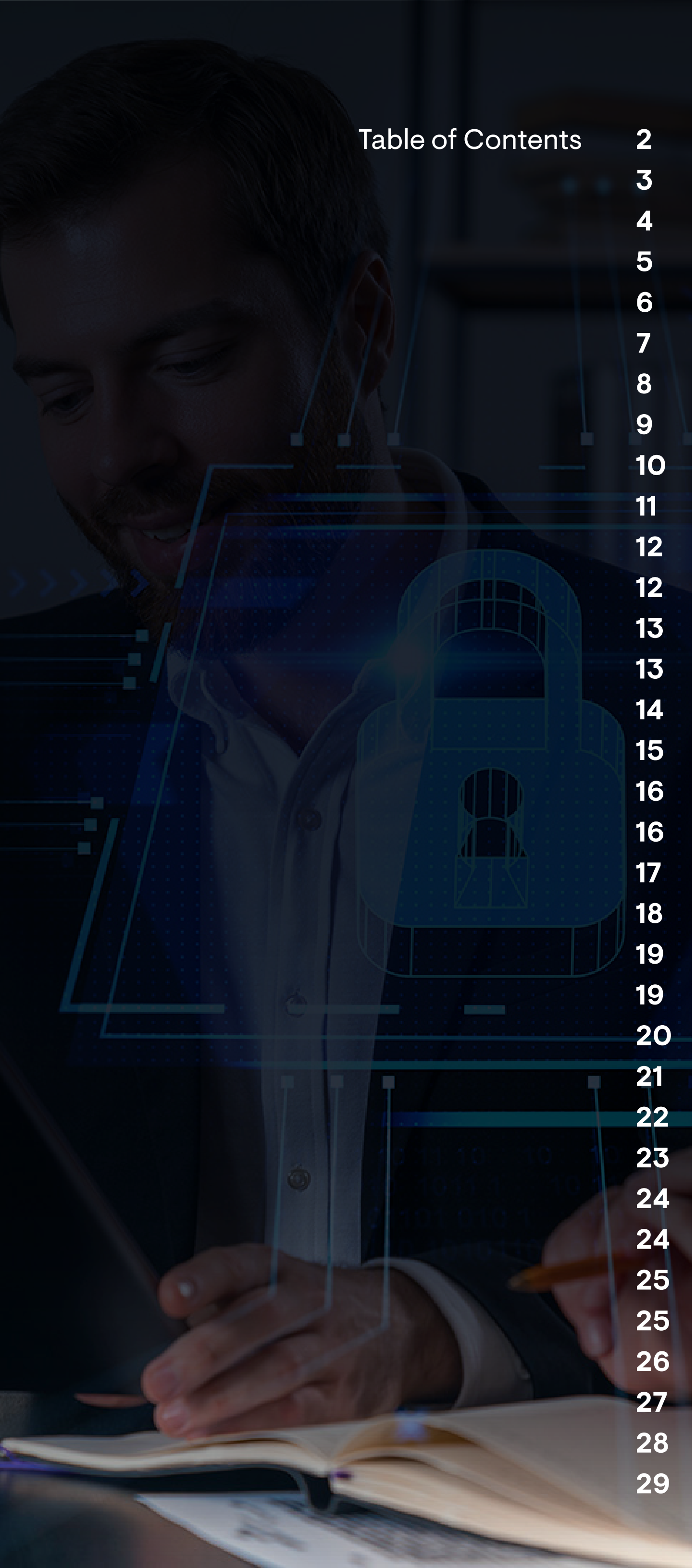


Table of Contents

Executive Summary

This summary of independent market research explores the nature of collaboration between network operations teams and cybersecurity teams. It identifies why network and security teams need to work together and explores the challenges enterprises encounter when they try to build partnerships between these groups. The report also identifies best practices for ensuring that this collaboration is successful.

From Conflict to Partnership: The Rise of NetSecOps

Two of the most important aspects of information technology (IT) are networking and security. Networks connect users, applications, and data to enable the consumption of digital services. Security protects users, applications, and data from malicious activity, such as unauthorized access, data leakage, and ransomware. Historically, the people responsible for these two IT domains were at odds. The core mission of network teams was to give people reliable access to IT assets, while the security team aimed to limit that access as much as possible. This dynamic led to cultural disconnects, turf battles, and misaligned processes.

This conflict of ideals and priorities is largely an artifact of history, from a time when IT infrastructure was static and predictable. All assets resided behind a security perimeter, data and applications lived in private data centers, users worked in corporate sites, and sites were connected by private or managed WAN services that were fundamentally secure and reliable. In other words, it was a simpler time when complexity was relatively low, the pace of change was positively glacial, and network and security teams had total control. The two factions could afford to be in conflict because those conflicts were less disruptive and the consequences were finite.

Hybrid Clouds, Hybrid Networks, and Hybrid Workers Have Raised the Stakes

Today, that control is gone. Data and applications have steadily migrated to the public cloud, often without the involvement of network and security teams. Users work from anywhere. The public internet is the new WAN. The traditional security perimeter vanished. Many network and security teams are struggling to regain control as the complexity of digital infrastructure skyrockets. Within this new normal, network teams and security teams must work together – and that is exactly what they are doing.

Over the last five years, Enterprise Management Associates (EMA) observed increased cooperation and collaboration between network and security groups. In some cases, these former rivals converged into one group. In other cases, they formalized partnerships to work together toward a common goal of building and operating secure hybrid infrastructure. EMA refers to this movement as NetSecOps. In October 2021, EMA published a research report dedicated to exploring these new partnerships called “NetSecOps; Aligning Networking and Security Teams to Ensure Digital Transformation.” Today, EMA is updating and expanding on that research with a new 2023 report that provides a deep dive into the drivers, benefits, and challenges of NetSecOps partnerships.

Demographics

For this new research, EMA surveyed 304 IT personnel in October 2023. Qualified respondents worked for organizations in which digital infrastructure was complex enough to require specialized networking personnel and teams and security personnel and teams, rather than one group of IT generalists that one might find in a smaller company. **Figure 1** reveals the overall demographics of EMA's survey. Most respondents were technical personnel, such as engineers, analysts, and architects. They primarily worked in network engineering, cybersecurity, or an IT executive's suite. Respondents hailed from medium to very large enterprises across North America (the United States and Canada) and Europe (France, Germany, and the United Kingdom). Seventeen industries were represented, the most numerous of which are listed in the chart.

FIGURE 1. DEMOGRAPHICS

Job Titles

61.5%	Technical personnel
21.1%	IT middle management
17.4%	IT executives

IT Groups

36.2%	IT executive suite
28.3%	Network engineering
14.5%	Cybersecurity/IT security
7.2%	Network operations/NOC
6.6%	IT architecture
8.3%	Cloud architecture/engineering
3.0%	Security operations/SOC

Top Industries

23.0%	Online services/software as a service
18.4%	Finance/Insurance/Banking
16.8%	Retail/Wholesales/Distribution
13.8%	Manufacturing
7.9%	Health care/Hospitals
3.6%	Professional services not related to IT
3.3%	Construction
2.4%	Transportation

Company Size (Employees)

45.7%	Medium enterprise (1,000 to 4,999)
37.5%	Enterprise (5,000 to 19,999)
16.8%	Large enterprise (20,000+)

Annual Revenue

3.9%	$100 million to <$250 million
8.6%	$250 million to <$500 million
24.0%	$500 million to <$1 billion
46.1%	$1 billion to <$5 billion
16.4%	$5 billion or more
2.0%	Unknown/Not applicable

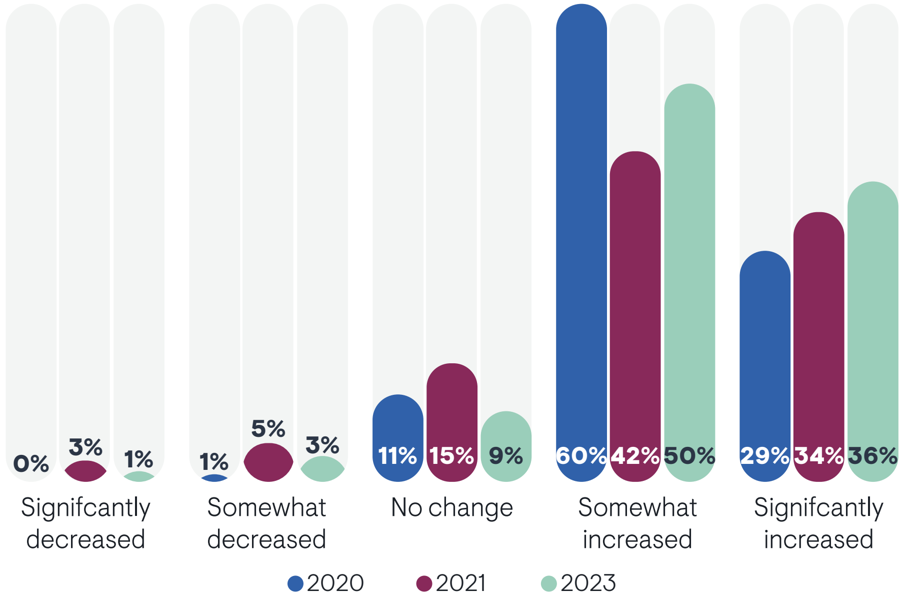
Region

67.1%	North America
32.9%	Europe

Network and Security Team Collaboration Continues to Accelerate

In 2020, EMA began surveying IT organizations about changes in the amount of collaboration that occurs between their network and security teams. **Figure 2** reveals that from 2020 to today, the overall number of organizations that perceive increased collaboration growth fluctuated between 76% and 89%, but the number of organizations that report intense growth in collaboration is steadily increasing, from 29% in 2020 to 36% today. While the overall amount of collaboration growth fluctuates, the number of IT organizations that are pushing hard for close collaboration is expanding.

FIGURE 2. NETWORK AND SECURITY COLLABORATION TRENDS FROM 2020 TO PRESENT



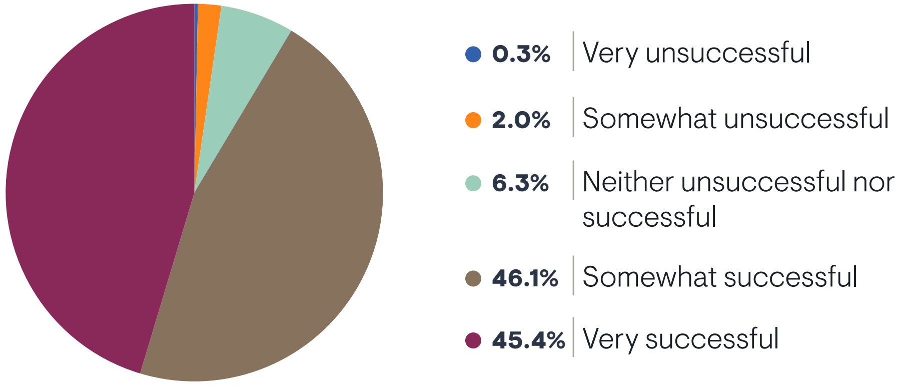
In all three years, IT executives perceived more significant growth in collaboration than IT middle managers and technical personnel, suggesting that executives believe more collaboration is occurring than is actually happening among rank-and-file personnel. IT leaders should assume this gap exists and that personnel may be struggling to comply with any executive directives that mandate close partnerships between the groups.

Sample Size = 304

Overall Success with Collaboration

Figure 3 reveals that 45% of respondents believe their organizations have been very successful with NetSecOps collaboration. In 2021, only 39% rated their success this high. More than 46% of this year's respondents perceived some success but believed there was some room for improvement. Larger companies experienced more success with collaboration. The network engineering team was more confident in success than members of IT architecture and network operations teams. Organizations that have siloed network and security teams and organizations that have fully converged these teams were having more collaboration success than organizations that only partially converged these teams.

FIGURE 3. OVERALL SUCCESS WITH COLLABORATION BETWEEN NETWORKING AND SECURITY PERSONNEL



Sample Size = 304

Collaboration Roadblocks

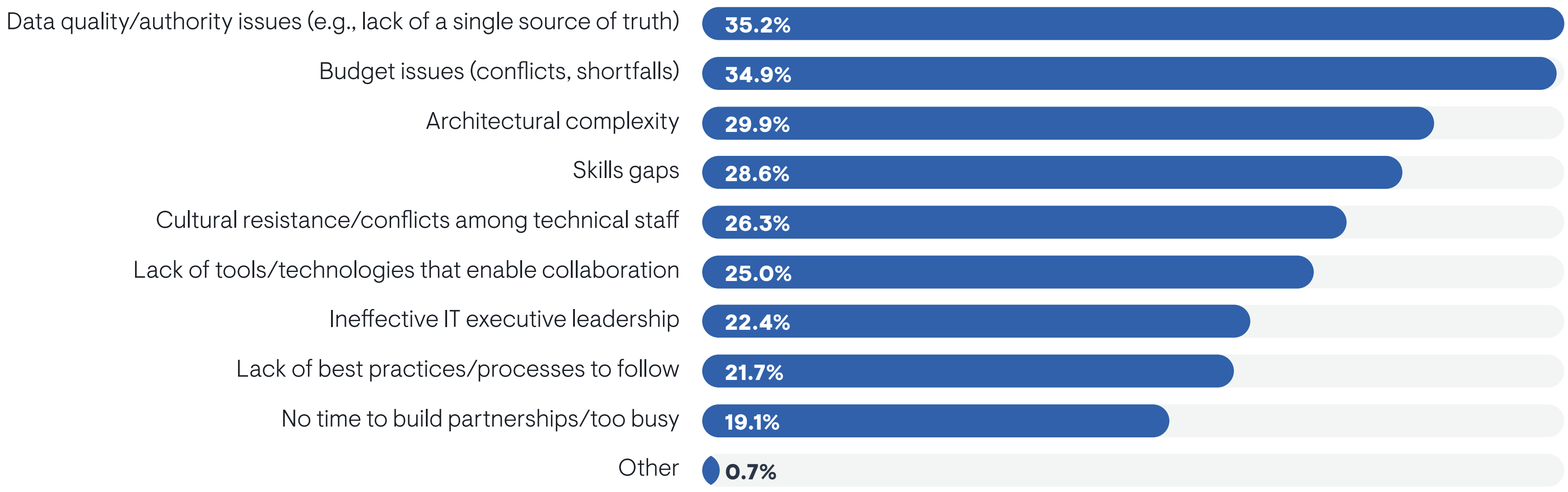
Figure 4 reveals the issues that can undermine the efforts of network and security teams to collaborate. Data quality and authority issues and budget issues are the leading problems. Organizations lack a single source of truth for network data to provide a definitive view of what's happening on the network. Also, organizations lack the necessary budget to acquire the tools, training, and personnel they need to execute on collaboration goals. Respondents who reported budget issues this year were more likely to be uncertain about their overall success with network and security collaboration.

Architectural complexity and skills gaps were the chief secondary challenges. Very large enterprises (20,000 or more employees) were more likely to struggle with skills gaps, as were organizations that had only partially converged their network and security teams. Cultural resistance was a tertiary issue, but it was felt most keenly by respondents who work in network engineering.

Cultural challenges and conflicts were major issues for a network engineering manager with a midmarket travel and hospitality enterprise. "Security wasn't ready to compromise. They weren't thinking about business requirements. They only thought about their own security team's requirements."

"If I were a CIO, I would try to address staffing levels," said a security architect with a Fortune 500 software and services enterprise. "You might keep costs down by keeping staff low, but it's a detriment to collaboration."

FIGURE 4. BIGGEST CHALLENGES TO COLLABORATION BETWEEN NETWORKING AND SECURITY PERSONNEL



Sample Size = 304

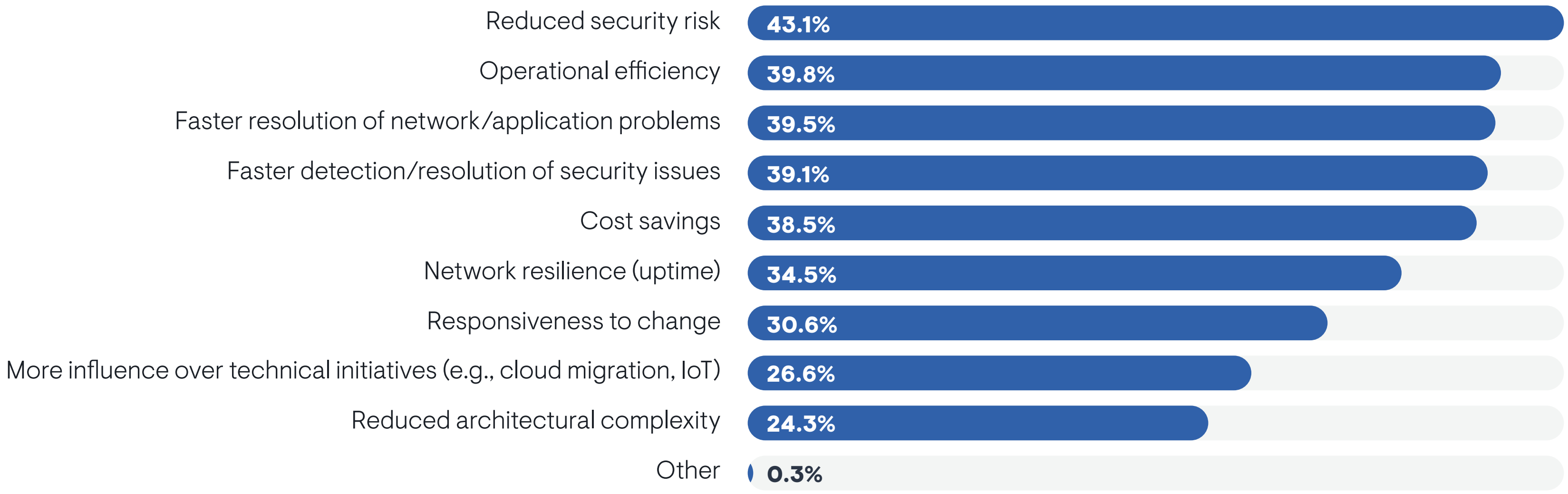
Benefits of Collaboration

Figure 5 identifies the benefits that organizations are earning from NetSecOps collaboration. The biggest opportunity is a reduction in security risk. Reduced risk was only a secondary benefit two years ago, suggesting that these partnerships have matured since 2021. The chart shows four secondary benefits, from operational efficiency and faster resolutions of network problems to faster detection and resolution of security incidents and reduced costs. The most successful collaborators were more likely to experience reduced security risk and faster resolution of network problems. Technical personnel were less likely than middle managers to perceive any reduced security risk. Larger enterprises also reported reduced security risk, while smaller companies perceived improved network resilience.

“The main benefit is that my team now has exposure to the [security teams’] environment. It helps us troubleshoot a lot of issues, but it also helps us make the right decisions for the business,” said a network engineering manager at a midmarket travel and hospitality enterprise. “They have exposure into what we’re doing on the network side, like which rules and policies we are deploying on our firewalls. We know each other’s environments and we’re eliminating knowledge gaps.”

He said collaboration has also reduced costs. “We were spending a lot of money on tools that we didn’t use in the past. It’s powerful when you can avoid spending $1 million on a specific tool when you can buy a platform that meets multiple needs for both groups.”

FIGURE 5. BENEFITS OF SUCCESSFUL COLLABORATION BETWEEN NETWORKING AND SECURITY PERSONNEL



Sample Size = 304

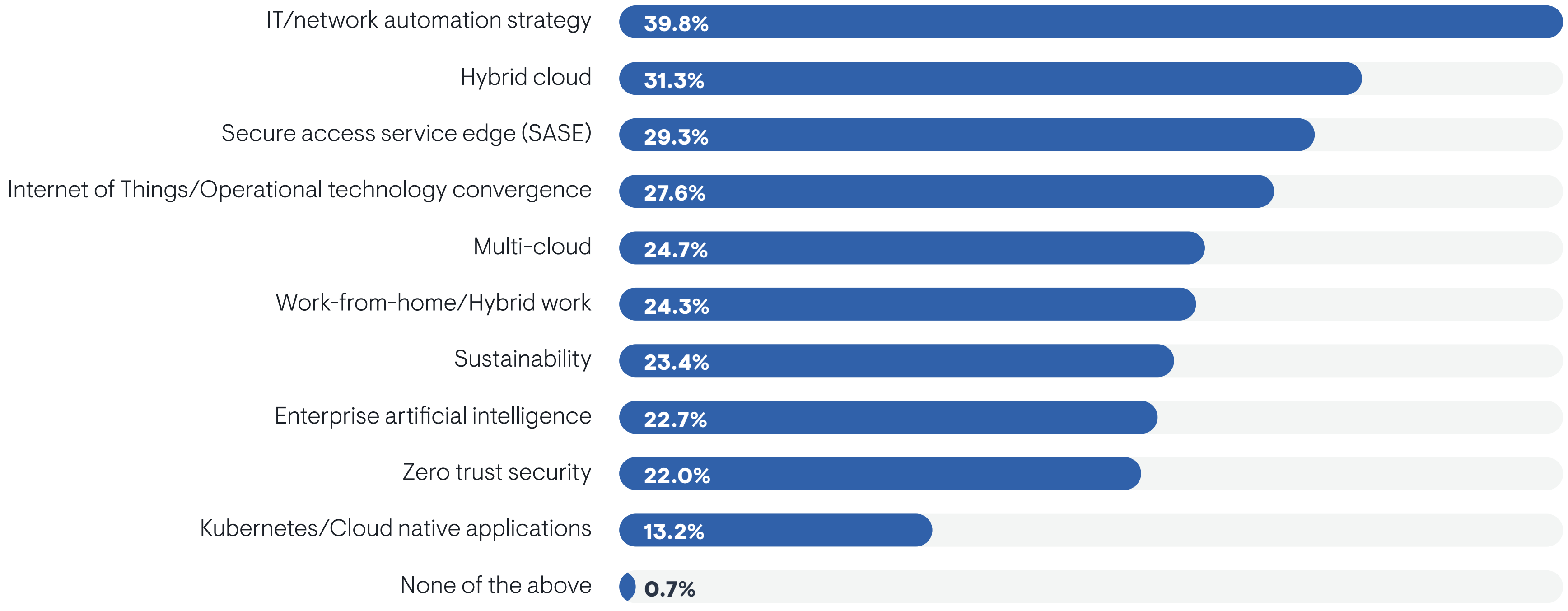
Drivers of Collaboration

Technologies and Initiatives that Push Partnerships

Figure 6 explores the technologies and initiatives that are most responsible for driving network and security team collaboration. The chart reveals that IT and network automation strategies are the most frequent catalyst of these partnerships. There are multiple potential dimensions to this finding. For instance, both groups may be under pressure to improve operational efficiency through automation. Also, automation is an opportunity to reduce network errors that lead to security vulnerabilities and it can improve compliance with network standards and security policies, which are important areas of collaboration between these groups.

Hybrid cloud, SASE, and IoT are secondary drivers. Multi-cloud is not far behind. Respondents who work within a cloud team were more likely to select hybrid cloud than those who work in network engineering or the IT executive suite. This research will explore the collaboration impacts of cloud and SASE in more detail shortly. Enterprise AI is a tertiary driver, but Europeans were more likely (31%) than North Americans (19%) to select it, suggesting that Europeans are more concerned about the network and security implications of AI.

FIGURE 6. TECHNOLOGIES AND INITIATIVES MOST RESPONSIBLE FOR DRIVING COLLABORATION BETWEEN NETWORKING AND SECURITY PERSONNEL

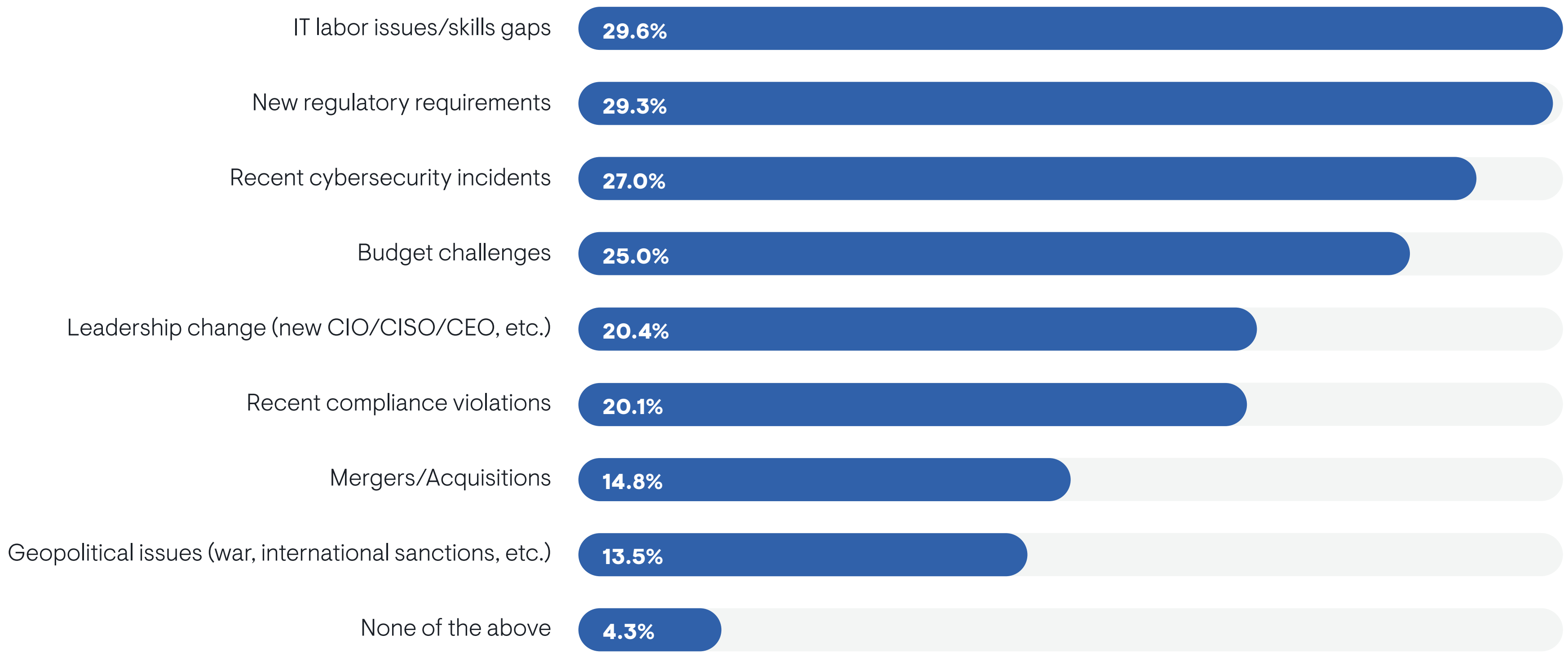


Sample Size = 304

Business Issues and Events that Demand Collaboration

Figure 7 identifies some of the business issues and events that trigger more collaboration between networking and security. The two biggest issues are labor and skills gaps in the technical organization and new regulatory requirements. Many organizations think they can solve skills gaps in networking and security by having the two teams pool their efforts. However, organizations that are less successful with NetSecOps collaboration were more likely to be driven by labor and skills gaps, suggesting that partnerships between these groups are not entirely effective at solving that issue. New regulatory requirements tended to drive organizations in which networking and security teams were still completely siloed from either other. It was also more influential among the largest enterprises in the survey (20,000 or more employees). Recent cybersecurity incidents and budget challenges were secondary triggers of collaboration. Budget issues were cited more often by North Americans than Europeans.

FIGURE 7. ISSUES AND EVENTS MOST RESPONSIBLE FOR DRIVING COLLABORATION BETWEEN NETWORKING AND SECURITY PERSONNEL



Sample Size = 304

Secure Access Service Edge

Secure access service edge (SASE) combines software-defined WAN (SD-WAN) technology with cloud-delivered security services into a unified solution. EMA views SASE as a major driver of NetSecOps collaboration given that it combines two technologies typically managed by separate teams (SD-WAN by networking and cloud-based security by security) into a single architecture. Ninety-six percent of the companies represented in this survey were engaged with SASE technology, including 39% who were in production with a solution, 30% who were implementing, and nearly 27% who were in early stages of evaluating SASE and planning an implementation.

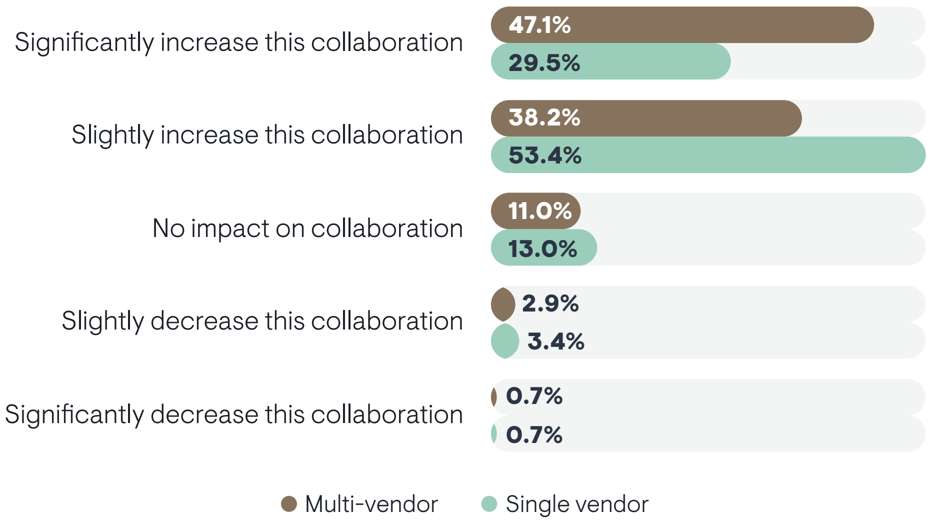
Among respondents whose organizations are engaged with SASE, nearly 83% believe the technology increases collaboration between networking and security teams. More than 37% describe this impact as significant.

Multi-Vendor SASE Requires More Collaboration

Given that SASE solutions integrate networking and security technologies into one architecture, enterprises have a couple of options for how to proceed. They can adopt a single-vendor SASE solution that provides both networking and security technology or they can adopt a multi-vendor strategy, which integrates an SD-WAN vendor's solution with one or more security vendor's solutions. EMA's research found that 47% of organizations prefer a multi-vendor SASE architecture and 50% prefer a single-vendor solution.

Figure 8 reveals that this choice of multi-vendor versus single-vendor can have implications for how network and security teams work together. When organizations follow a multi-vendor path, SASE tends to drive more collaboration between the two groups. For instance, the network team may own the SD-WAN component and the security team may own the cloud security component. The two groups will find themselves working closely around implementation, change management, and operational monitoring and troubleshooting.

FIGURE 8. SINGLE-VENDOR VERSUS MULTI-VENDOR SASE STRATEGIES AND THE IMPACT OF SASE ADOPTION ON NETSECOPS COLLABORATION

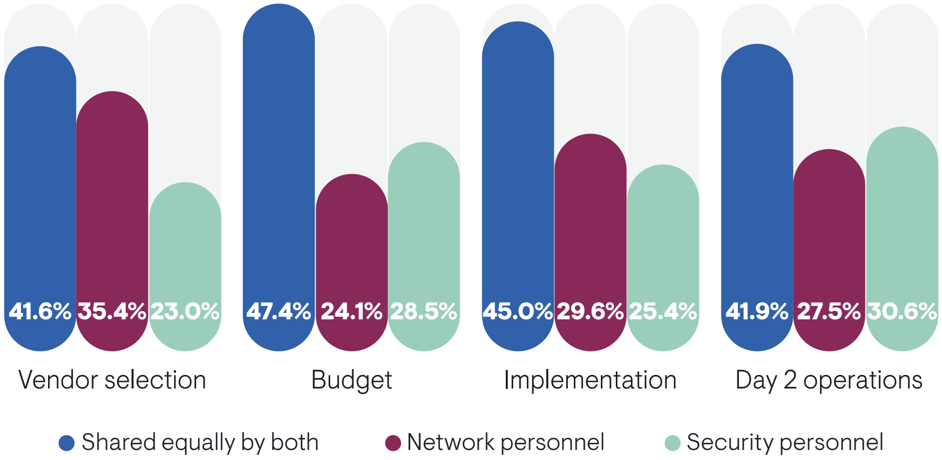


Sample Size = 291

SASE Responsibilities

Figure 9 provides insight into how network and security teams carve out responsibilities for SASE technology by examining who owns vendor selection, budget, implementation, and day 2 operations. Clearly, many organizations expect the two groups to share each of these responsibilities, especially around budget. However, the majority of organizations expect one or the other group to own each stage of the SASE lifecycle. Network teams are more likely to lead on vendor selection and implementation, while security teams are more likely to be responsible for budget and day 2 operations.

FIGURE 9. WHO HAS RESPONSIBILITY FOR EACH OF THE FOLLOWING ASPECTS OF YOUR ORGANIZATION'S ENGAGEMENT WITH SASE TECHNOLOGY?



Sample Size = 291

Public Cloud

Ninety-nine percent of EMA's survey respondents indicated that their organizations are in the public cloud. In fact, 58% revealed that they are using multiple infrastructure as a service (IaaS) providers. 84% of cloud adopters believe cloud use drives increased collaboration between network and security teams, and 39% describe these increases as significant.

"Cloud pushes networking and security together a little bit," said a network engineer with a midmarket technology reseller. "I see instances in which the network is touching the cloud and it's pretty clear that security needs to be notified up front. Network and security teams will have a high-level talk about what they're all okay with and what they can allow to connect."

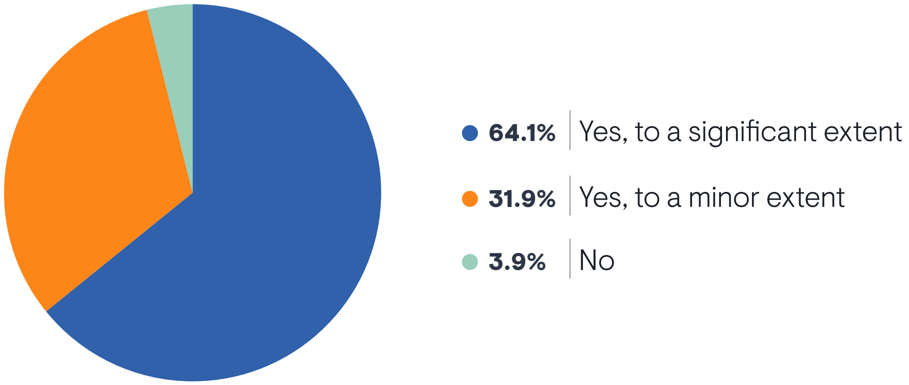
Respondents told EMA that the top four areas of collaboration in the cloud are:

1. Technology implementation (38%)
2. Security incident response/remediation (36%)
3. Network troubleshooting (32%)
4. Infrastructure planning and design (31%)

Security Teams Need Network Data

EMA believes that network and security collaboration is growing in response to a shift in priorities in the cybersecurity world. Many security organizations that formerly devoted most of their time to monitoring hosts and protecting applications and data are now turning their attention to the network. Thus, they need access to more and more network data. The network team's ability to deliver this data becomes an essential collaboration point. **Figure 10** confirms this theory, revealing that in 96% of companies, the security team's need to analyze network data is driving increased collaboration between network and security teams. More than 64% say this is a significant factor in collaboration growth. The network engineering team and the IT executive suite were the most likely groups to perceive this dynamic. Also, technical personnel in general are seeing this data issue drive collaboration more than middle managers.

FIGURE 10. DOES THE SECURITY TEAM'S NEED TO ANALYZE NETWORK DATA DRIVE INCREASED COLLABORATION BETWEEN NETWORK AND SECURITY PERSONNEL IN YOUR ORGANIZATION?



Sample Size = 304

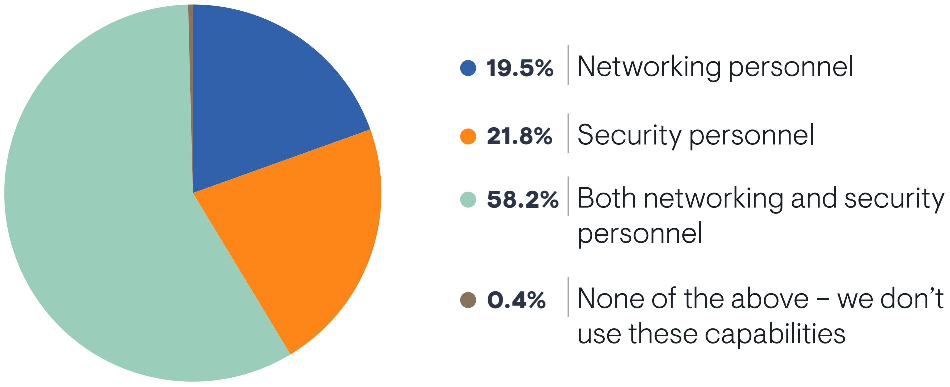
Enabling NetSecOps Partnerships

Security Insights from Network Performance Management Tools

Network performance management tools typically support network monitoring, troubleshooting, and capacity management use cases. However, more than 86% of research respondents told EMA that these tools currently supply them with security insights, which can be potentially valuable to network and security collaboration. In fact, organizations that have such tools reported more success with collaboration.

Figure 11 reveals who uses these security insights. In nearly 20% of organizations, only the network team uses them. In 22%, only the security team does. In the other 58%, both teams leverage these insights. IT executives mostly perceived both groups making use of these capabilities, but technical personnel were more likely to have a siloed view, seeing only one or the other group engaging with them.

FIGURE 11. WHO TYPICALLY ENGAGES WITH AND DIRECTLY USES THE NETWORK PERFORMANCE MANAGEMENT TOOL FEATURES THAT PROVIDE SECURITY INSIGHTS?

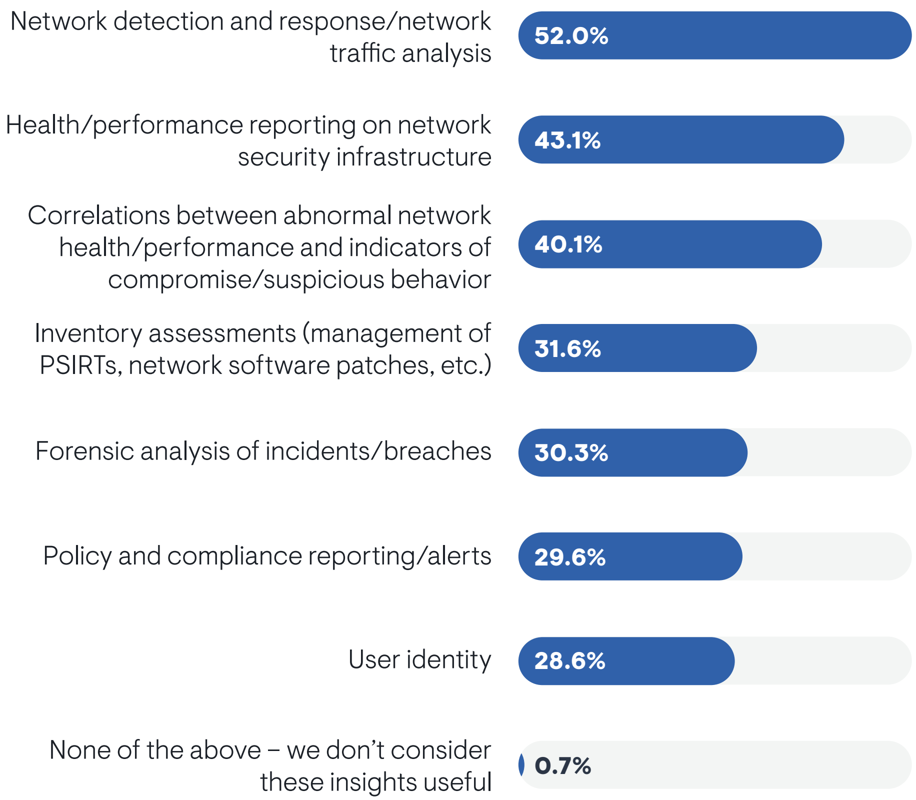


Sample Size = 261

NPM Security Insights that Organizations Use

Figure 12 reveals the kinds of security insights from NPM tools that are delivering value to organizations. Most organizations are leveraging network detection and response (NDR) functionality in these tools. Many NPM tool vendors now offer such capabilities, often as a separate product. NDR analyzes traffic patterns to find suspicious activity rather than relying on signature matching. Members of the cybersecurity team were especially interested in NDR.

FIGURE 12. WHAT KINDS OF SECURITY INSIGHTS DO YOU THINK ARE MOST USEFUL TO GET FROM NETWORK PERFORMANCE MONITORING TOOLS?



Sample Size = 304

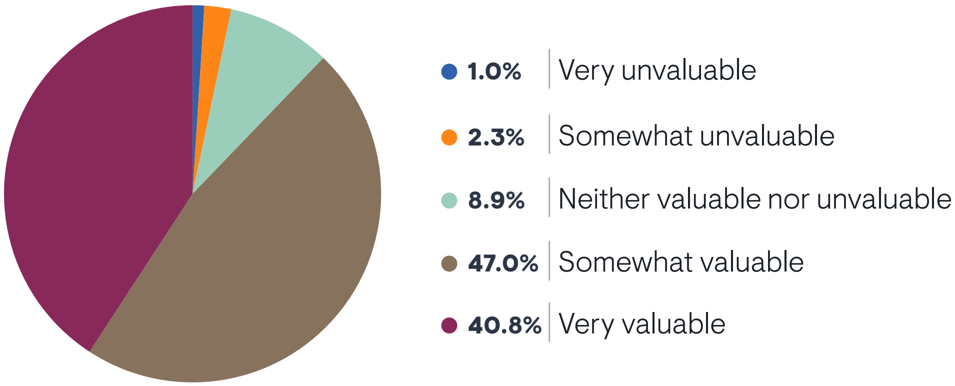
Many organizations are also using NPM to monitor the health and performance of network security infrastructure and to correlate abnormal network health and performance insights with suspicious behavior. The network engineering team was especially likely to see the value of monitoring the health and performance of network security infrastructure.

Inventory assessment is less popular overall, but organizations that are experiencing the most success with network and security collaboration were more likely to see value from such a capability. Policy and compliance reporting was also less popular, but technical personnel perceived more value from it than IT middle managers.

Shared Monitoring Tools

Network teams and security teams have traditionally used separate tools to monitor the network. In some cases, security teams have traditionally focused monitoring on hosts and endpoints, rather than networks. With many NPM vendors increasingly offering security capabilities, **Figure 13** explores whether organizations perceive any value in deploying a shared tool for network monitoring. Forty-seven percent believe it would be somewhat valuable to share a tool across network and security teams, with nearly 41% thinking it would be very valuable. IT executives were more likely (55%) than technical personnel (35%) to believe a shared tool would be very valuable, suggesting the opportunity isn't quite as strong as IT leaders believe. However, organizations experiencing the most success with NetSecOps collaboration were the most enthusiastic about shared tools.

FIGURE 13. IF YOUR NETWORK AND SECURITY PERSONNEL ADOPTED A SHARED TOOL FOR NETWORK PERFORMANCE MONITORING AND NETWORK SECURITY MONITORING, DO YOU THINK SUCH A TOOL WOULD BE VALUABLE?



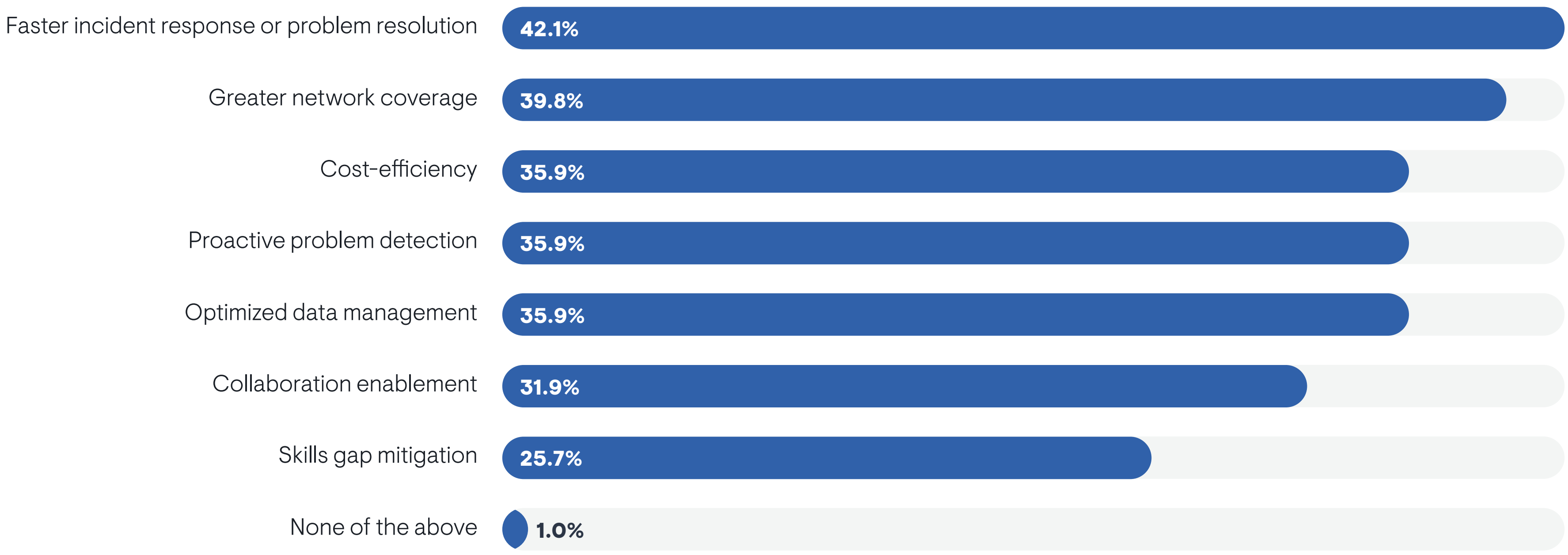
Sample Size = 304

Benefits of a Shared Tool

Figure 14 examines the benefits that research respondents believe their network and security teams would derive from using a shared monitoring tool. The biggest opportunities are faster responses and resolutions of problems and incidents and better overall coverage of the network by a tool. Cybersecurity professionals were more likely to anticipate faster responses and fixes.

Cost-efficiency, optimized data management, and collaboration enablement were the secondary benefits. Respondents that reported the most success with NetSecOps collaboration were more likely to see the opportunity for better data management. Organizations that maintain siloed network and security groups were more likely to see the potential of collaboration enablement with a shared tool.

FIGURE 14. WHICH OF THE FOLLOWING BENEFITS DO YOU THINK YOUR ORGANIZATION COULD MOST LIKELY EXPERIENCE FROM USING A NETWORK MONITORING TOOL THAT NETWORKING AND SECURITY PERSONNEL SHARE?

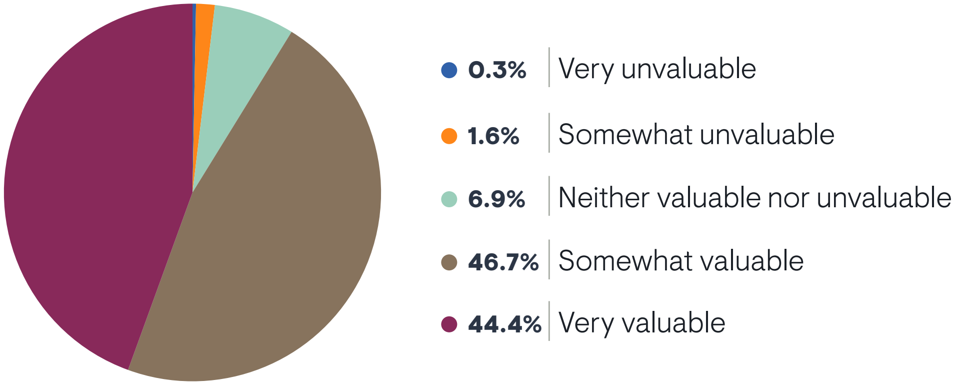


Sample Size = 304

Network Automation Tools

Network automation tools can be a valuable enabler of network and security collaboration, as **Figure 15** suggests. More than 91% of organizations believe it can be at least somewhat valuable for these partnerships. The responses to this question were almost identical to responses to a similar question EMA posted in 2021. IT executives perceive more potential value in automation than technical personnel. Organizations that are the most successful with network and security collaboration are extremely enthusiastic about the role that network automation plays in such partnerships.

FIGURE 15. VALUE OF NETWORK AUTOMATION TOOLS IN FACILITATING COLLABORATION BETWEEN NETWORKING AND SECURITY PERSONNEL

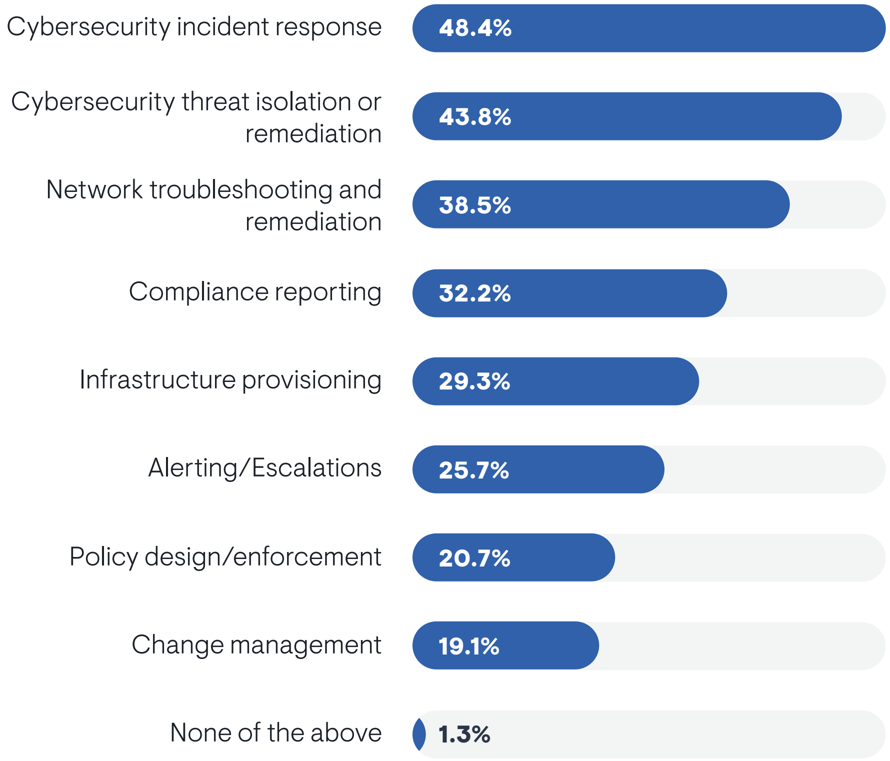


Collaborative Tasks Targeted for Automation

Figure 16 reveals that organizations are typically trying to automate three classes of workflows: cybersecurity incident response, cybersecurity threat isolation and remediation, and network troubleshooting and remediation. Organizations that report the most success with network and security collaboration are more likely to target automation of network troubleshooting. Technical personnel are less interested in automating threat isolation and remediation than IT middle managers and executives. However, members of cybersecurity teams were the most interested in automating threat isolation and remediation.

Sample Size = 304

FIGURE 16. TASKS TARGETED FOR AUTOMATION AS PART OF EFFORTS TO IMPROVE COLLABORATION BETWEEN NETWORKING AND SECURITY PERSONNEL



A security architect with a Fortune 500 software and services enterprise is especially focused on automating data gathering from the network. ”My goal is to get API access to each device and pull the information I need using Python scripts or PowerShell. That helps us get more visibility faster.”

IT executives are more likely to perceive self-service networking and security than technical personnel.

Sample Size = 304

How Network and Security Teams Work Together

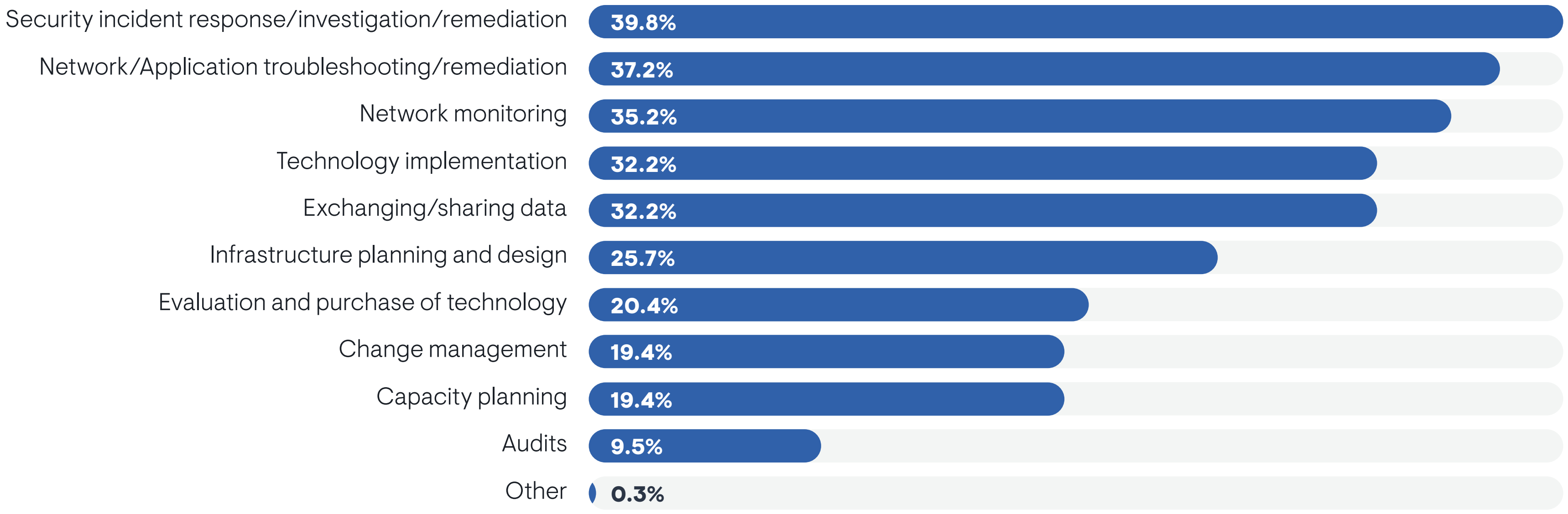
Tasks and Processes

Figure 17 reveals the tasks and processes on which respondents believe network and security teams should focus their collaboration. Security incident response and remediation is the top priority, suggesting that network teams should play a supporting role to ensure that security teams can investigate and fix security incidents as quickly as possible. IT executives are extremely focused on this issue while technical personnel tend to look at it as a secondary priority.

On the other hand, the number-two priority is network and application troubleshooting and remediation, suggesting that security teams should take steps to support network teams on one of their core missions, too.

Change management is a low priority for NetSecOps collaboration; however, organizations that maintain fully siloed networking and security groups make this a top collaboration priority. Capacity planning is also a low priority, but technical personnel were twice as likely as executives to think it's an important collaboration target. Audits are an afterthought for NetSecOps collaboration, but employees of the largest enterprises in EMA's survey (20,000 or more employees) were twice as likely as smaller companies to target them.

FIGURE 17. TASKS AND PROCESSES THAT ARE THE MOST CRITICAL AREAS OF COLLABORATION BETWEEN NETWORKING AND SECURITY PERSONNEL

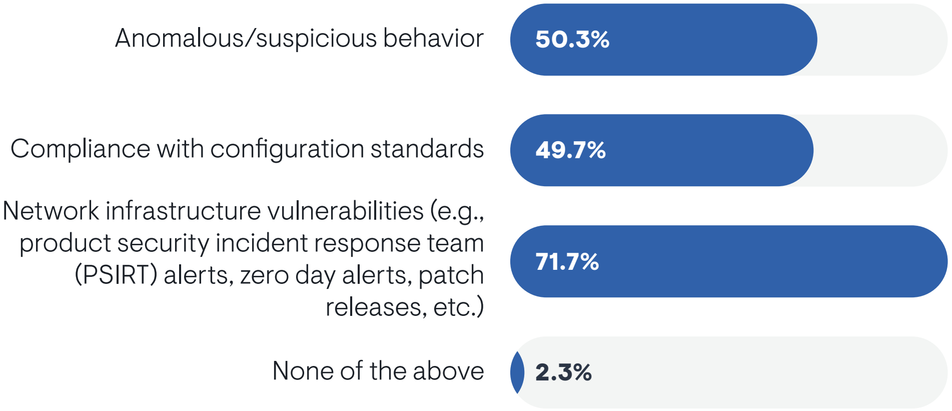


Sample Size = 304

Monitoring the Security Posture of the Network

EMA believes that network and security collaboration encourages network teams to actively monitor their infrastructure for security risks. **Figure 18** reveals that nearly 72% of organizations are actively monitoring their network infrastructure for vulnerabilities, such as zero day alerts and product security incident response team (PSIRT) alerts. Additionally, half are actively monitoring the network for anomalous and suspicious behavior and for compliance with configuration standards. Larger enterprises (20,000 or more employees) are especially likely to monitor for suspicious network behavior.

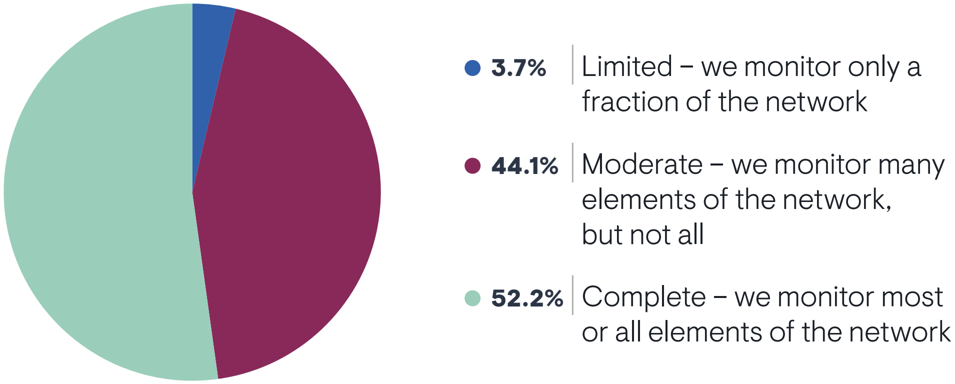
FIGURE 18. DOES YOUR ORGANIZATION ACTIVELY MONITOR NETWORK INFRASTRUCTURE AND SERVICES FOR ANY OF THE FOLLOWING?



Sample Size = 304

Figure 19 reveals the extent to which organizations are able to actively monitor their networks in this way. More than 52% say they can monitor their entire network actively for vulnerabilities, compliance, and threats. These organizations tended to report the most success with network and security collaboration. More than 44% can monitor most of the network, but have some blind spots. Nearly 4% monitor only a fraction of their networks. Members of the network engineering team and the IT executive suite reported more complete visibility. Members of IT architecture groups reported more blind spots.

FIGURE 19. HOW EXTENSIVE IS YOUR ABILITY TO ACTIVELY MONITOR THE SECURITY AND COMPLIANCE POSTURE OF YOUR NETWORK?



Sample Size = 297

Network Data: A NetSecOps Collaboration Foundation

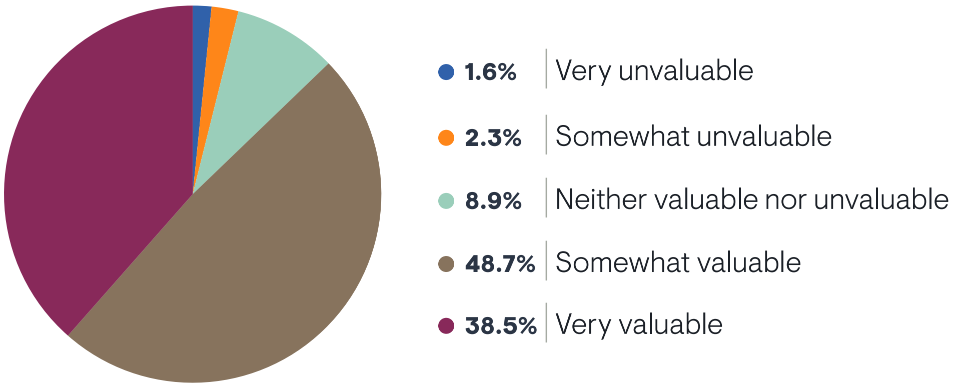
The security team's need to analyze network data is a major factor in why network and security teams have increased their collaboration in recent years. This section explores how that data provides a foundation for collaboration.

Network Packets Drive Collaboration

Packet data is a rich source of intelligence for security teams. Packet headers offer clues about potential trouble, but the plaintext payloads of packet data allow security teams to match malicious data with signature-based security solutions. Packet data also allows organizations to reconstruct an incident during forensic analysis.

Figure 20 reveals that 87% of respondents believe it is at least somewhat valuable for security teams to have access to full packet data, with 39% saying this access is essential. Members of IT architecture teams did not see much value in providing this data to security, but both network engineering and cybersecurity teams agreed that it was very valuable. In EMA's experience, security teams often rely on the network team's expertise to get these packets. Either the security team requests data as needed or the network team establishes a repository that allows the security team to gather the data on demand.

FIGURE 20. HOW VALUABLE IS IT FOR YOUR SECURITY TEAM TO HAVE ACCESS TO FULL PACKET DATA ASSOCIATED WITH THE TRAFFIC THAT TRAVERSES YOUR ORGANIZATION'S NETWORK?

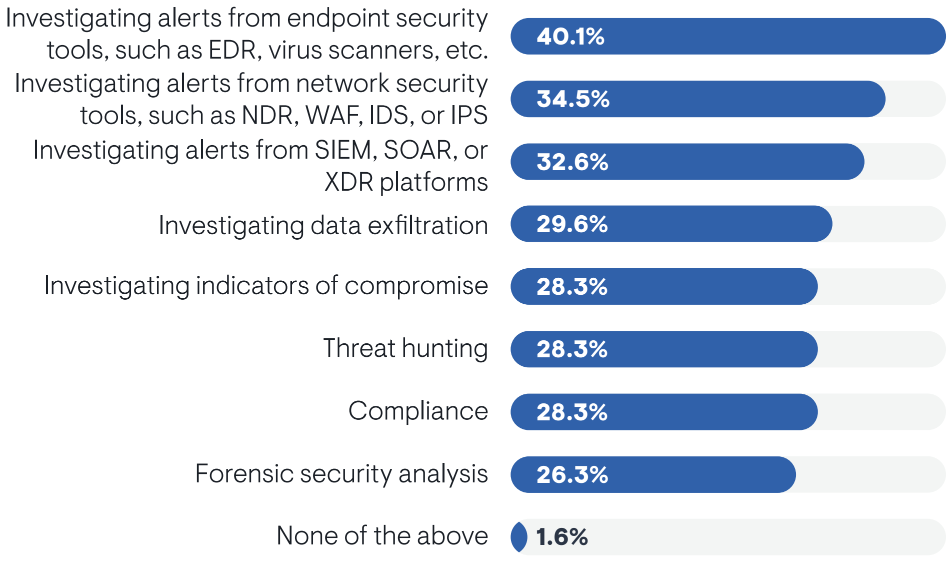


Sample Size = 304

Use Cases for Packets

Figure 21 reveals how security teams use this packet data. The primary use case involves using network data to investigate alerts tied to host-based security solutions, such as endpoint detection and response (EDR) or virus scanners. Clearly, security teams are recognizing that network data can illuminate their host-based security investigations.

FIGURE 21. USE CASES MOST RESPONSIBLE FOR DRIVING THE SECURITY TEAM'S NEED FOR FULL PACKET DATA



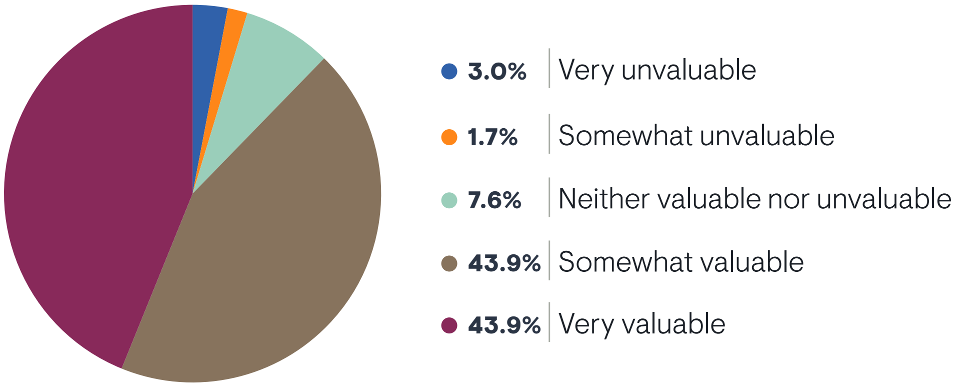
All other use cases were secondary, with investigations of alerts from network security tools and investigations of alerts from security event management platforms (like SIEMs and XDR) slightly more popular than other actions. Threat hunting was a more common use case among technical personnel and middle managers than IT executives.

Sample Size = 304

Cloud Traffic Data

Cloud adoption is a major driver of NetSecOps collaboration. **Figure 22** reveals that cloud traffic data is a major factor in this collaboration. Nearly 88% of respondents said that it is at least somewhat valuable for both networking and security personnel to have access to cloud network traffic. Organizations that are the most successful with NetSecOps collaboration are the most likely to say this traffic data is essential to both teams. Very large enterprises are also especially interested in getting this data.

FIGURE 22. HOW VALUABLE IS IT FOR YOUR NETWORK AND SECURITY TEAMS TO HAVE ACCESS TO NETWORK TRAFFIC DATA IN YOUR ORGANIZATION'S PUBLIC CLOUD ENVIRONMENTS?

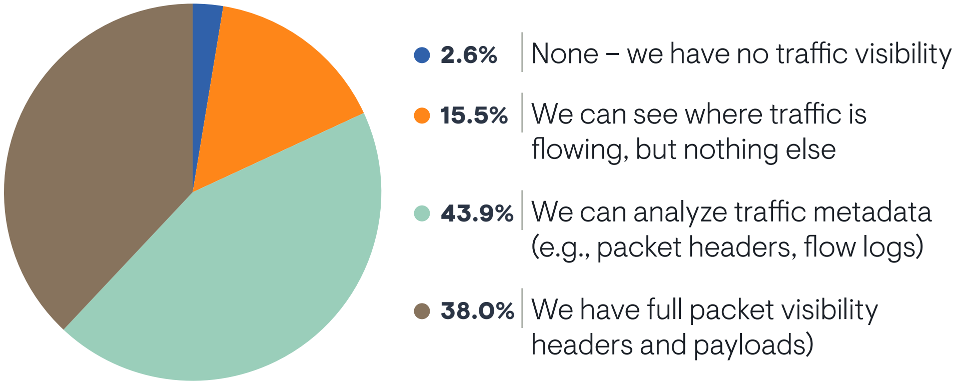


Sample Size = 303

Depth of Cloud Traffic Visibility

Figure 23 characterizes the level of traffic visibility that network and security teams currently have in the cloud. Thirty-eight percent have full packet access while nearly 44% have access to metadata, such as packet headers or flow logs. Nearly 16% can see where traffic is flowing, but nothing else. EMA found that deeper visibility into cloud traffic correlates with better overall collaboration between network and security teams. EMA believes that these teams can partner better on tasks like security investigations and performance troubleshooting when they can dig into packet payloads in the cloud.

FIGURE 23. IN YOUR PUBLIC CLOUD ENVIRONMENTS, TO WHAT EXTENT ARE YOUR NETWORK AND SECURITY TEAMS GETTING VISIBILITY INTO NETWORK TRAFFIC TODAY?



Sample Size = 303

IT executives were more likely to report full packet visibility (55%). Only 37% of technical personnel perceived that depth of insight into cloud traffic, suggesting that IT executives are misinformed on how much traffic intelligence their organizations have in the cloud.

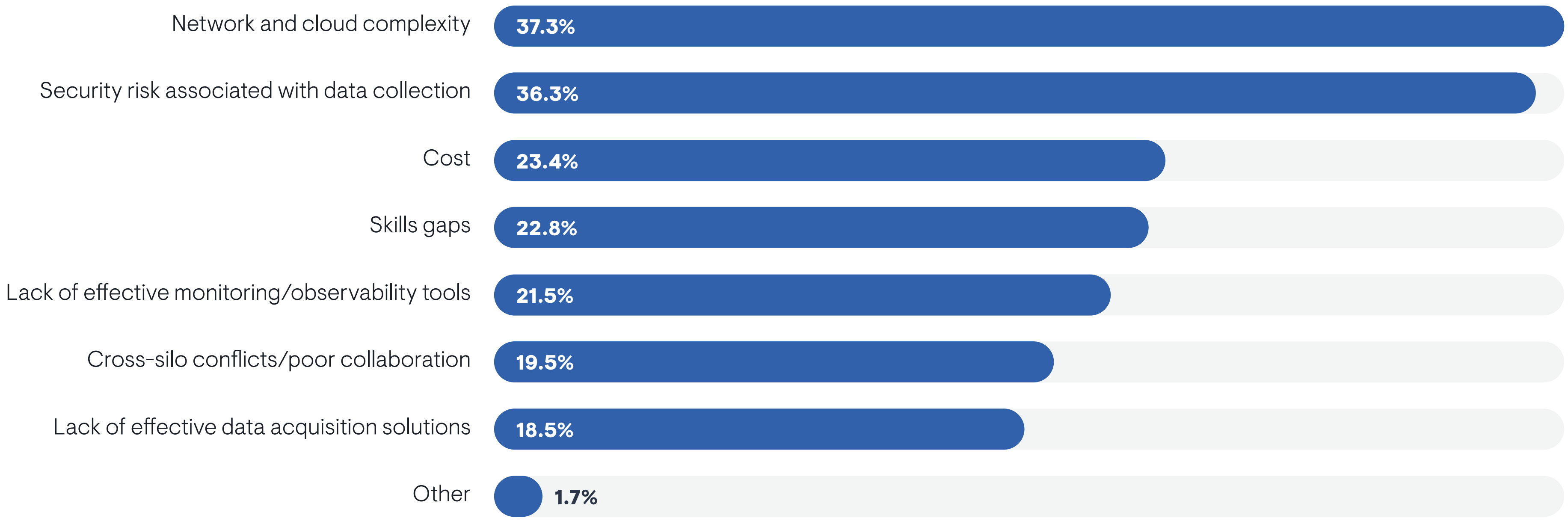
EMA's analysis revealed that organizations have better visibility into cloud traffic when IT leadership successfully encourages network and security teams to deploy shared tools to enhance collaboration. We also found that deep cloud traffic visibility enabled this collaboration to reduce security risk, speed up network problem resolution, and boost both teams' influence over technical initiatives, like cloud migration and transformation. In other words, deep cloud traffic visibility empowers both teams to assume leadership roles in the cloud.

Challenges to Cloud Visibility

Figure 24 reveals the leading barriers to gaining sufficient visibility into cloud traffic data. Surprisingly, cost is only a secondary issue. Instead, organizations struggle with architectural complexity and security risk associated with data collection. The former suggests that network and security teams are struggling to understand the full picture of their company's cloud environments. The latter suggests that they are concerned about the integrity of the tools they use to gather this data. Those tools may be susceptible to malicious activity. Cybersecurity professionals were especially concerned about security risk, while people who work in an IT executive suite were not.

While cost was only a secondary issue overall, members of cloud teams were very concerned about it. Network engineering professionals were less concerned. Among other secondary challenges, cross-silo conflicts and collaboration issues were a big concern for technical personnel. Skills gaps were primarily a problem for organizations that have partially converged their network and security teams.

FIGURE 24. CHALLENGES TO ACCESSING AND ANALYZING TRAFFIC DATA IN THE CLOUD

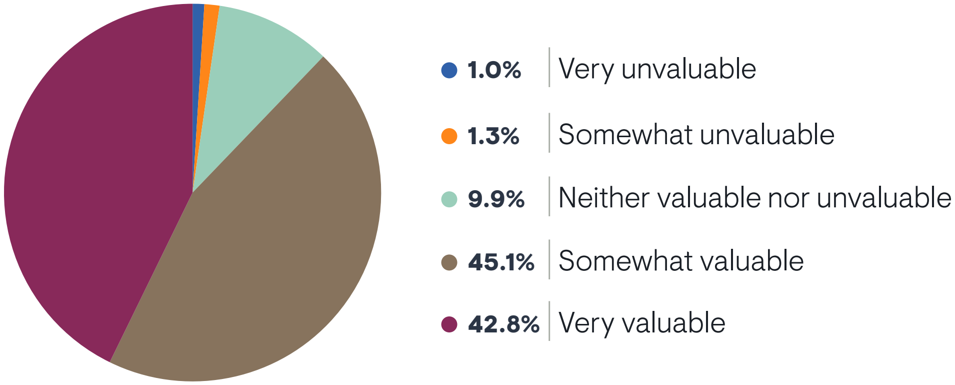


Sample Size = 303

DNS Data

DNS is now a mainstream point of vulnerability, with malicious actors targeting DNS infrastructure with DDoS attacks and using DNS traffic to disguise command and control communications and data exfiltration. Thus, security teams increasingly need to monitor and analyze DNS data. **Figure 25** reveals that 87% of organizations believe it is at least somewhat valuable for the security team to have access to DNS logs and query data. Members of network engineering and cybersecurity teams were especially likely to think it is very valuable for the security team to access DNS data. EMA's analysis found that organizations are more successful with NetSecOps collaboration when they recognize the importance of DNS data to security teams.

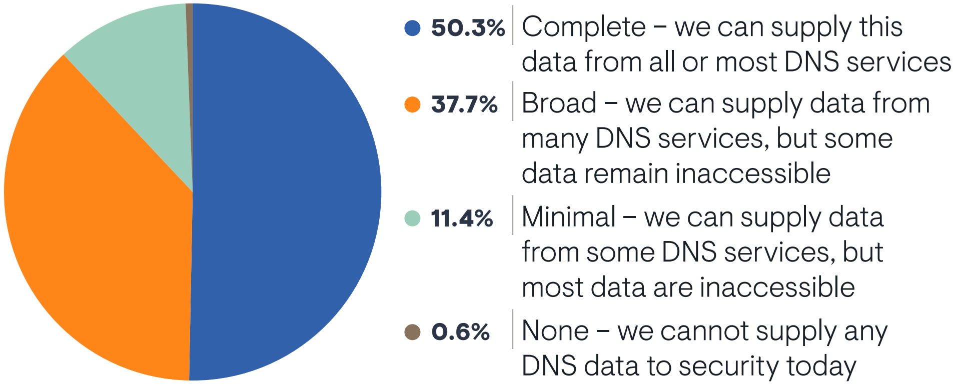
FIGURE 25. VALUE OF PROVIDING SECURITY TEAM WITH ACCESS TO DNS LOGS AND DNS QUERY DATA



The network team often struggles to supply a complete set of DNS data to security because ownership of DNS infrastructure is often fractured. While network teams own a large portion, cloud teams, DevOps teams, and server teams will often maintain their own DNS servers. Network teams struggle to gain visibility and control over all DNS services. **Figure 26** details this challenge. Only half of network teams can supply data from all DNS services to security teams. Nearly 38% can deliver most DNS data, with some of it is remaining inaccessible. Another 11% can only provide data from a fraction of DNS infrastructure.

Sample Size = 304

FIGURE 26. EXTENT TO WHICH NETWORK TEAMS CAN CONSISTENTLY DELIVER DNS LOGS AND QUERY DATA TO SECURITY TEAMS FROM ALL DNS SERVICES



"We've had a lot of projects around DNS to make sure that there aren't any unapproved DNS queries and that there is less risk of random DNS servers being used," said a security architect with a Fortune 500 software and services enterprise. "We track DNS logs and put unapproved DNS queries into a naughty list. Then, we reach out to network engineering and ask them why this is happening."

Organizations that are more successful with network and security collaboration have a more comprehensive ability to deliver DNS data to security teams. Also, when network data is a major driver of collaboration between network and security teams, the network team is better able to deliver DNS data to security teams.

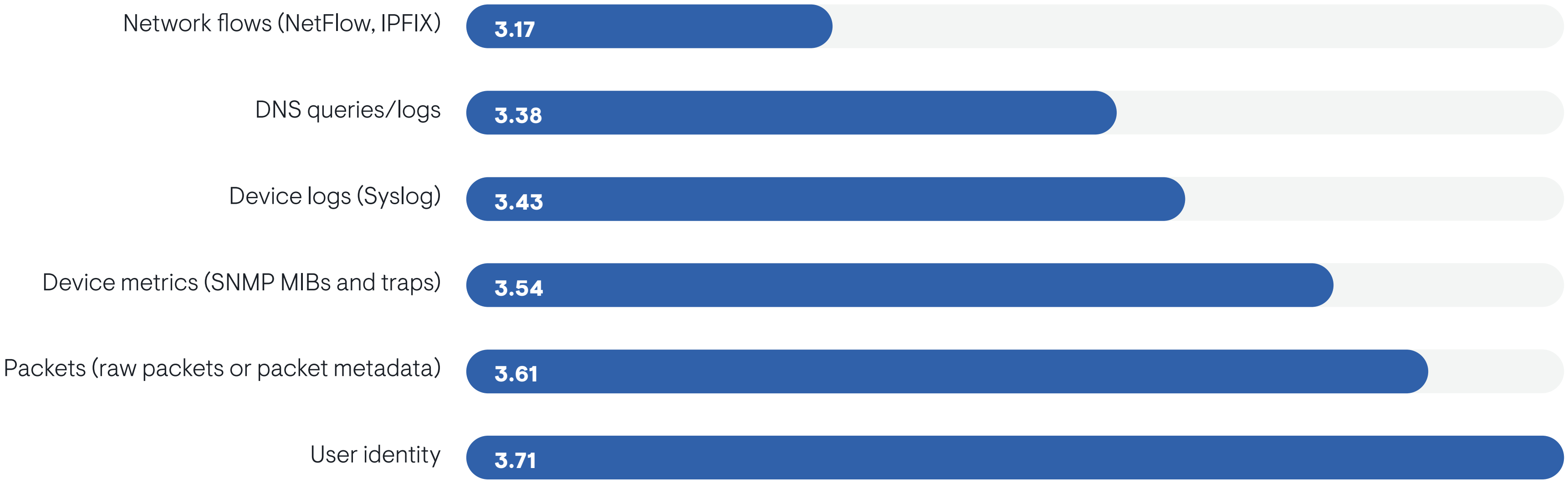
Sample Size = 167

Early Warnings of Security Trouble

Figure 27 reveals the network data that best helps organizations get an early warning about security problems. Network flows are clearly the most essential. This traffic metadata can reveal unusual communications without providing much detail about the nature of the communications.

DNS data and network device logs are the other most valuable network data sources. Packets and user identity are least valuable, suggesting that security teams use these latter sources of data more for analysis of security problems than detection.

FIGURE 27. RANK THE FOLLOWING TYPES OF NETWORK DATA IN TERMS OF USEFULNESS FOR PROVIDING YOUR ORGANIZATION WITH AN EARLY WARNING ABOUT SECURITY PROBLEMS: 1 IS MOST IMPORTANT, 6 IS LEAST IMPORTANT



Sample Size = 304

Conclusion

Collaboration between network and security teams continues to grow, especially with enterprises adopting technologies that drive these groups closer together, including automation tools, public cloud services, and SASE.

When these groups partner effectively, IT organizations can reduce overall security risk, drive operational efficiency, and speed up the detection and resolution of security incident and network fault and performance issues.

There isn't any one right way to establish good collaboration. In fact, some organizations do well with siloed network and security teams that established shared workflows and processes, while others found success by recently converging these groups into one team.

However, it's quite clear that network automation tools can facilitate effective collaboration. So, too, can shared network monitoring tools, or at least network monitoring tools that are extended to offer security insights.

Moreover, network data is an essential currency in the world of NetSecOps collaboration. Organizations must establish an authoritative and accurate repository of network data to support collaboration. Data quality and authority issues emerged as a major challenge to NetSecOps partnerships while it's quite clear that network data facilitates this collaboration, both in on-premises networks and in the cloud. Packets and DNS logs are both essential, but so are network flow records and network device syslogs. EMA recommends that network teams establish authoritative sources of truth for network data to ensure that these groups have a reliable, shared view of the world when they work together.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT analyst research firm that specializes in going "beyond the surface" to provide deep insight across the full spectrum of IT management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 www.enterprisemanagement.com 4368.010324