EMA
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Sponsored by: NETSCOUT

NetSecOps: Aligning Networking and Security Teams to Ensure Digital Transformation

October 2021 EMA Research Report Summary

By Shamus McGillicuddy

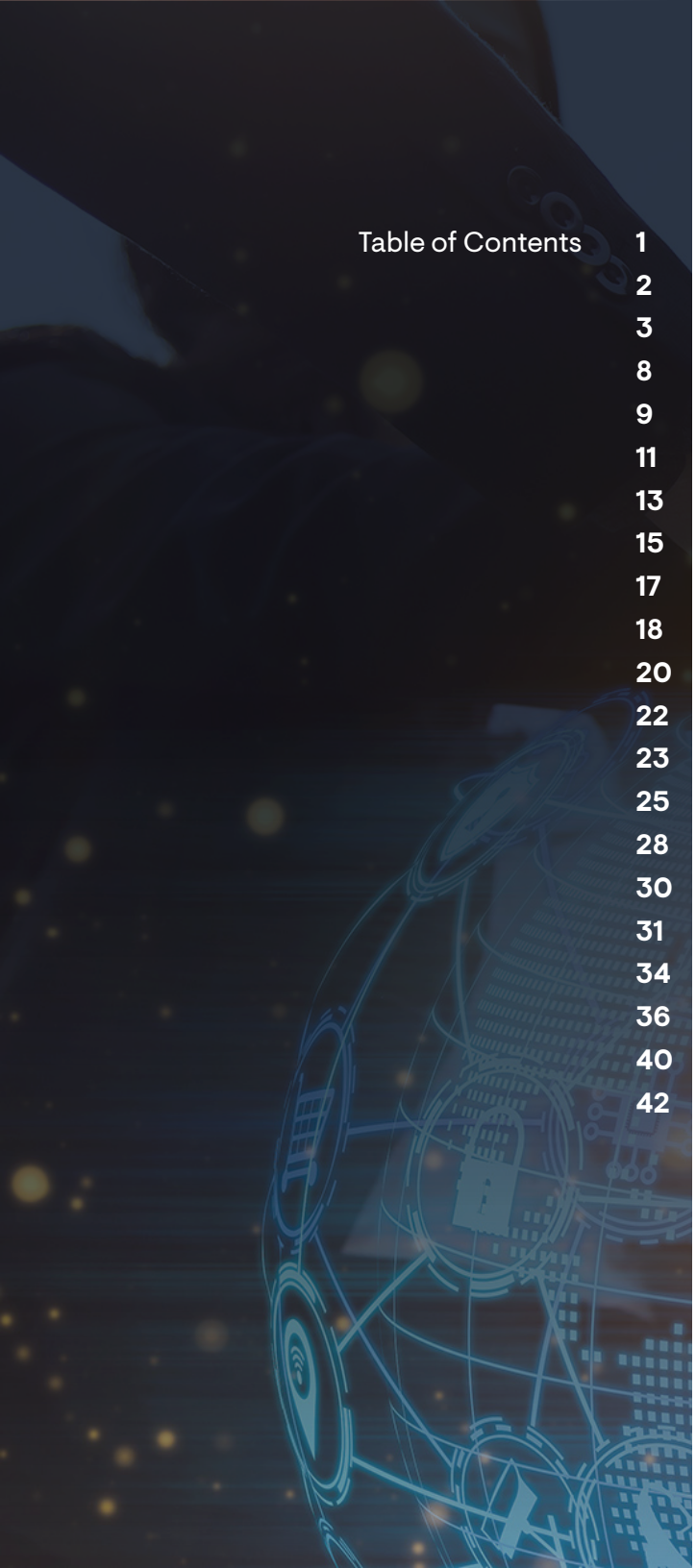


Table of Contents

Introduction

For many years, EMA has observed signs that enterprises are trying to improve alignment between their network infrastructure and operations teams and their information security and cybersecurity teams. EMA market research has revealed increased collaboration between these groups. Also, vendors introduced solutions that facilitate this collaboration. For instance, network performance management vendors have started offering security solutions based on their existing intellectual property. In conversations with IT leaders, the importance of this collaboration comes up again and again. EMA refers to this expanding focus on network and security collaboration as NetSecOps.

Collaboration between network and security groups has always been important. One group is responsible for enabling communication, and the other is responsible for protecting that communication. Security has always been a part of building and operating networks. "I believe that everyone is responsible for security," a director of network engineering and operations for a $7 billion healthcare enterprise recently told EMA. "It's not just the security team's job to do security. Network engineers need to develop security-oriented solutions."

The importance of this partnership has only increased as companies adopt new architectures that open potential security vulnerabilities, such as hybrid, internet-based networks, public cloud, the Internet of Things, and work-from-anywhere connectivity.

Unfortunately, these NetSecOps partnerships are not easy. Security teams and network teams are focused on opposing mandates. Each group views the other group as an impediment or source of trouble. "When the network team is building something and working on a deadline, they see the security team as a roadblock to hitting a milestone, especially if leadership is pushing them to run things tightly," said a network security architect at a $2.5 billion software company.

As digital infrastructure becomes more distributed and hybridized, connectivity between applications, data, users, and devices must be highly available, high-performing, and completely secure. Network and security teams need to work together to ensure this hybrid architecture. With that in mind, EMA sought to understand the nature of NetSecOps partnerships. This research summary reveals the highlights the results of a detailed online survey of technology professionals and in-depth interviews with several stakeholders in billion-dollar enterprises. The following fey findings will be explored throughout this document.

Key Findings

- More than 75% of network and security teams have increased their level of collaboration in recent years.
- NetSecOps partnerships primarily lead to faster resolutions of security issues, reduced security risk, and improved operational efficiency.
- Only 39% of organizations believe they have been completely successful with NetSecOps collaboration.
- Data quality and authority issues, cross-team skills gaps, budget issues, and architectural complexity are the chief roadblocks to NetSecOps collaboration.
- The security team's need to analyze network traffic data drives NetSecOps collaboration in 83% of organizations.
- 97% of organizations are trying to consolidate network packet capture infrastructure that will be shared by networking and security.
- 90% of organizations believe network packet brokers are important to NetSecOps collaboration.
- 80% of organizations are interested in consolidating onto a single network traffic monitoring and analysis tool shared by network and security teams.
- 75% of network teams shared data from their DDI management solutions with security teams.
- 91% of organizations believe that automation tools are important to facilitating NetSecOps collaboration.

Demographics Overview

EMA surveyed 366 technology professionals about their experience with collaboration between network teams and security teams.

EMA surveyed 366 technology professionals about their experience with collaboration between network teams and security teams.

Figure 1 and **Figure 2** reveal the roles that survey participants play in their technology organization. The first chart shows equivalent job titles held by participants, and the second chart reveals equivalent functional groups that they work within. About one-third of participants work in middle management, one-quarter are technology executives, and nearly 40% are subject matter experts. Nearly 20% are in a security team, while more than one-quarter are in an IT executive suite. The rest work in IT architecture, network engineering, and network or data center operations.

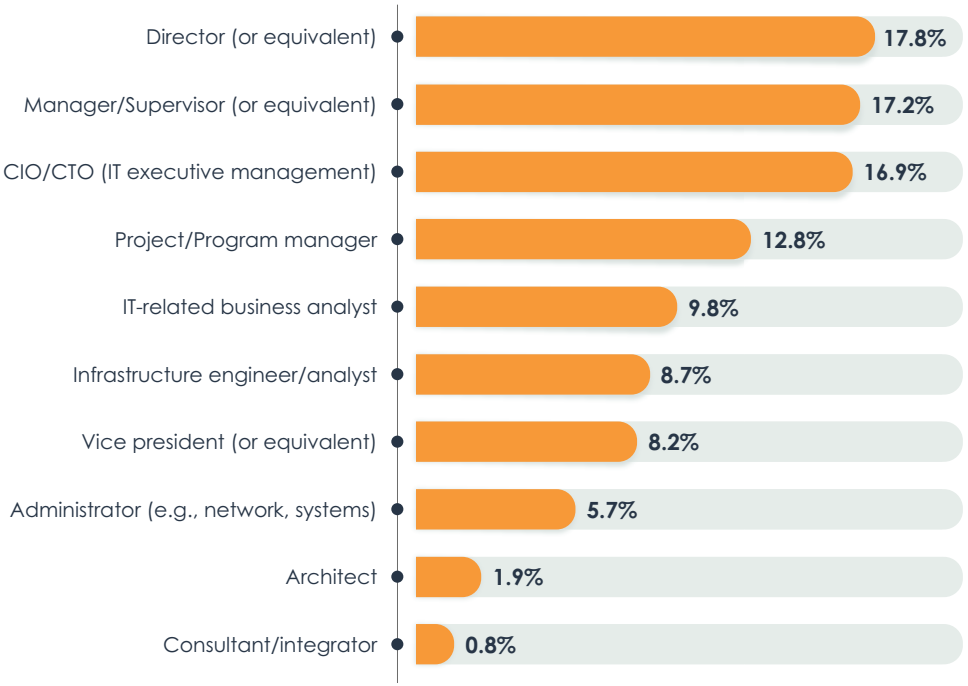


Figure 1. Job Titles

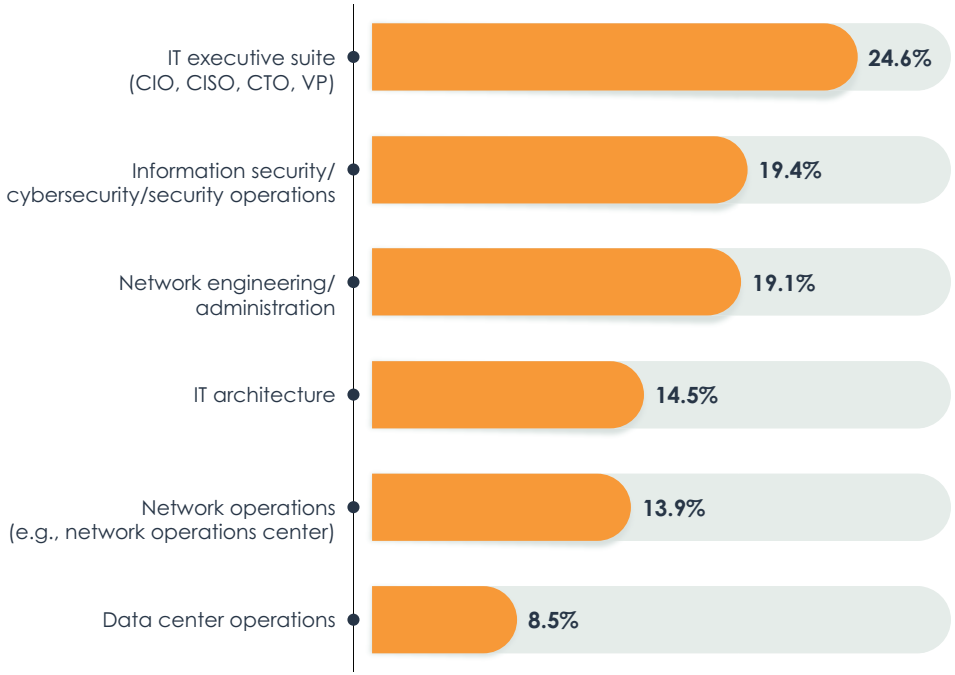


Figure 2. Functional Groups

Sample Size = 366

Figures 3, **4**, and **5** provide insight into the enterprises that these research participants work within. Half of them are based in North America and half are in Europe. The majority work for large or very large enterprises. The four most numerous vertical industries represented are IT services/consulting/managed services companies, retail/wholesale/distribution, manufacturing, and finance/banking/insurance.

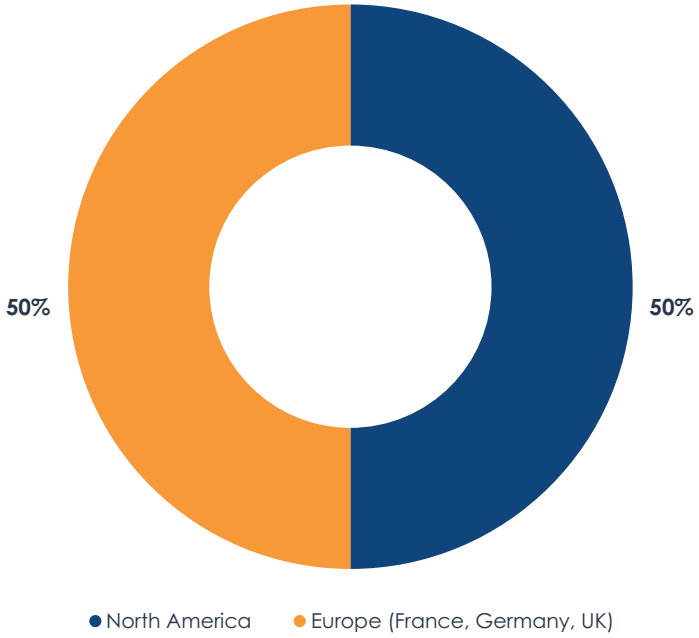


Figure 3. Location of research participants

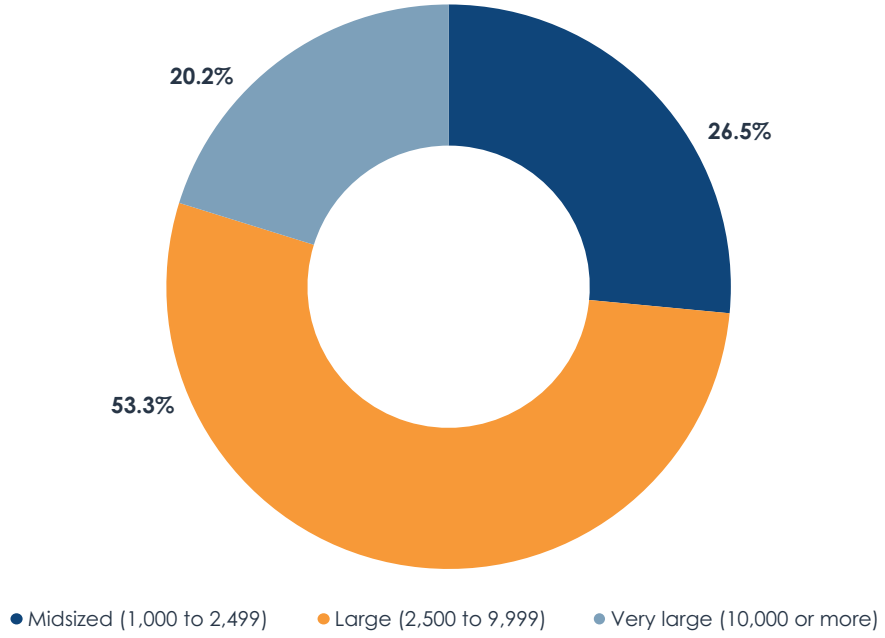


Figure 4. Company size by number of employees

Sample Size = 366

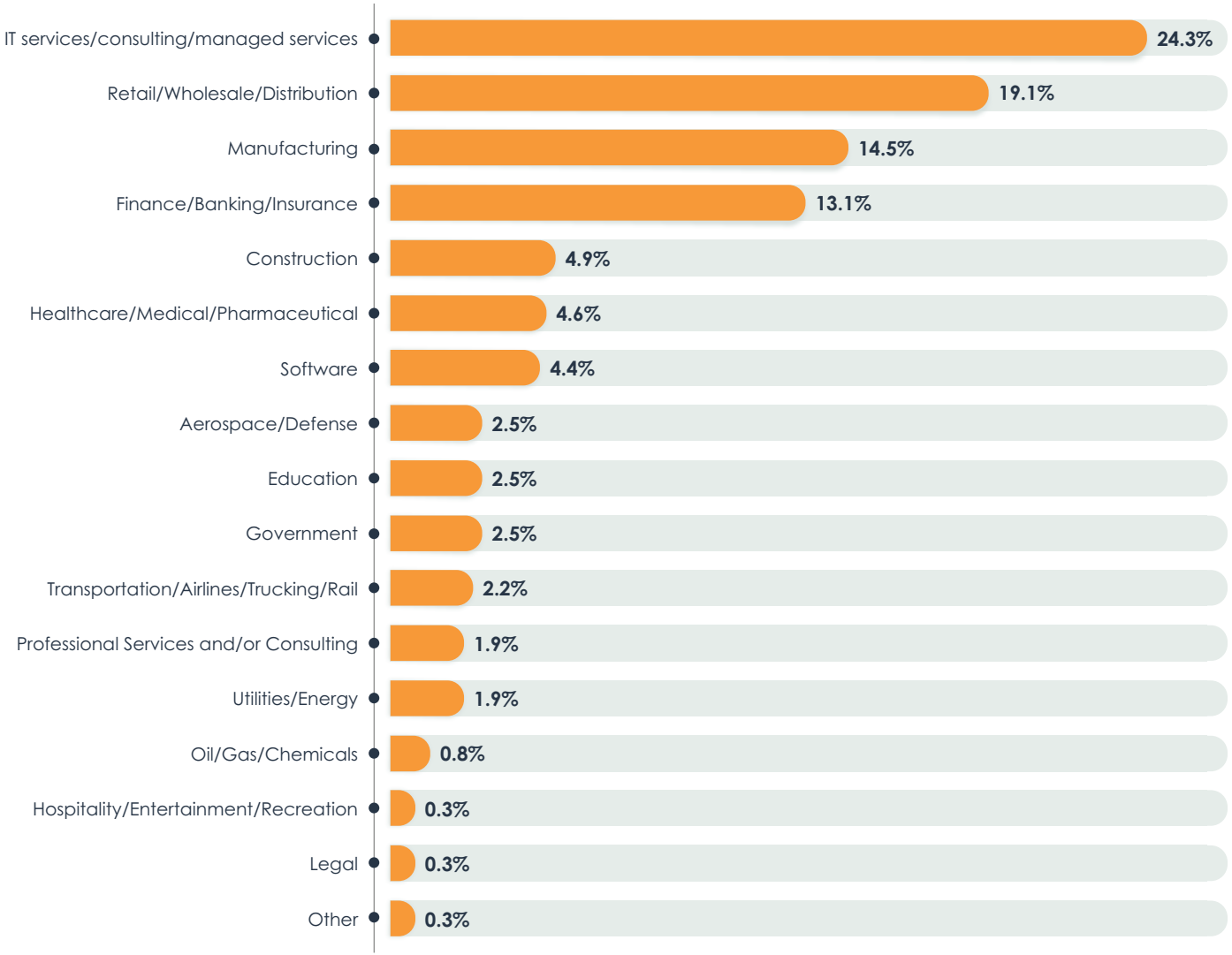


Figure 5. Industries

Sample Size = 366

Finally, EMA wanted to confirm that these survey participants have sufficient knowledge of network infrastructure and operations inside their organizations. We asked them to describe the extent to which their role is dedicated to designing, implementing, and/or managing network infrastructure. **Figure 6** reveals that the vast majority are dedicated primarily to networking, while a small number have more of a cross-domain role, and an even smaller number only collaborate with the networking team. Participants who revealed that they have no significant responsibility for networks or who have no interaction with the network team were disqualified.

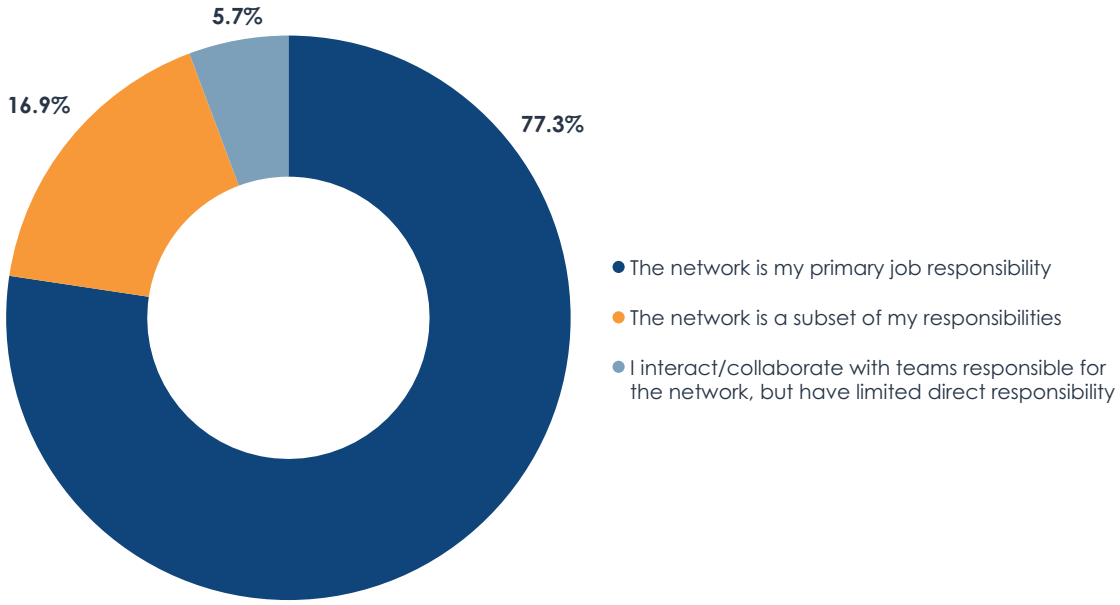
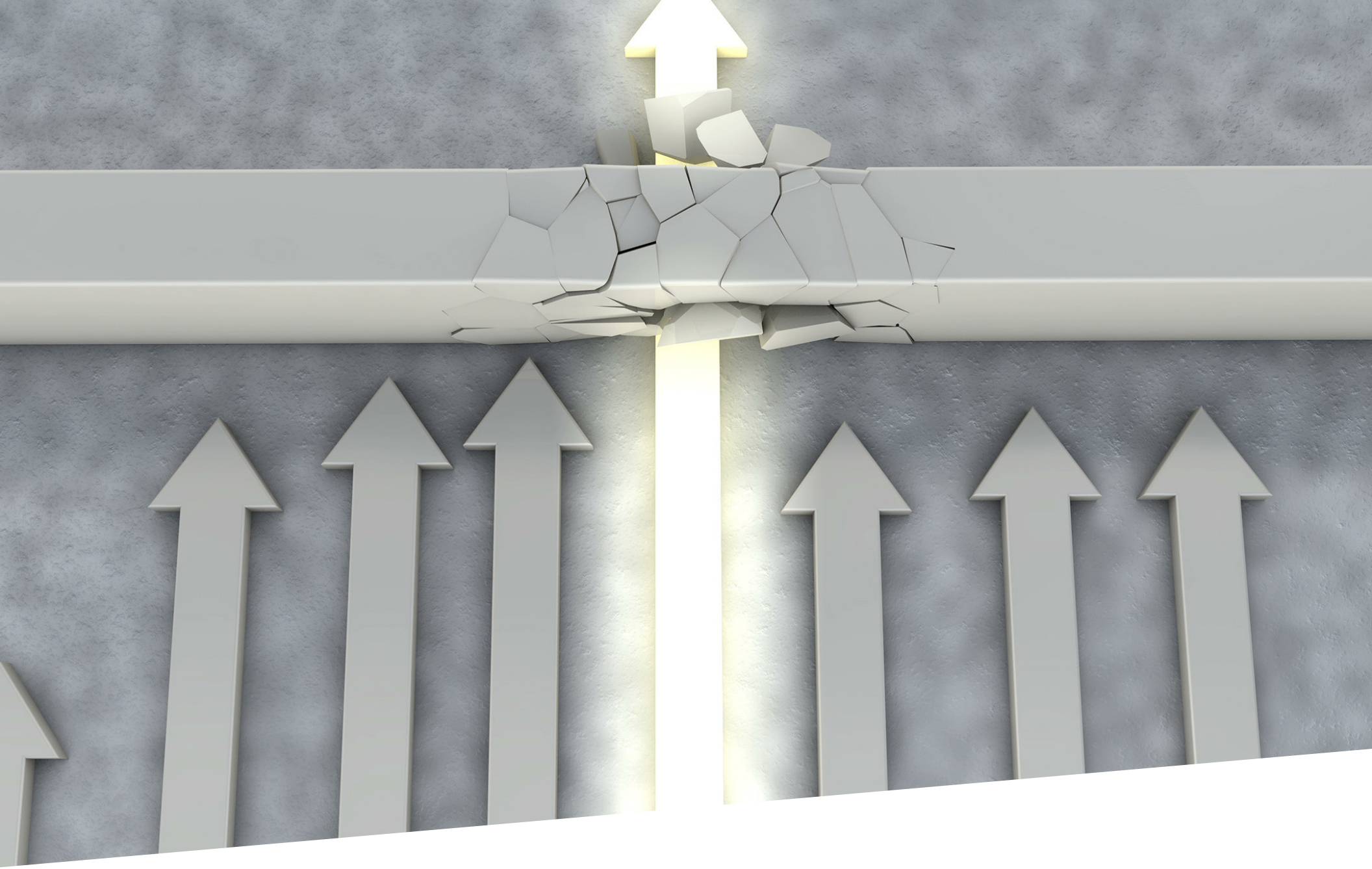


Figure 6. To what extent is your role within the IT organization dedicated to designing, implementing, and/or managing network infrastructure?

Sample Size = 366



Breaking Down Silos Between Networking and Security

EMA's priority was to investigate NetSecOps collaboration in mature IT organizations, where specialized teams have traditionally focused on network engineering, network operations, information security, cybersecurity, and so on. We asked potential survey participants to describe how their IT organization is structured around networking and security. We disqualified people from the survey if they worked for smaller and immature organizations that have nonspecialized teams.

Some IT Organizations are Dissolving Network and Security Silos

Figure 7 reveals that qualified participants were often working for organizations where network and security groups are starting to integrate. While nearly 60% work in companies where specialized groups manage networking and security separately, the rest have recently combined these groups, usually only partially. For example, they might be consolidating into a unified network and security group to work in certain domains, such as the data center or the cloud. Specialized groups are more common in Europe, while partially or fully consolidated groups are more common in North America. Throughout this report, EMA will highlight differences in how enterprises approach NetSecOps collaboration, based on how IT organizations are organized to support networking and security.

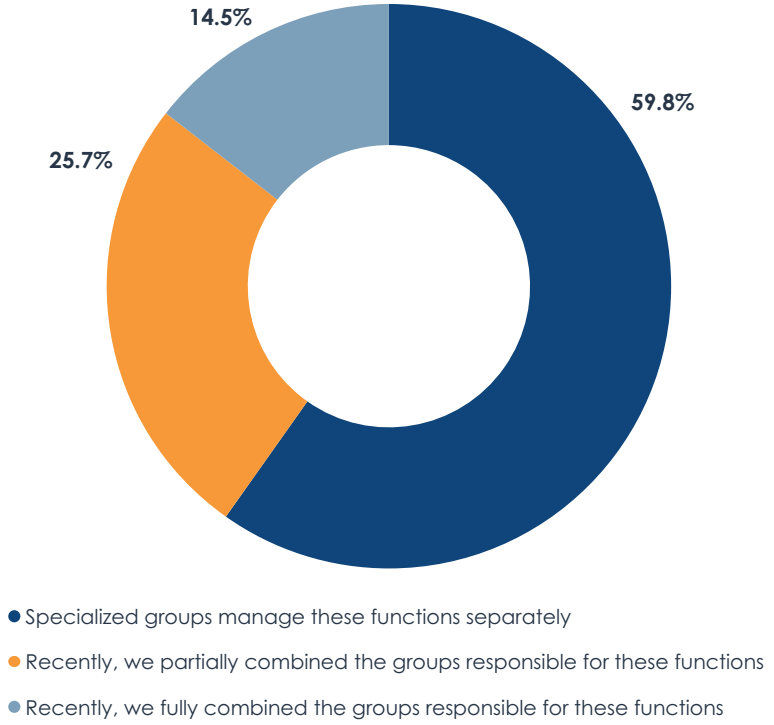


Figure 7. Which of the following best describes how your IT organization is structured around networking and security?

Sample Size = 366

"Over the last few years, we've been extremely collaborative," said a director of global networking for an $80 billion technology company. "We're working on automating the network, and we're looking to provide functionality to other teams, like security via APIs.

"Over the last few years, we've been extremely collaborative," said a director of global networking for an $80 billion technology company. "We're working on automating the network, and we're looking to provide functionality to other teams, like security via APIs. We're trying to automate more and more so they can subscribe to feeds, whether it's DNS infrastructure, the firewalls, and multiple other things."

"Yes, we're collaborating more," said a network security architect with a $2.5 billion software company. "It's not massive. It's slow to grow. All the teams understand that we have to work together and build things with security in mind. It's easier for [the network infrastructure teams] to include us in the beginning. Teams are setting up meetings with us to tell us what they're doing."

Figure 8 reveals why some enterprises are starting to integrate aspects of network and security operations. Three quarters of IT organizations have observed an increase in the amount of collaboration that takes place between these functional groups. Awareness of this trend is highest in the upper echelons of organizations. IT executives and middle management were more likely than technical specialists to see significant increases in collaboration.

Within organizational silos, information security and cybersecurity professionals were the most likely to perceive significant increases in collaboration. Members of IT architecture groups, network operations teams, and data center operations teams were the least likely to report significant increases in collaboration, suggesting a disconnect between silos.

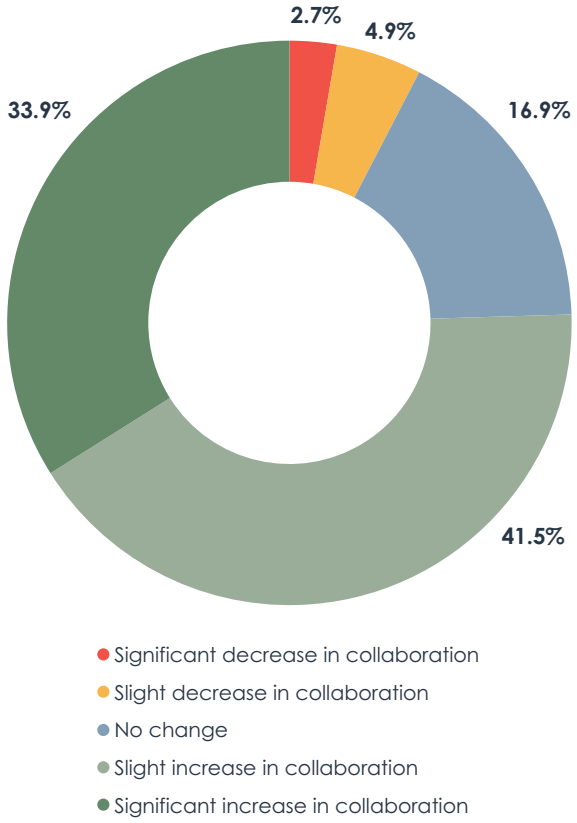


Figure 8. Current trends in the amount of collaboration that occurs between network teams and security teams

Sample Size = 366

The Roles of CIOs and CISOs

While grassroots partnerships can emerge between silos, true NetSecOps collaboration will require top-down leadership. For instance, a network engineer who recently worked for two very large financial services companies said he saw limited collaboration due to lack of top-down leadership. "In one company, management was aware of how siloed networking and security were," the network architect said. "In the other company, executive leadership would basically put out their desire to have that kind of communication, but never put anything in place to make it happen. At both companies, security was always siloed. They stayed to themselves. You could reach out to them to get approvals and talk about what architectural hurdles you were facing, but it was ad hoc. You really didn't know what they were working on, and they didn't know what you were working on."

CIOs and CISOs may be overconfident about how well their top-down leadership is being received.

In 92.3% of organizations, IT leaders have introduced formal policies and programs to encourage and improve collaboration. This was especially common in companies with 2,500 to 9,999 employees (98.5%). **Figure 9** reveals how successful these policies and programs have been. Only 36% of survey participants believed IT leadership had been completely successful. Nearly half saw room for improvement, and 13% perceived some degree of failure.

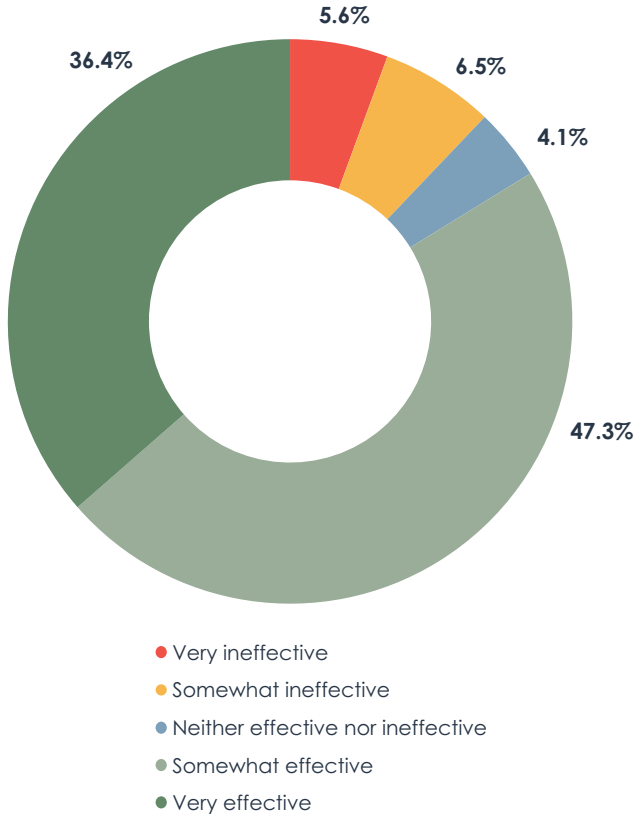


Figure 9. Effectiveness of policies and programs introduced by IT leadership to improve collaboration

Sample Size = 308

IT executives were the most likely to say these policies and programs were very effective (53.3%). Only 20.2% of technical specialists like engineers and architects felt that way. CIOs and CISOs may be overconfident about how well their top-down leadership is being received. Organizational structure also correlates with perceptions of effectiveness. For instance, organizations that have fully combined or converged networking and security teams are the most likely (51.9%) to say IT leadership has succeeded in driving collaboration. That being said, organizations in which these two functions are still siloed into different groups were also somewhat more likely (40.2%) to report very effective programs and policies. Those enterprises which have only partially converged networking and security were the least likely (18.4%) to say IT leadership was very effective in driving collaboration. This points to a need for an all-or-nothing approach. Partially converging groups does not encourage successful collaboration.

Figure 10 reveals the kinds of policies and programs CIOs and CISOs introduce to encourage better partnerships between networking and security. First, IT leaders are reaching for an old favorite, implementing formalized best practices and processes, like ITIL (Information Technology Infrastructure Library) or ITSM (Information Technology Service Management).

Most enterprises also reported that leadership had reorganized IT groups or leadership, instituted budget sharing, and provided new training opportunities to improve collaboration. Employee incentives like bonuses and salaries were the least popular tactic.

"I've been added to committees, and we have quarterly meetings where global security comes and presents," said a director of global networks with an $80 billion technology company. "We come up with priorities for collaboration based on business priority."

The organizations with the most effective policies and programs for improved NetSecOps collaboration were most likely to pursue the following four programs:

1. Best practices and polices, like ITIL and ITSM
2. Budget sharing
3. Reorganizations of groups and leadership
4. Budget increases

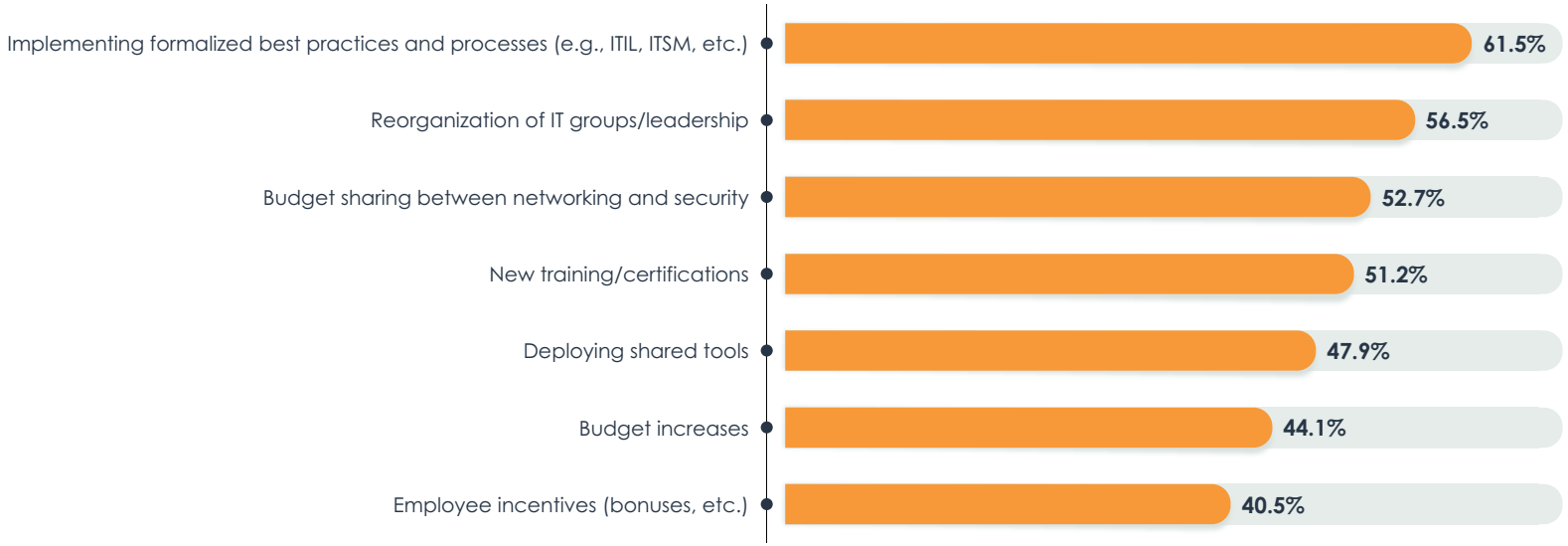


Figure 10. Policies and programs that IT leaders introduce to encourage and improve NetSecOps collaboration

Sample Size = 338,
Valid Cases = 338,
Total Mentions = 1,198

Drivers of NetSecOps Collaboration

Specific technology initiatives can drive increased collaboration between networking and security. EMA asked survey participants to answer yes or no as to whether each of seven leading technology trends is prompting these teams to work together. **Figure 11** is an aggregation of the yes responses to those questions. It reveals that the cloud, work-from-anywhere, data center automation, and the Internet of Things are all major drivers of NetSecOps collaboration. Europeans were more likely than North Americans to identify SD-WAN/SASE and zero trust security as significant drivers of collaboration.

"The key driver is cloud adoption," said a network architect with a $100 billion bank. "It requires a certain kind of change in mindset. The cloud is all about agility and quick turnarounds. It requires more collaboration. Now, if you put an antiquated security policy in the cloud, it defeats the entire purpose of the cloud."

The cloud, work-from-anywhere, data center automation, and the Internet of Things are all major drivers of NetSecOps collaboration.

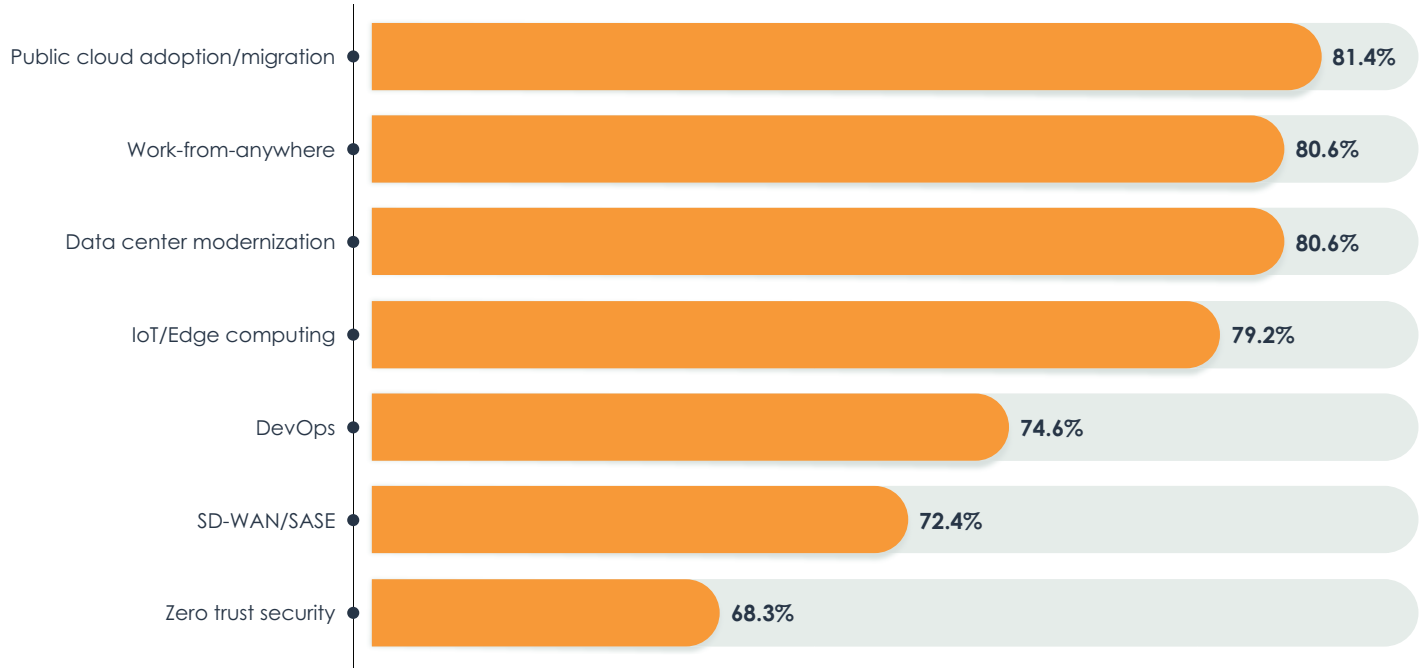


Figure 11. Technical initiatives are driving increased collaboration between network teams and security teams

Sample Size = 366

Benefits and Challenges of NetSecOps Collaboration

Overall, most research participants felt rather good about how networking and security work together. Eighty-six percent reported at least some success, although **Figure 12** shows that nearly 47% believe they are only somewhat successful, meaning they see some room for improvement.

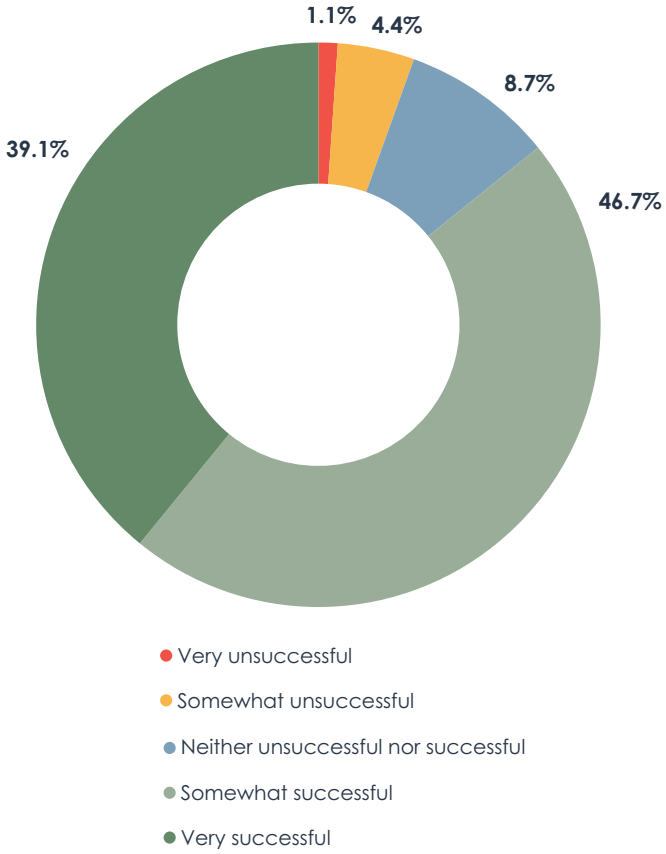


Figure 12. Overall success with NetSecOps collaboration

Sample Size = 366

Benefits of Collaboration

Figure 13 reveals the kinds of returns that organizations earn when they successfully foster NetSecOps collaboration. Clearly, improved security is the biggest opportunity. A majority of survey respondents selected both faster resolutions of security issues and reduced security risk. Operational efficiency, faster resolution of service problems, increased influence over technical initiatives, and overall network resilience were all secondary benefits. "Things move faster with good collaboration. There are less roadblocks," said a network architect with a $100 billion bank.

One architect saw improved resilience and reduced security risk. "Successful collaboration leads to a tighter implementation to meet requirements," said a network security architect with a $2.5 billion software company. "We get more viewpoints and ideas in terms of past experience. You will get a final product that is more secure, better implemented, and can recover from disaster." Security professionals were more likely to call out faster resolution of security issues as a benefit, while network engineering team members tended to select faster resolution of user experience and network performance issues. This disparity suggests that silos have different views of how NetSecOps collaboration can benefit an organization. However, both security and network engineering teams were more likely than others to perceive heightened influence over technical initiatives, which could serve as common ground when these groups are searching for reasons to embrace partnerships with each other.

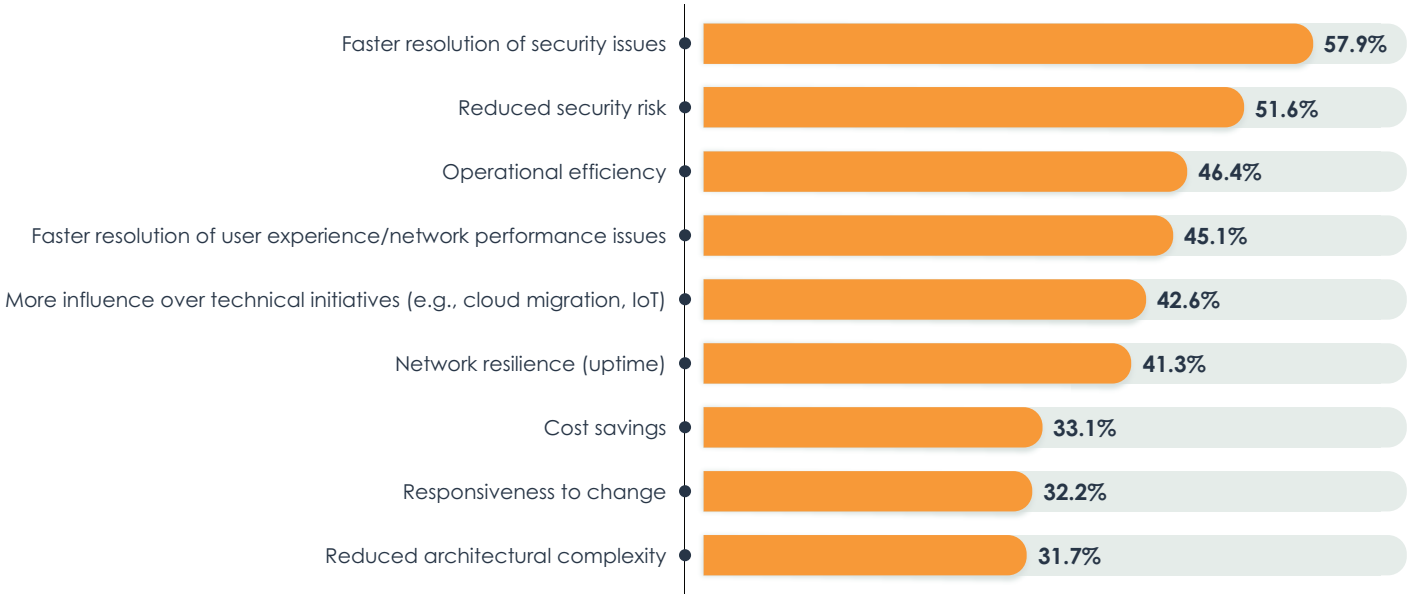


Figure 13. Benefits experienced by organizations when the network team and security team successfully collaborate

Sample Size = 366, Valid Cases = 366, Total Mentions = 1,398

Collaboration Challenges

Figure 14 details the top challenges that network teams and security teams face when they try to collaborate. The top issue is data. When sharing, network and security teams struggle with the quality of that data and authority of different data sets. One data set indicates one thing, while another data set indicates another. Data quality and authority are bigger issues for organizations that are the most successful with NetSecOps collaboration, suggesting it's a difficult issue to solve. IT organizations that have reorganized to fully combine network and security teams are more likely to struggle with data quality and authority, while siloed organizations are the least likely. This points to a potential problem that arises when organizations try to consolidate their tools and data.

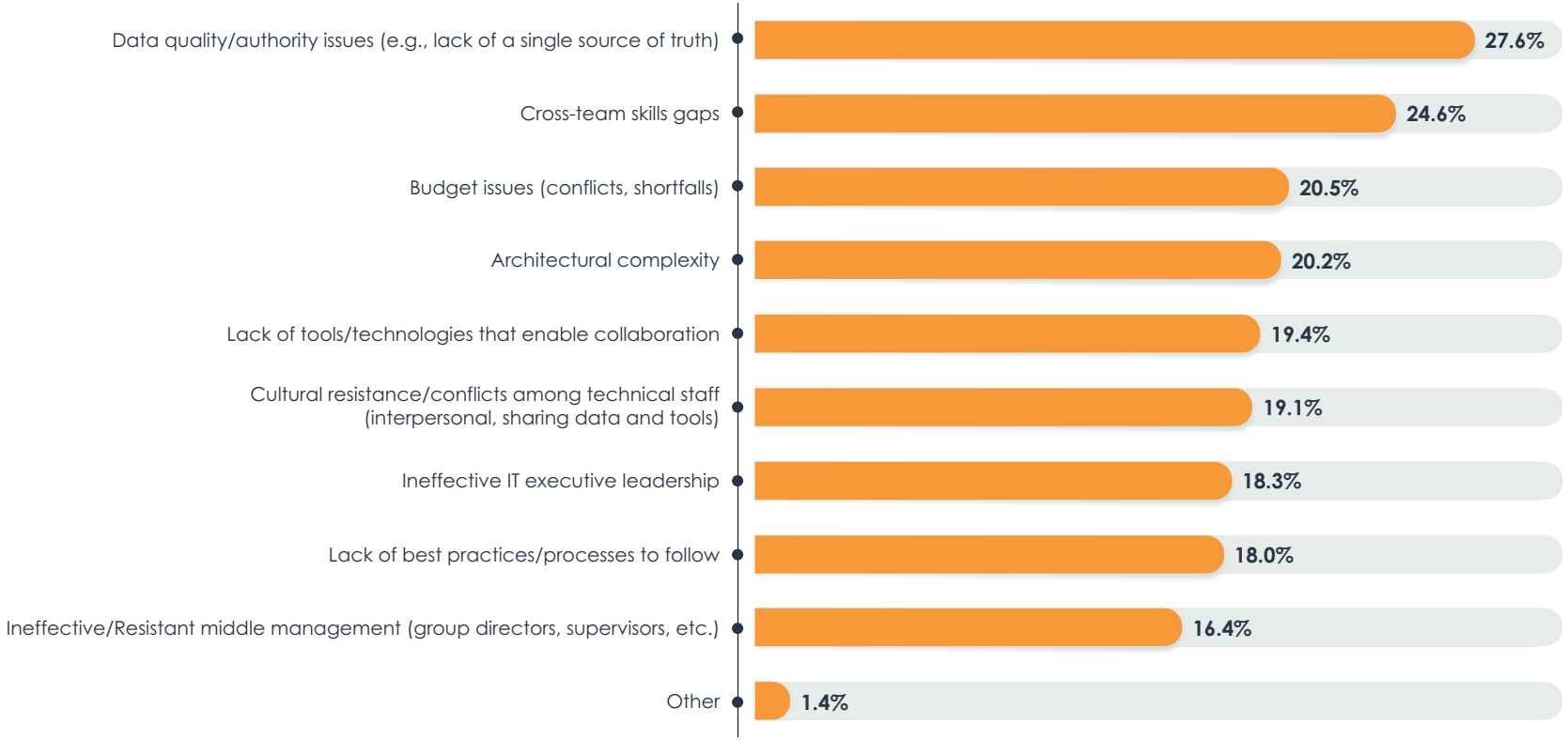


Figure 14. Leading roadblocks to collaboration between the network team and security team

Sample Size = 366, Valid Cases = 366, Total Mentions = 679

"Security people in general are not super well-versed in networking," said a network engineer who recently worked for two very large financial services companies.

Cross-team skills gaps are also a top challenge. "Security people in general are not super well-versed in networking," said a network engineer who recently worked for two very large financial services companies. "I do think cross-group knowledge is where that divide comes from. There would be a clash because of knowledge gaps, one team trying to butt heads with other team because they didn't agree with what the other team doing because of a knowledge gap."

"We talk to security every two or three months, and they want to ask a lot of theoretical questions that aren't particularly relevant to what is being discussed," said a network architect with a $15 billion retail company. "We will tell [the security team] that the application team is about to do something, and we ask them if they think it's a good idea or bad idea. They get too esoteric. They ask, 'Why is the application team putting this here instead of there?' That ship has already sailed. The application team made its decision. We often get the sense that [security] doesn't understand what the business is."

The other top challenges are budget issues, architectural complexity, a lack of tools and technologies that enable collaboration, and cultural resistance. Organizations in which IT executives have introduced very effective policies and programs to encourage NetSecOps collaboration are less likely to struggle with architectural complexity and budget issues. On the other hand, organizations that are less successful with collaboration are the most likely to struggle with architectural complexity, suggesting it is one of the most difficult hurdles to overcome.

Cultural conflicts can stem from the silo mentalities that many teams perpetuate, and they can be exacerbated by a lack of resources. "The silos are a big thing because they come with their own set of prioritizations," said a director of network engineering and operations for a $7 billion healthcare enterprise. "If you look at security, I don't envy them. They're severely understaffed, as we are. With contentions around staffing, they focus more on their own silo priorities versus the priorities of the enterprises as a whole. And then collaboration falls apart."

Finally, Europeans were the most likely to struggle with cultural resistance and a lack of best practices and processes. Many of the individuals that EMA spoke with called out cultural and political issues.

How Network and Security Teams Work Together

"Change management is the most important," said a director of global networks with an $80 billion technology company. "We've trained security to look at certain things even before it comes to us.

EMA asked research participants to identify the general tasks for which they think it is most important for network and security teams to collaborate. **Figure 15** reveals technology implementation is the top priority, followed by infrastructure planning and design and technology evaluation and purchasing.

Operational monitoring is important to nearly one-third of organizations. It is a higher priority for organizations that have fully converged network and security teams. This involves the implementation and use of monitoring tools to ensure performance and security visibility. "We ask [the network team] during a build, what kind of visibility do you have if someone is coming after this asset?" said a network security architect at a $2.5 billion software company. "Where is logging going? How is it being stored if it is PCI-related? We're focused on making sure tools are fed the proper information."

Change management and troubleshooting/incident response are the lowest priorities. Network engineering and network operations teams were more likely to select change management, while security teams and IT executives were less likely to select it. Change management is also a more common focus for Europeans, but it's more popular with organizations that are less successful with collaboration, too.

"Change management is the most important," said a director of global networks with an $80 billion technology company. "We've trained security to look at certain things even before it comes to us. If someone requests a change to routing or firewalls, the first person that approves that change is the info security team. It is tedious. People say, 'I don't want to be on a weekly call for an hour and a half because we have a lot of changes.' We explain, 'You need to listen in because it might be service-impacting.'"

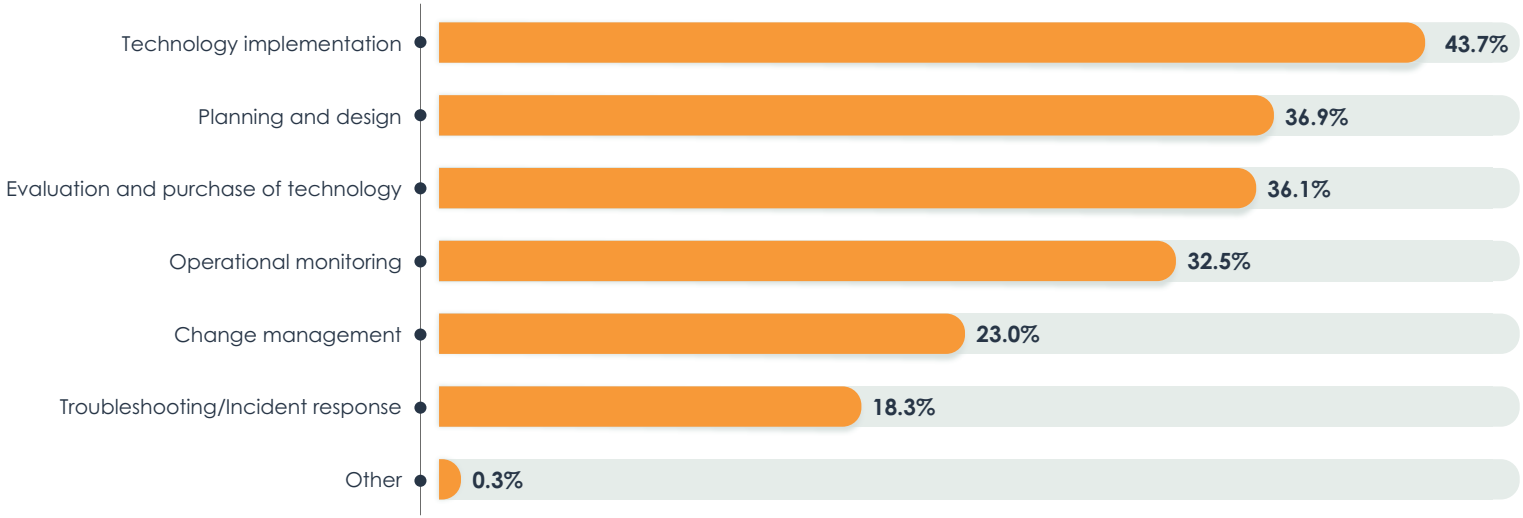


Figure 15. Tasks for which NetSecOps collaboration is most important

Sample Size = 366, Valid Cases = 366, Total Mentions = 698

Network Data: Driver and Enabler of NetSecOps Collaboration

Network data is essential for network and security collaboration because it allows these teams to gain a shared view of digital infrastructure and services. However, the security team's need for network data can also be a driver of this collaboration. Quite often, the network team owns network data and serves as a gatekeeper that the security team was working with to access data for analysis. Also, some security groups have a limited understanding of network data, such as packets and flows. Instead, their days are spent analyzing endpoint data, like logs. They may rely on the network team to help them understand network data.

Security Teams Require Access to Network Traffic Data

A security team's need to analyze network data is leading to increased collaboration with the network team in 83% of enterprises.

Figure 16 reveals that a security team's need to analyze network data is leading to increased collaboration with the network team in 83% of enterprises. The most successful collaborators are even more likely to cite this trend (89.5%). Large enterprises (10,000 or more employees) were the least likely to affirm this trend, as were members of data center operations teams. Individuals from network engineering and information security teams were more likely to answer "yes."

Processes of sharing network data are important. Systems should be established to ensure the security team knows how acquire the data it needs as efficiently as possible. This means establishing mechanisms for sharing data and ensuring good communication.

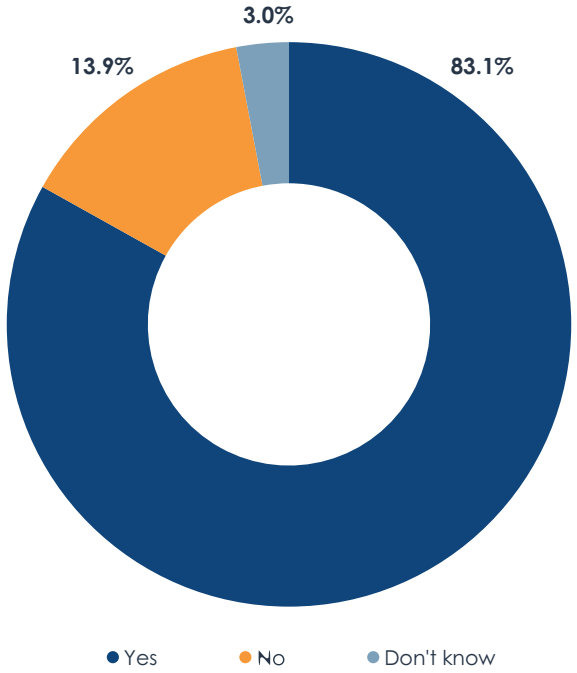


Figure 16. Does the security team's need to analyze network traffic data cause your organization's network team and security team to collaborate more?

Sample Size = 366

Figure 17 identifies how security teams use the traffic data they require. Network detection and response (NDR), or network traffic analysis (NTA), is the major priority. Most enterprises are also trying to support incident response and real-time packet payload analysis. Organizations that are the most successful with NetSecOps collaboration are more likely to focus on all three of these use cases. Members of information security teams are also more likely to prioritize these uses of traffic data.

Forensic packet analysis and compliance are lower priorities. The IT executive suite and the IT architecture group had the most interest in compliance. Information security, network engineering, and network operations teams were more likely to select forensic packet analysis.

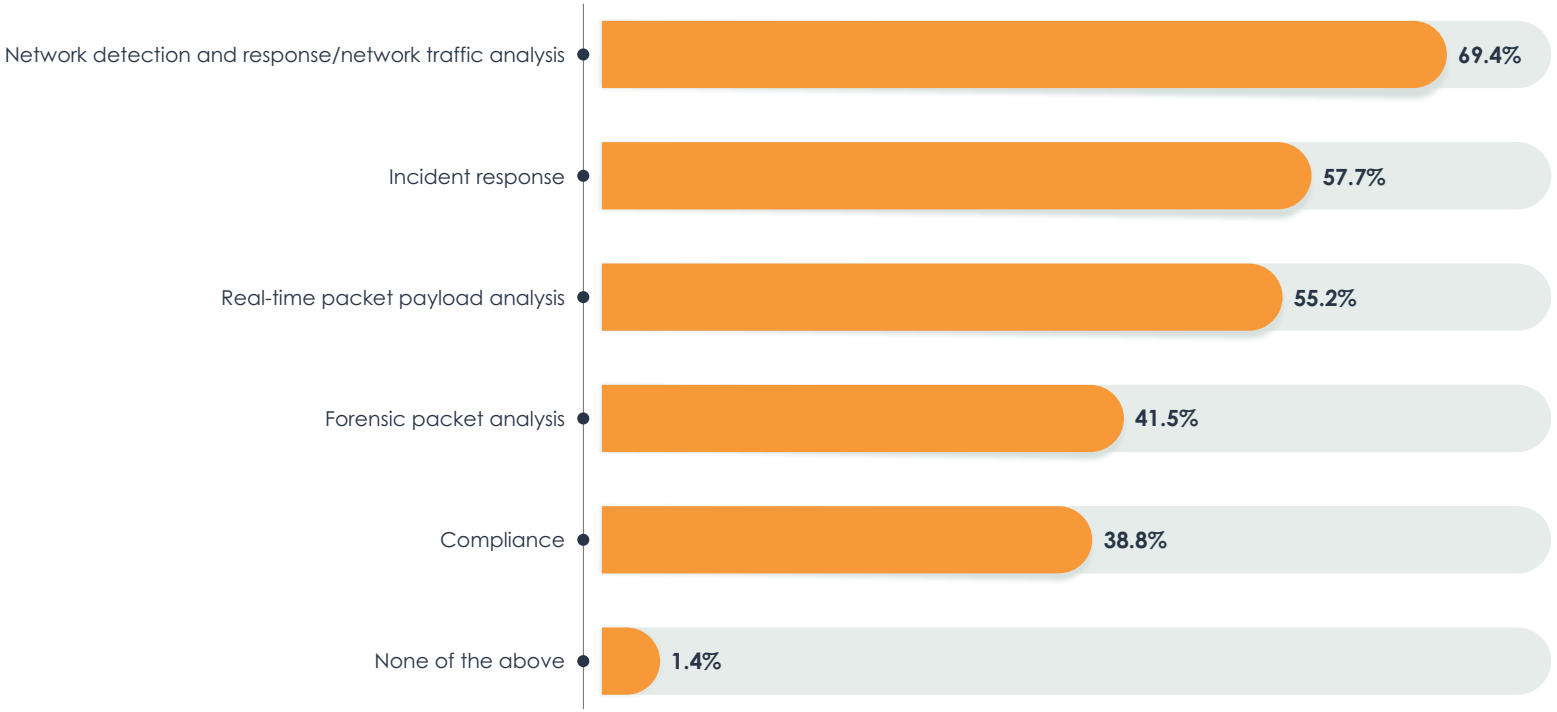


Figure 17. How security teams use the traffic data

Sample Size = 366, Valid Cases = 366, Total Mentions = 966

Packet Capture and Collaboration

Both network teams and security teams need to collect packet data for a variety of reasons, including forensic security analysis and performance troubleshooting. **Figure 18** reveals that packet capture requirements between these groups are aligned. The majorities of both groups are seeking continuous capture of all raw packets that cross the wire, although security teams are slightly more likely to set these requirements. Large minorities of both groups take an ad hoc or on-demand approach, capturing raw packets in response to an event. Very few of both groups restricted themselves to packet metadata collection, which provides only a shallow view of network activity.

Individuals in information security, network engineering, and the IT executive suite were more likely to identify continuous capture of all packets as a requirement for both teams. Members of network operations teams, who are less likely to troubleshoot complex issues, were less likely to identify continuous capture as a requirement for either team. Organizations that are the most successful with NetSecOps collaboration were the most likely to say the network team requires continuous packet capture.

Both groups are seeking continuous capture of all raw packets that cross the wire, although security teams are slightly more likely to set these requirements.

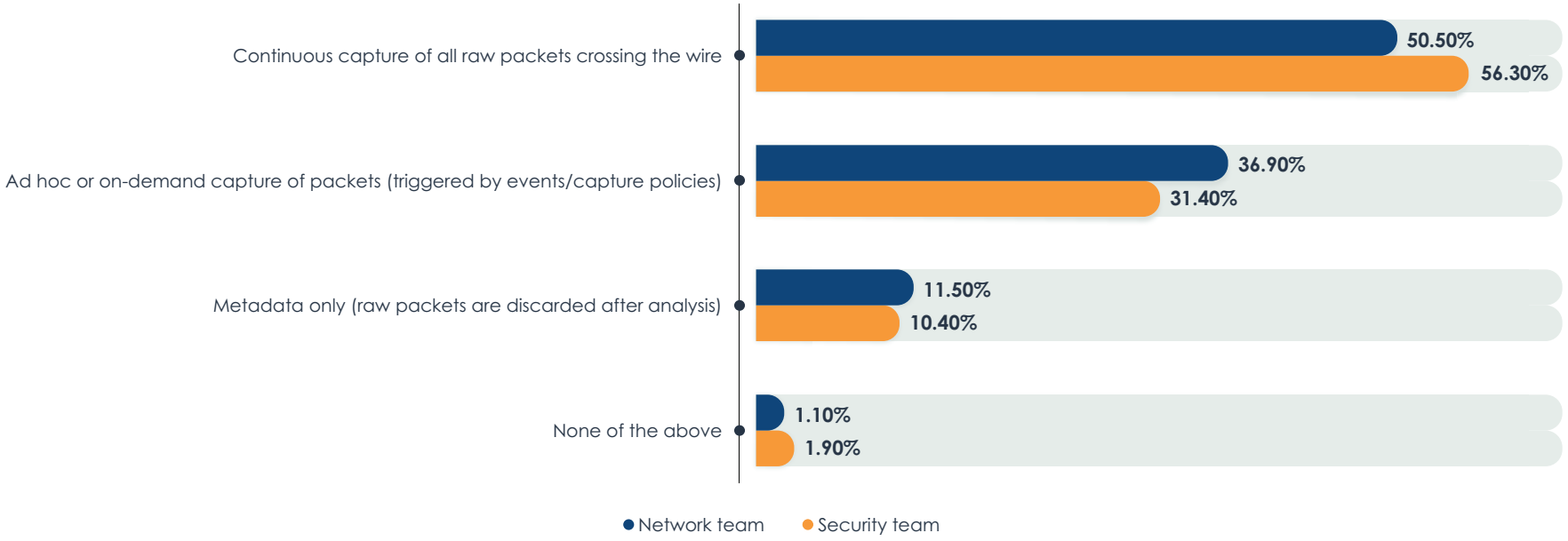


Figure 18. Network packet capture requirements

Given that conflicting data sets between network and security silos often challenge NetSecOps collaboration, EMA asked research participants whether their organizations are interested in consolidating packet capture infrastructure. **Figure 19** reveals that 97% are interested in consolidation; however, more than 40% are only willing to partially consolidate, possibly due to architectural complexity. For instance, some teams may have analysis tools with integrated packet capture resources. In other cases, security or compliance policies may forbid data from certain parts of the network. Large companies (10,000 or more people), which tend to have more complexity, were less likely to pursue full consolidation.

Organizations that are the most successful with NetSecOps collaboration were the most likely to pursue full consolidation of packet capture infrastructure.

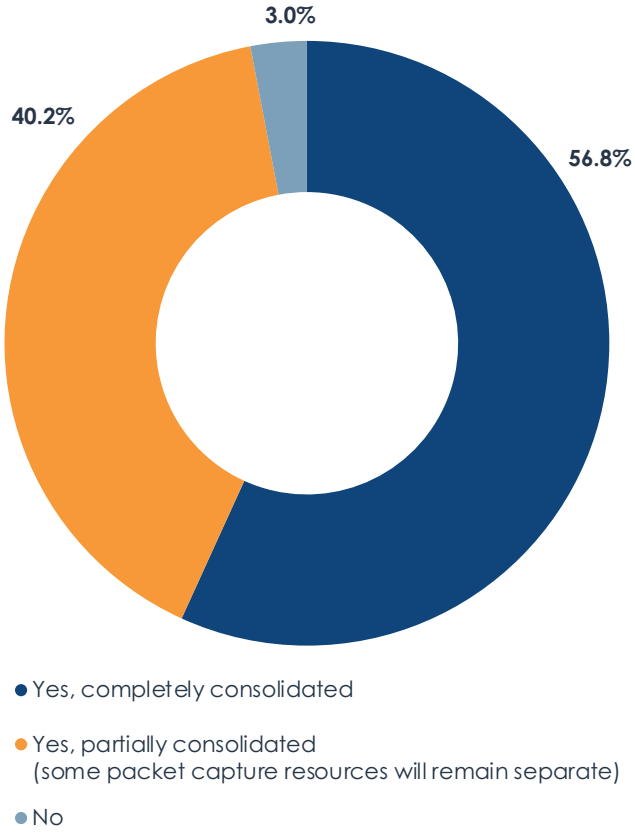


Figure 19. Are your organization's network team and security team interested in consolidating to a shared packet capture infrastructure?

Sample Size = 366

Figure 20 digs into the reasons why network and security teams are considering packet capture infrastructure consolidation. First, they see consolidation as a way to reduce security and compliance risk. Consolidation reduces the number of data stores that must be protected.

Many also believe consolidation will reduce data conflicts, expand overall visibility, and improve tool agility. Tool agility was a priority for smaller enterprises (1,000 to 2,499 employees). Americans prioritized expanded visibility and Europeans favored tool agility. Reduced packet storage costs was the least popular benefit, especially among the most successful collaborators, but it was a priority for members of network engineering teams.

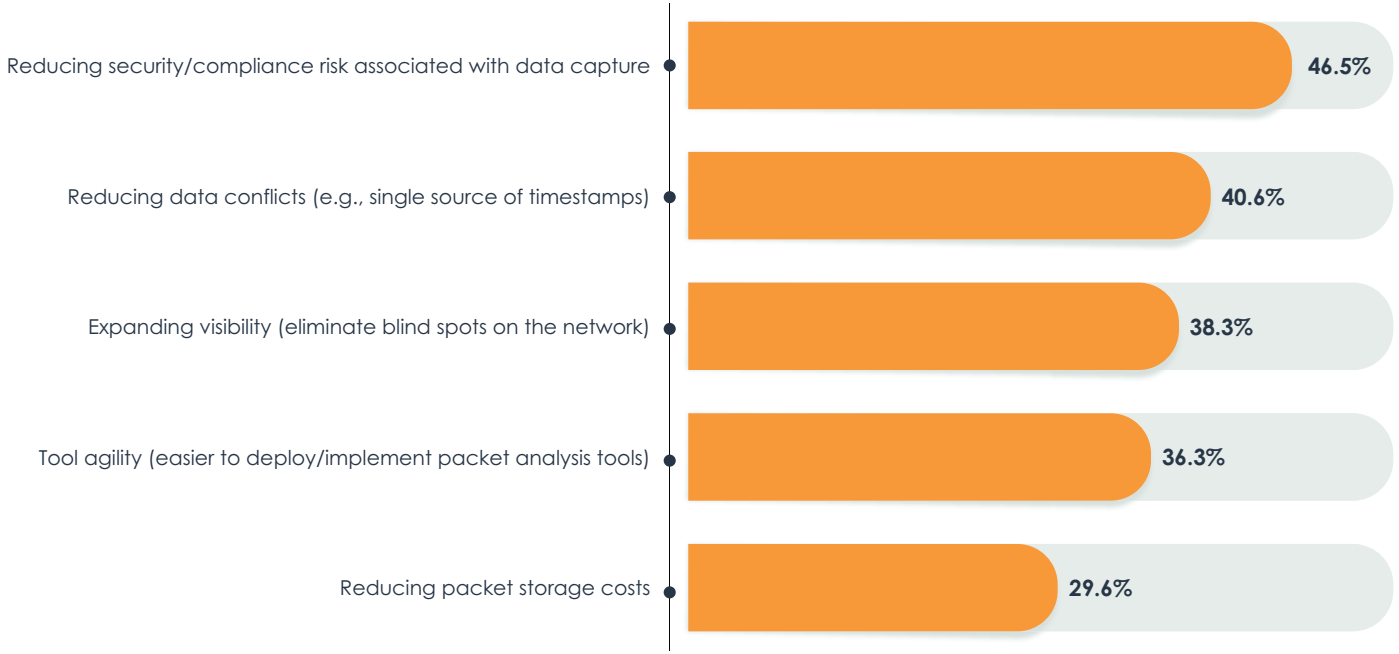


Figure 20. Potential benefits that drive interest in packet capture infrastructure consolidation

Sample Size = 355, Valid Cases = 355, Total Mentions = 679

Network Packet Brokers and Collaboration

More than 74% of research participants said that collaboration challenges sometimes interrupt the security team's access to network data, and 26% said this happens frequently. One way of preventing these interruptions is using network packet brokers (NPBs), appliances that aggregate, optimize, and distribute packet data to network analysis tools.

NPBs can improve how network teams and security teams work together. A network visibility fabric based on NPBs can simplify the process of sending optimized traffic data to each team's analytics tools. **Figure 21** reveals that 90% of survey participants believe that NPBs can facilitate NetSecOps collaboration, but only 43.8% say these solutions are very important.

90% of survey participants believe that NPBs can facilitate NetSecOps collaboration.

Best-in-class collaborators are the most likely to say NPBs are very important to supporting collaboration. IT executives tended to see the importance of these solutions more than people in middle management or technical specialists.

Network engineering teams often own and manage NPBs. The security team isn't always aware of the potential benefits of such solutions. For instance, virtual agentless NPBs can be deployed in multiple scenarios to support visibility and security for hybrid infrastructure. Enterprises can deploy them in virtualized data center infrastructure to deliver better visibility into east-west traffic flows. In the public cloud, they can provide access to cloud packet flows. Network teams are usually aware of these deployment scenarios, and good collaboration can ensure that the security team can take advantage of them.

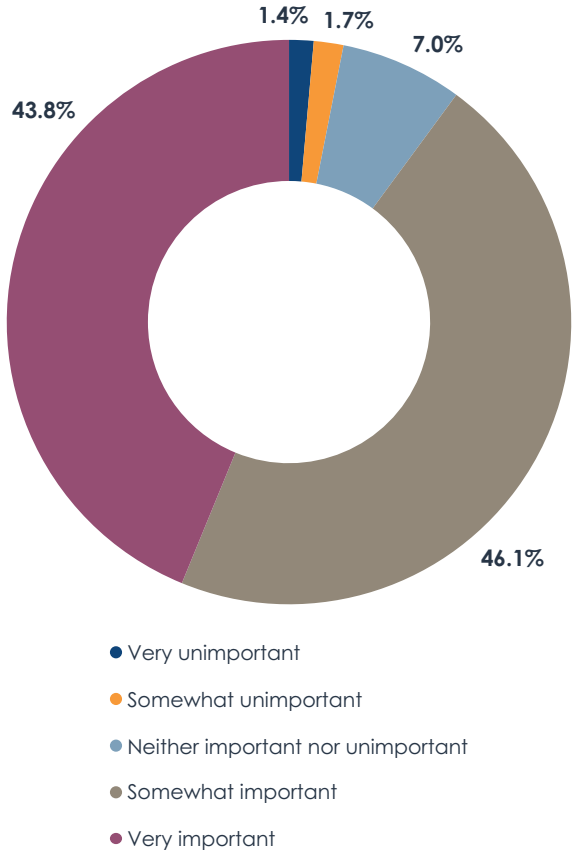


Figure 21. Importance of network packet brokers to facilitating collaboration between the network team and security team

Sample Size = 345

Figure 22 reveals strong interest in these use cases. More than half of research participants said they require virtual NPBs for both these environments. Only 6% said they have no need for this software. Enterprises that are the most successful with NetSecOps collaboration tend to require virtual NPBs for both virtual data centers and the public cloud. Less successful collaborators tend to choose just one or the other. Awareness of both use cases should be spread to the security group. Larger companies in this research tended to be less likely to require both use cases.

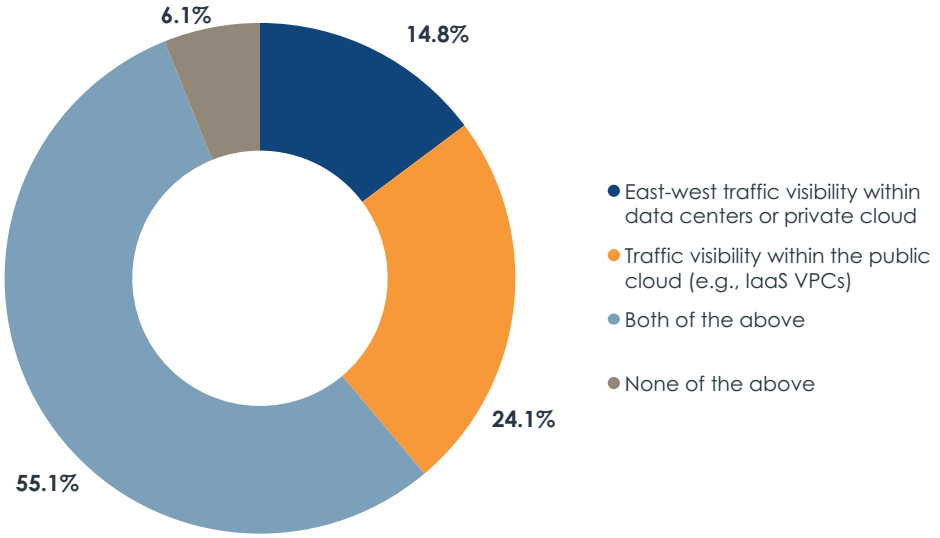


Figure 22. Requirements for agentless virtual network packet brokers for any of the following scenarios.

Sample Size = 345

Enabling Collaboration with Network Management and Analytics Tools

Each team in an organization has a set of tools that it uses to fulfill is duties. When teams collaborate, shared tools can be an enabler.

Siloed Traffic Monitoring Tools

Traffic monitoring is often siloed in organizations. Both network teams and security teams monitor traffic using different tools.

However, **Figure 23** reveals that 82.2% of network teams let security teams use their traffic monitoring tools. Members of network engineering teams and security teams were the most likely to report this tool sharing. Network operations teams, data center operations teams, and IT architecture teams were less likely. This tool sharing is also more common in organizations that are the most successful with NetSecOps collaboration.

"We are open to sharing our tools," said a director of network engineering and operations for a $7 billion healthcare enterprise. "We have some traffic monitoring and synthetic monitoring tools that [security] is sometimes interested in using to troubleshoot performance of their hardware. For instance, is the firewall introducing issues?"

Unfortunately, security teams aren't always adept at leveraging a network team's traffic monitoring tool, in part because these tools aren't designed to support the requirements of a security team.

82.2% of network teams let security teams use their traffic monitoring tools.

"It depends," said a network architect with a $100 billion bank. "Generally, when you are buying a solution, you aren't thinking about the other team's needs. My criteria is to select a tool that is network-centric, focused on my needs. It's very difficult to have a tool that serves different needs. There are some tools that can offer it, but most of the tools have a particular focus in one direction or another."

"I see the possibility," said a network engineer who has worked recently for two very large financial services companies. "We used an NPM tool that had some security insights in it. When the network engineering team was rolling that out, we engaged security because we saw that there was some value in the real-time alerts it offered. While the security team is most of the time off to themselves, the network team is still very security-centric. So, when a security concern or opportunity would come up, we would reach out and say, 'This is something you should use.'"

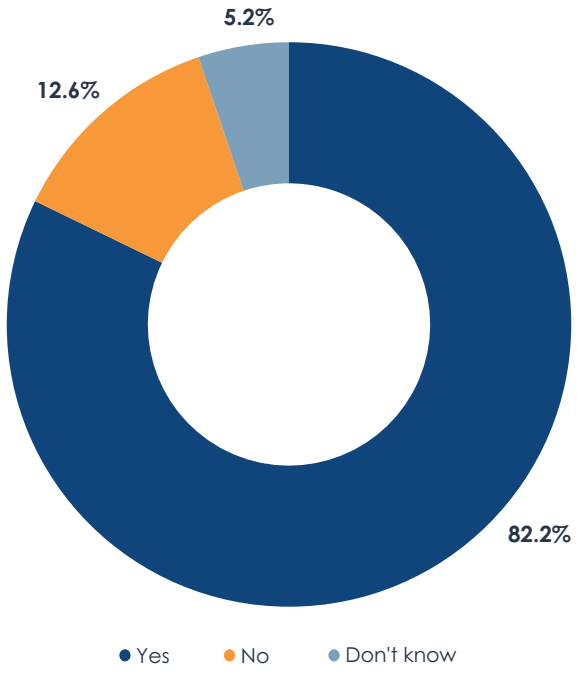


Figure 23. Does the network team ever let the security team use their traffic monitoring tool(s)?

Sample Size = 366

Figure 24 reveals that most organizations are interested in consolidating toolsets so that network and security teams have one traffic monitoring and analysis tool. Interest in this consolidation is higher among IT executives than middle managers and technical specialists. It is also more common among organizations that are the most successful with network and security team collaboration. Larger companies are the least interested.

"I think there is potential value [with consolidation]," said a director of network engineering and operations for a $7 billion healthcare enterprise. "A NOC and SOC share a lot of the same functions, so I can see them sharing a lot of the same tooling if it wasn't cost-prohibitive."

"I would have no problem with that. A lot of stuff has to be built to enable a tool. It makes no sense to build it twice," said a network architect with a $15 billion retail company.

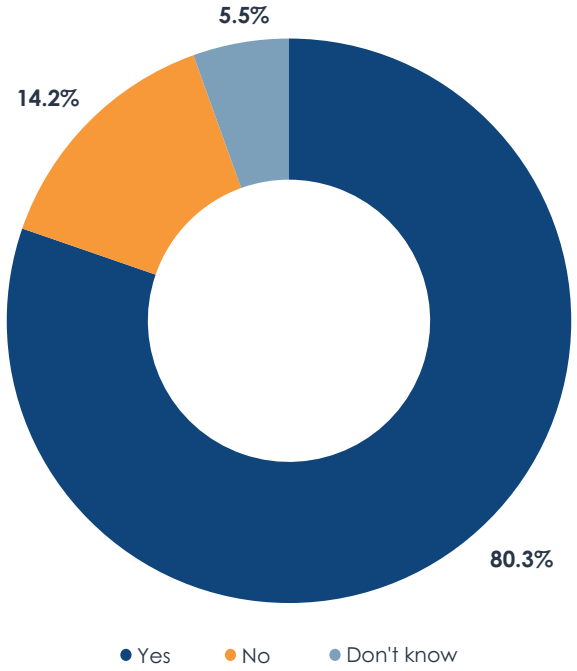


Figure 24. Is your organization interested in consolidating onto a single network traffic monitoring and analysis tool that serves both the network team and the security team?

Sample Size = 366

Figure 25 examines why network and security teams don't adopted a shared traffic monitoring tool. Overall, 89.3% of respondents identified at least one challenge. First, organizations cannot find solutions that meet the requirements of both teams. IT executives are less likely to see this as an issue, but individuals from network operations, network engineering, information security, and IT architecture teams are all more likely to cite this problem. While many network performance management solutions have introduced security operations capabilities, both the network and security silos recognize that some of these solutions aren't quite ready to displace security tools. This barrier is less likely to be a factor for organizations that reported the most success with NetSecOps collaboration, suggesting they've found a better way to define requirements for a shared tool.

The other chief barriers are less technical. The chief secondary issues include a lack of clarity about the benefits of sharing a tool and the individual teams arguing over how to share budgets for such a tool. IT executives and members of the network engineering team are more likely to cite unclear business benefits, but security teams and network operations teams consider this a minor issue. IT executives are less likely to see budget sharing as an issue, but members of network engineering, network operations, and information security teams all see it as a leading issue.

Finally, teams are butting heads over who should own and administer a shared tool. Many are also dealing with skills gaps that make a shared tool unlikely. Members of the network engineering team especially see conflicts over tool ownership as a problem. North Americans were the most likely to see skills gaps as a problem.

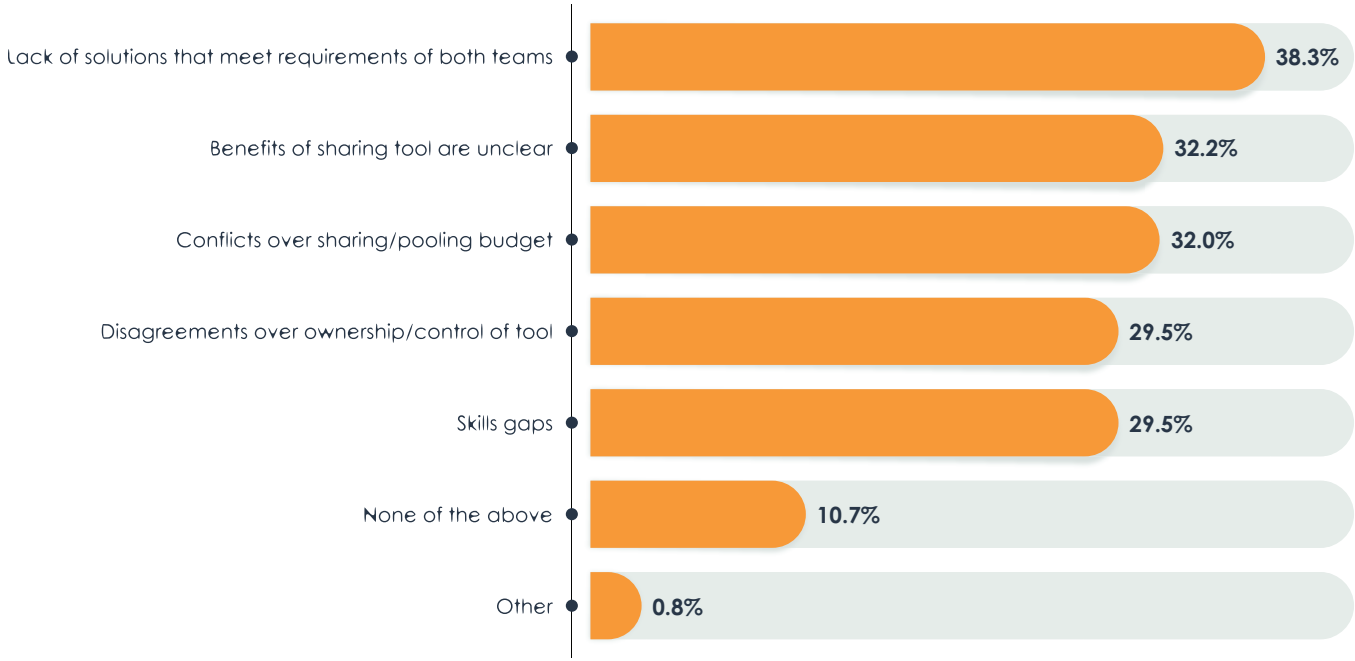


Figure 25. Barriers to the network team and security team adopting a shared tool for network traffic monitoring and analysis

Sample Size = 366, Valid Cases = 366, Total Mentions = 633

DNS, DHCP, and IP Address Management

DNS, DHCP, and IP address management (DDI) management tools are essential for NetSecOps collaboration. Network teams rely on DDI management tools to build resiliency in core infrastructure and to drive operational efficiency. Security teams are increasingly aware that DDI infrastructure is a potential vector for attack. They also recognize that the DDI data can help with investigations into security issues.

"I think the security team is interested in [DDI tools] because they allow you to really dig in and figure out where stuff is in your infrastructure a lot faster," said a director of network engineering and operations for a $7 billion healthcare enterprise.

"I think the security team is interested in [DDI tools] because they allow you to really dig in and figure out where stuff is in your infrastructure a lot faster," said a director of network engineering and operations for a $7 billion healthcare enterprise. "Now, as we look at DNS being an indicator of security, DDI tools have become more important as you adopt a plethora of services and try to remain flexible and scalable. DNS and DHCP are foundational services."

Unfortunately, not every security team understands the value of DDI tools and the data they contain. "[Security doesn't] seem to care about [DDI]," said a network architect with a $15 billion retail company. "But they do come back to us and say, 'What is this subnet?' Having access to IPAM would save them a lot of time. There is no reason why they couldn't access it."

Figure 26 reveals that 75.4% of network teams share data from their DDI management tools with the security team. Organizations that are the most successful with NetSecOps collaboration are the most likely to report DDI data sharing. Members of the network engineering teams and information security teams were the most likely to be aware of this data sharing, while people in network operations, data center operations, and the IT executive suite were the least aware of this.

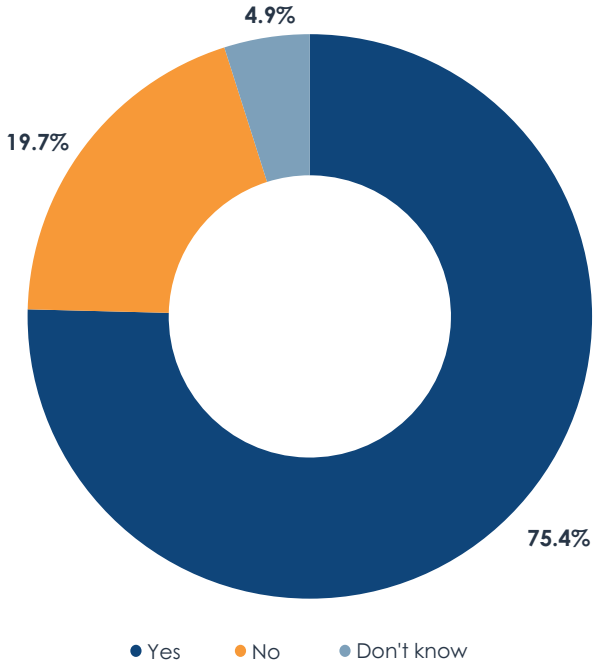


Figure 26. Does your network team share data from its DDI management tools with the security team?

Sample Size = 366

Figure 27 reveals that nearly all organizations have integrated or are planning to integrate DDI management tools with the security team's tools. This will allow the security team to pull data on demand, but it may also allow them to provision core network services on their own. Members of the network engineering and information security teams and people who work in IT executive suites were more likely to say this integration has already been done. Members of IT architecture, data center operations, and network operations were less likely to say this.

EMA also found that organizations that are the most successful with NetSecOps collaboration are more likely to have done this integration already.

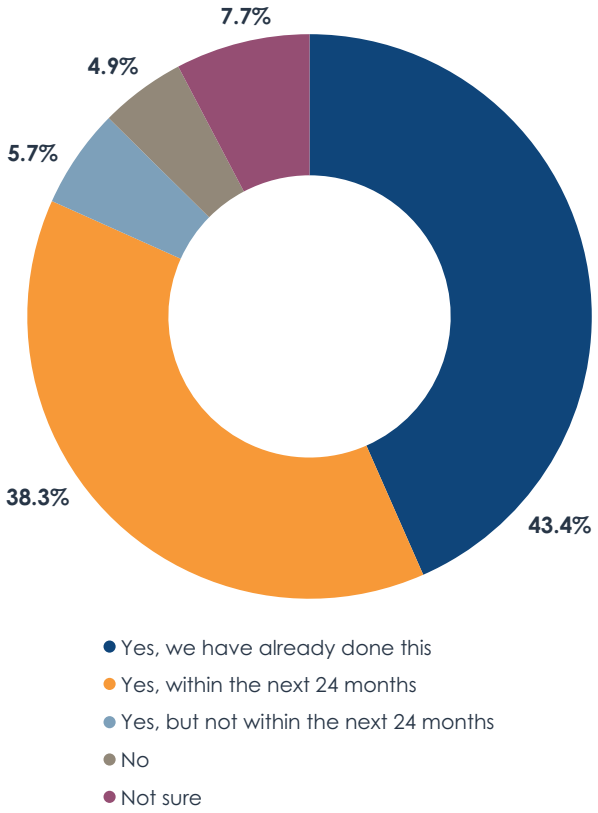


Figure 27. Is your network team planning to integrate its DDI management tools with the tools used by the security team?

Sample Size = 366

Figure 28 reveals that more than three-quarters of enterprises are implementing or planning to implement solutions specifically designed to address DNS security, such as a DNS firewall. IT executives and middle managers were more likely to report plans to adopt these solutions. Organizations that are the most successful with NetSecOps collaboration were also more likely to have plans to acquire a DNS security solution. Europeans showed more interested in this technology than North Americans.

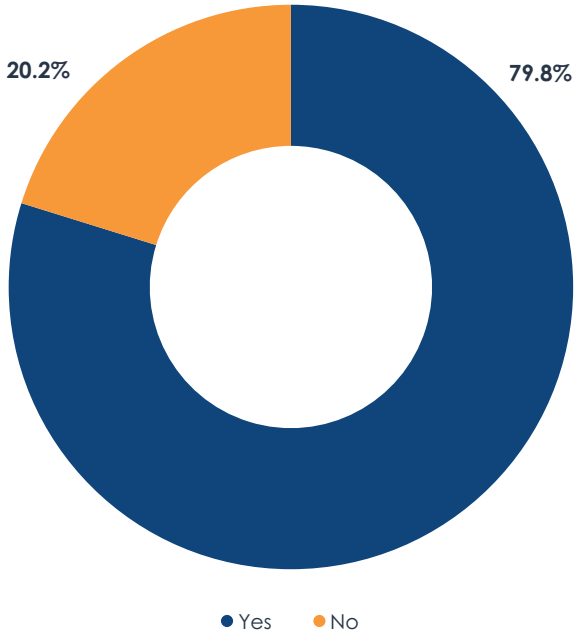


Figure 28. Is your organization using or implementing technology specifically to address DNS security?

Network Automation Tools

Network automation tools can streamline processes like change management, service orchestration, and security audits. Thus, these tools can be important to NetSecOps collaboration. **Figure 29** confirms this. More than 90% believe automation tools are important to this collaboration, with 44.8% saying they are very important.

"Automation gives us consistent configurations, consistent controls, and easy rollouts of changes," said a director of network engineering and operations for a $7 billion healthcare enterprise. "It also allows us, from a data collection standpoint, to get better insight into what's going on in the network. That consistency reduces risk."

"It would be easier to issue reports and inventories and to make changes that meet the security team's requirements with automation," said a network architect with a $15 billion retail company. "It would be easier to supply sample scripts to them to review."

IT executives and middle managers are more likely to rate automation as very important. Technical specialists are less convinced. The most successful collaborators are also most likely to identify automation as very important.

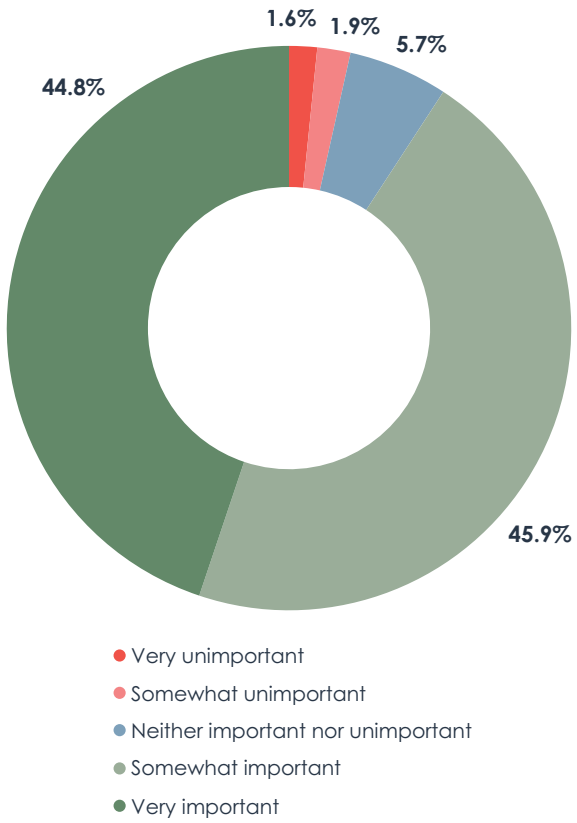


Figure 29. The importance of automation tools to facilitating collaboration between the network team and security team

Sample Size = 366

Figure 30 identifies the types of automation tools that organizations believe best support collaboration. Network change and configuration management and security policy automation tools are the most valuable. The IT executive suite was especially likely to select security policy automation tools, while network engineering teams were less likely. Successful collaborators also tended to favor this class of tools.

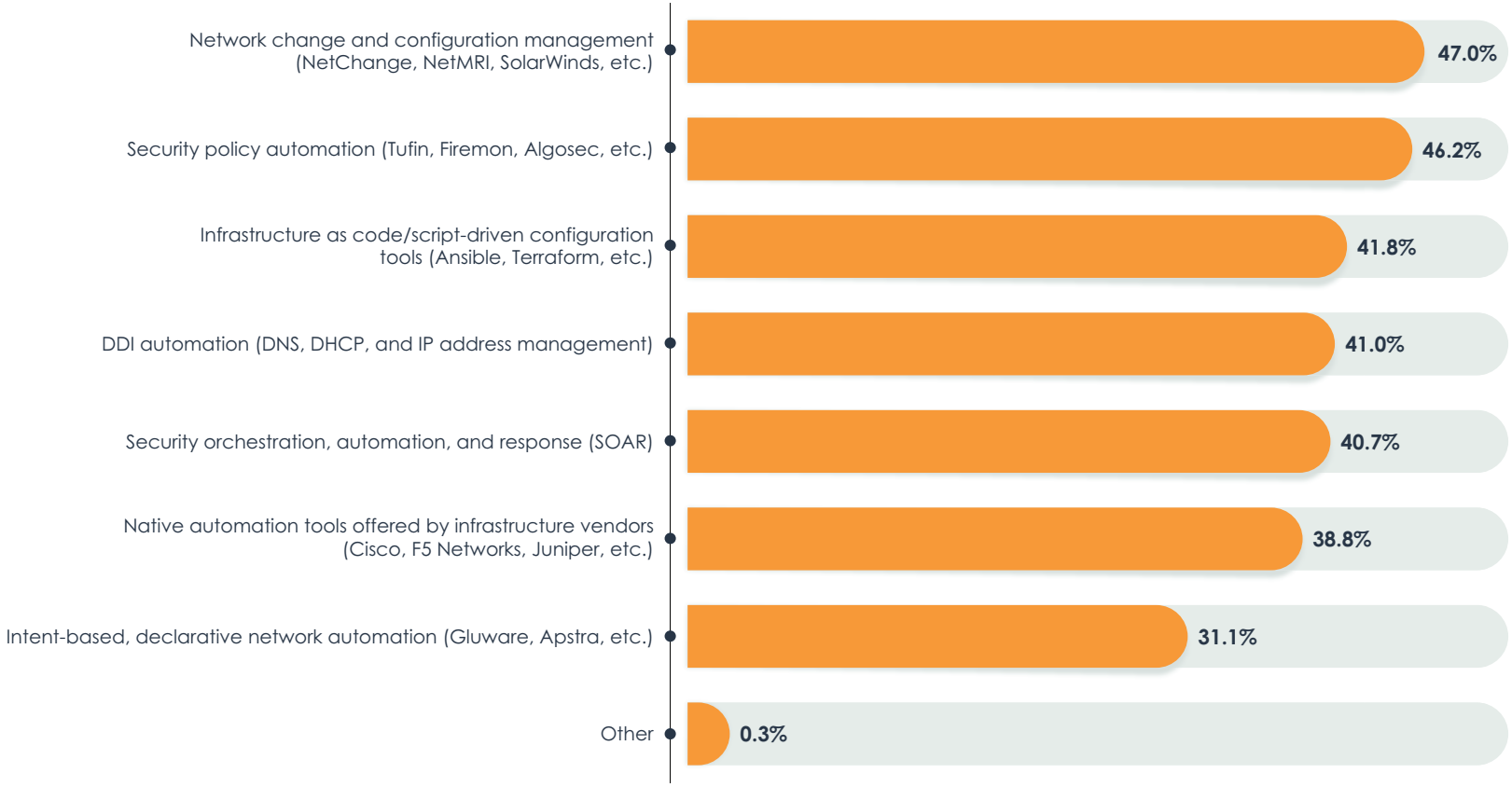


Figure 30. Automation technologies that are useful for facilitating collaboration between network teams and security teams

Sample Size = 366, Valid Cases = 366, Total Mentions = 1,050

Secondary automation targets were incident response or troubleshooting and infrastructure lifecycle management. Members of the security team were very interested in automating incident response. The lowest priorities for automation were network design and policy management. North Americans were a little more likely than Europeans to select policy management.

As enterprises embrace hybrid multi-cloud and DevOps operating models, automation can be an enabler. DevOps and cloud teams want more agility and control over their application environments. A self-service model for network and security infrastructure and services can provide them that agility and control. **Figure 31** reveals that three-quarters of organizations are facilitating self-service orchestration of networking and security resources with automation.

Respondents in information security, network engineering, and the IT executive suite were the most likely to be pursuing this, while people in IT architecture, network operations, and data center operations were laggards. Very successful NetSecOps collaborators were the most likely to adopt self-service models.

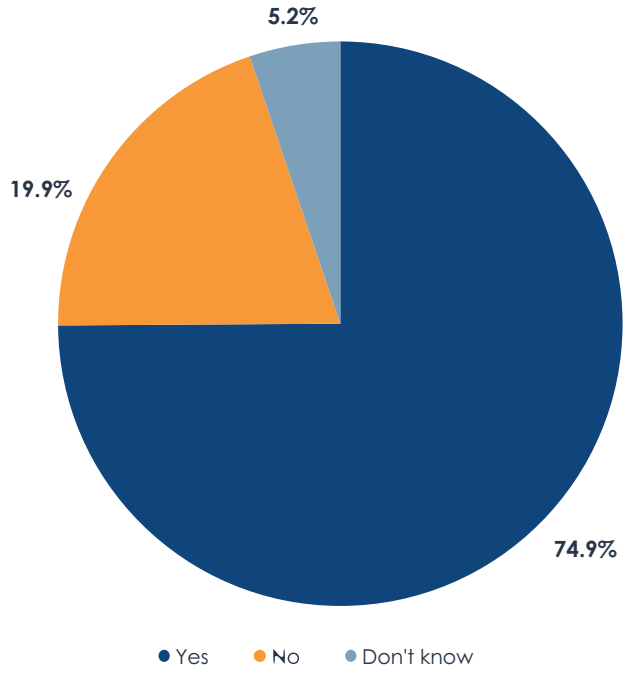


Figure 31. Is your organization adopting automation solutions to facilitate self-service orchestration of networking and security resources for production application teams?

Sample Size = 366

Figure 32 reveals which resources network and security teams are trying to provide via self-service models. Application security policies and DNS management and security are the biggest priorities. Layer 4-7 network services and application observability are secondary priorities. IP address management and switching and routing policies were the lowest priorities.

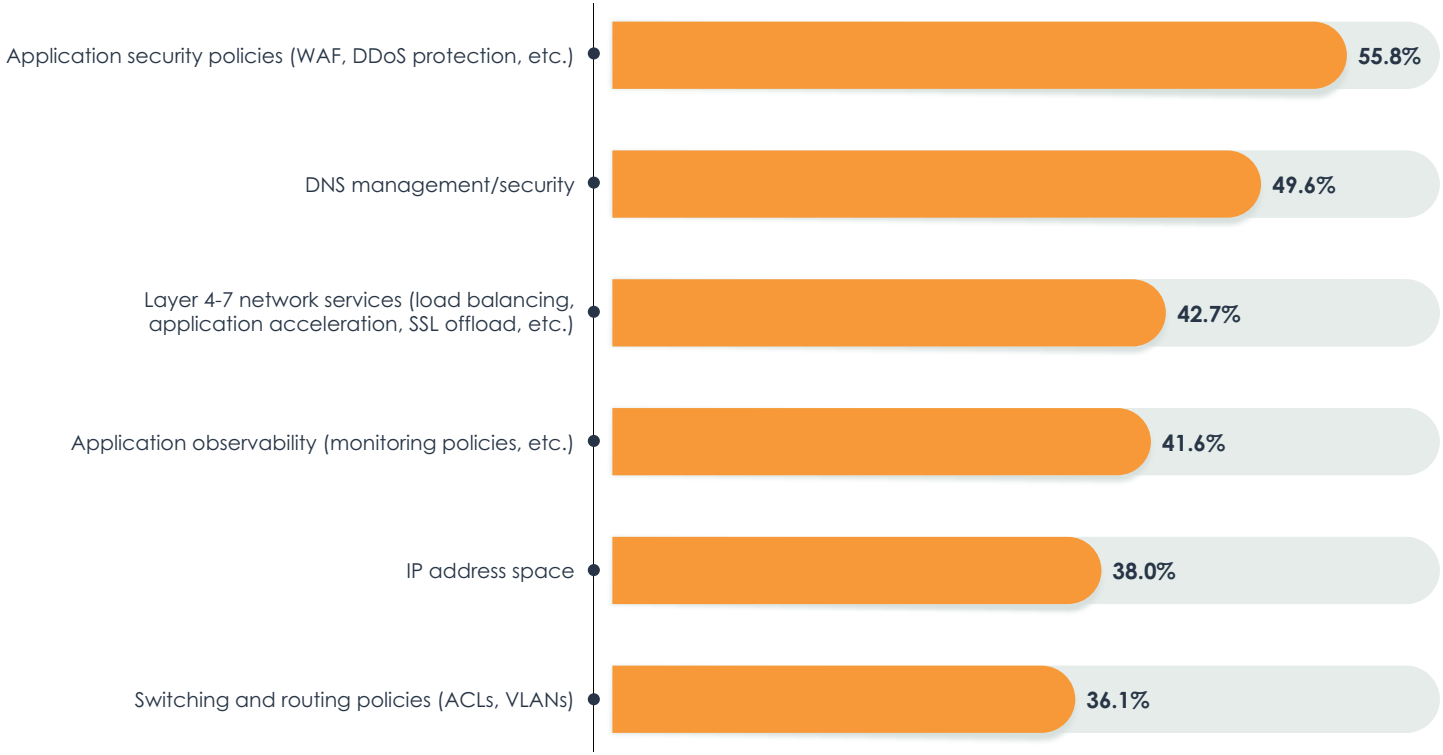


Figure 32. Capabilities that organizations are automating to present as self-service resources for application teams

Sample Size = 274, Valid Cases = 274, Total Mentions = 723

Conclusion

This research has confirmed that network and security teams are ramping up collaboration to enable and secure new digital architectures, like hybrid multi-cloud, work-from-anywhere, and IoT. NetSecOps collaboration isn't easy. CIOs and CISOs must make it happen. They have good people working below them, but those people often work within silos with structures that inhibit collaboration.

EMA can confirm through this research that collaboration is more effective when CIOs and CISOs lead from the top and prioritize partnerships within their organizations. Data is the starting point for collaboration. Network teams must ensure that the quality of their data is exemplary, and they must ensure that the security team can access network data when they need it.

The network management toolset is also a major enabler of collaboration, from infrastructure monitoring tools that can confirm that the security team's network hardware is up and running to traffic analysis tools that can provide both performance and security insights. Network and security teams are interested in sharing traffic monitoring tools, but EMA suspects that it will take time for this to happen. Both groups have trusted tool vendors that they will be reluctant to set aside. DDI tools, network automation, and AIOps also offer tremendous value in NetSecOps partnerships.

Network and security teams aren't natural partners. Their core missions are fundamentally opposed. Still, network teams recognize the importance of building security into everything they do, and they know that the security team has deep expertise that can help. With the right leadership, these partnerships can flourish.

NetOps & SecOps Improve Collaboration With NETSCOUT

Risk

Becoming more proactive by reducing security risks and vulnerabilities throughout their global network was a primary goal for a service company's IT team. The NetOps and SecOps teams targeted three specific areas: maintaining updated secure socket layer (SSL)/transport layer security (TLS) certificates, removing weak ciphers, and identifying/remediating exploitive protocols potentially used to introduce malware attacks to their environment. Due to several recent acquisitions, ensuring compliance with IT requirements required visibility to support both NetOps and SecOps responsibilities.

Analysis & Identification

NetOps and SecOps teams enhanced their collaboration by using a common network monitoring data source. The IT team selected NETSCOUT's real-time, packet-based service assurance solution, including InfiniStreamNG (ISNG) and vSTREAM virtual instrumentation, for network and application monitoring. nGeniusONE Service Assurance solution uses this smart data for smarter analytics to help organizations protect availability and performance enterprise-wide. Real-time, in-depth analytics, support for 1,000+ protocols and applications, alerting, troubleshooting, forensics, and packet decode capabilities provided a single source of truth for Net/SecOps to jointly leverage.

NetOps configured nGeniusONE and ISNG appliances to monitor for several security concerns.

Expiration Analysis of SSL Certificates - Proactive analysis of SSL certificates with nGeniusONE revealed the number of certificates in use, certificates that were approaching expiration, certificate versions, and identification of expired certificates. Analysis indicated that nearly half of the certificates monitored in one location were approaching expiration. In another location, the IT organization uncovered several expired certificates. SecOps was able to update the expired certificates and avoid expiration of others with nGeniusONE details.

TLS Cipher Suite Analysis - ISNGs were configured for SSL protocol monitoring. nGeniusONE analysis showed the different ciphers in use, some of which were older and weaker than the levels approved by the service company's IT organization (e.g., Au_RSA). Due to the company's several recent acquisitions, ensuring use of secure ciphers was a priority, and these details helped SecOps upgrade the weak ciphers to stronger ciphers, closing that gap to secure their environment quickly.

SMB v1 Vulnerability - The nGeniusONE solution was configured to identify and monitor the SMB v1 protocol, in reality hoping not to discover it running in the network at all. Otherwise, they were vulnerable to targeted malware attacks (e.g., WannaCry, NotPetya). SMB v1 was discovered scattered across a few locations. With IP addresses from nGeniusONE, NetOps and SecOps quickly disabled the app, making the corporate network much more secure.

Benefits

Given the importance of proactive management and minimizing security risks and vulnerabilities throughout their global network, the combined efforts of NetOps and SecOps using the nGeniusONE solution was critical. With members of both teams able to analyze the same network and application traffic details, communications were more informed, visibility was strong into potential security risks, and mean time to knowledge and resolution (MTTK/MTTR) were faster and helped IT achieve higher operational efficiencies. The service company also reaped the benefits of a more cost-effective approach to gaining packet-level visibility with a single source of truth from the NETSCOUT solution. The NetOps and SecOps teams will continue to protect the organization from avoidable vulnerabilities.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data 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 EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at **www.enterprisemanagement.com**. You can also follow EMA on **Twitter** or **LinkedIn**.

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 **www.enterprisemanagement.com**

4129.101821