IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Prepared for:

Zero Trust Networking: How Network Teams Support Cybersecurity

November 2024 EMA Research Summary Report

By **Shamus McGillicuddy**, VP of Research
Network Infrastructure and Operations

Table of Contents

Executive Summary

This summary report of market research examines how network infrastructure teams support enterprise zero trust security initiatives. Based on a survey of 270 IT and security professionals who are currently engaged with zero trust efforts, this report explores the zero trust partnerships that network teams form with cybersecurity groups as they work together to modernize secure remote access and network segmentation. It also reveals how network teams ensure that network performance and user experience are optimal in a zero trust architecture.

Introduction

Zero trust is a well-known cybersecurity paradigm that reflects the reality that defenses built around network perimeters are no longer viable. This is especially the case for the majority of enterprises that have built hybrid IT environments characterized by public cloud services, internet connectivity, hybrid work, and the consumerization of IT technology.

Zero trust involves the use of granular authentication and authorization policy controls that apply least-privilege access to networks and data. According to the National Institute of Standards and Technology (NIST), zero trust "assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location."[1] Zero trust also assumes a state of compromise on the network, and it emphasizes a reduction in potential lateral movement by malicious actors. Organizations seek to minimize lateral movement through granular network segmentation.

Naturally, a cybersecurity group typically spearheads zero trust security inside an organization, but network technology (including network segmentation and secure remote access solutions) are foundational components of a zero trust implementation. Enterprise Management Associates (EMA) believes network infrastructure teams are key enablers of a zero trust strategy. In fact, EMA research found this year that 30% of enterprises cited zero trust security as a major driver of their overall approach to network operations. The network team increasingly sees zero trust security shaping how they build and manage their networks.

This research summary explores how network infrastructure and operations teams partner with cybersecurity teams to plan, implement, and manage a zero trust architecture. It explores that partnership and the tools and technologies that network teams leverage in that partnership, including modern secure remote access solutions, network segmentation technology, and network observability tools.

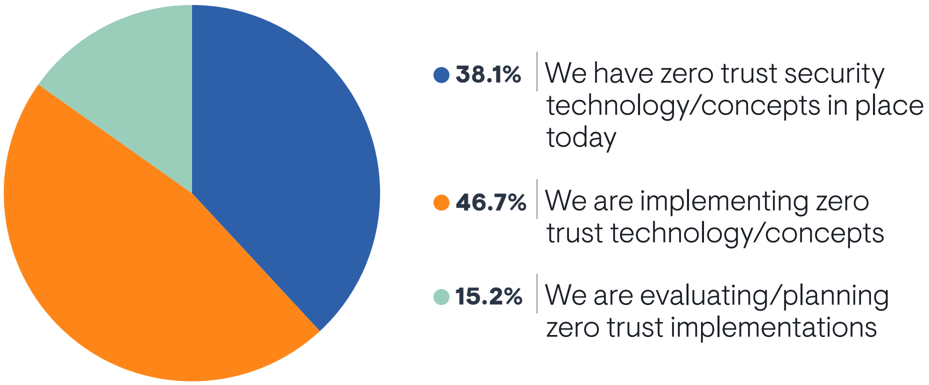
[1] https://csrc.nist.gov/pubs/sp/800/207/final

Methodology

EMA surveyed 270 IT professionals for this research project in September 2024. **Figure 1** reveals the demographic overview of these survey participants. EMA sought a mix of engineers, architects, middle managers, and executives in IT and security groups. Respondents worked for midsized to very large companies in a variety of industries and they were based in North America and Europe.

To qualify for participation in this research, respondents had to work in an organization that was engaged with zero trust security concepts. **Figure 2** reveals their answers to a qualifying question. More than 38% have implemented zero trust on their network, 47% are amid such an implementation, and the rest are evaluating and planning one. EMA rejected any potential respondents who indicated that their organizations were not currently engaged with zero trust in any way.

FIGURE 2. WHICH OF THE FOLLOWING BEST DESCRIBES YOUR COMPANY'S ENGAGEMENT WITH ZERO TRUST SECURITY?



Sample Size = 270

FIGURE 1. DEMOGRAPHICS OVERVIEW

Job titles

14.4%	IT/Network/Security engineers
3.7%	IT-related business analysts
6.7%	IT/Network/Security architects
12.2%	Project/Program managers
18.5%	IT/Security-related managers/supervisors
18.9%	IT/Security-related directors
8.5%	IT/Security-related vice presidents
17.0%	CIOs/CTOs/CISOs

IT groups

20.7%	IT executive suite
20.4%	Cybersecurity
18.9%	Cloud architecture/engineering
15.9%	Network/IT operations
10.4%	Network engineering
7.8%	IT architecture
5.9%	Security operations

Geography

68.1%	North America
31.9%	Europe

Company size (number of employees)

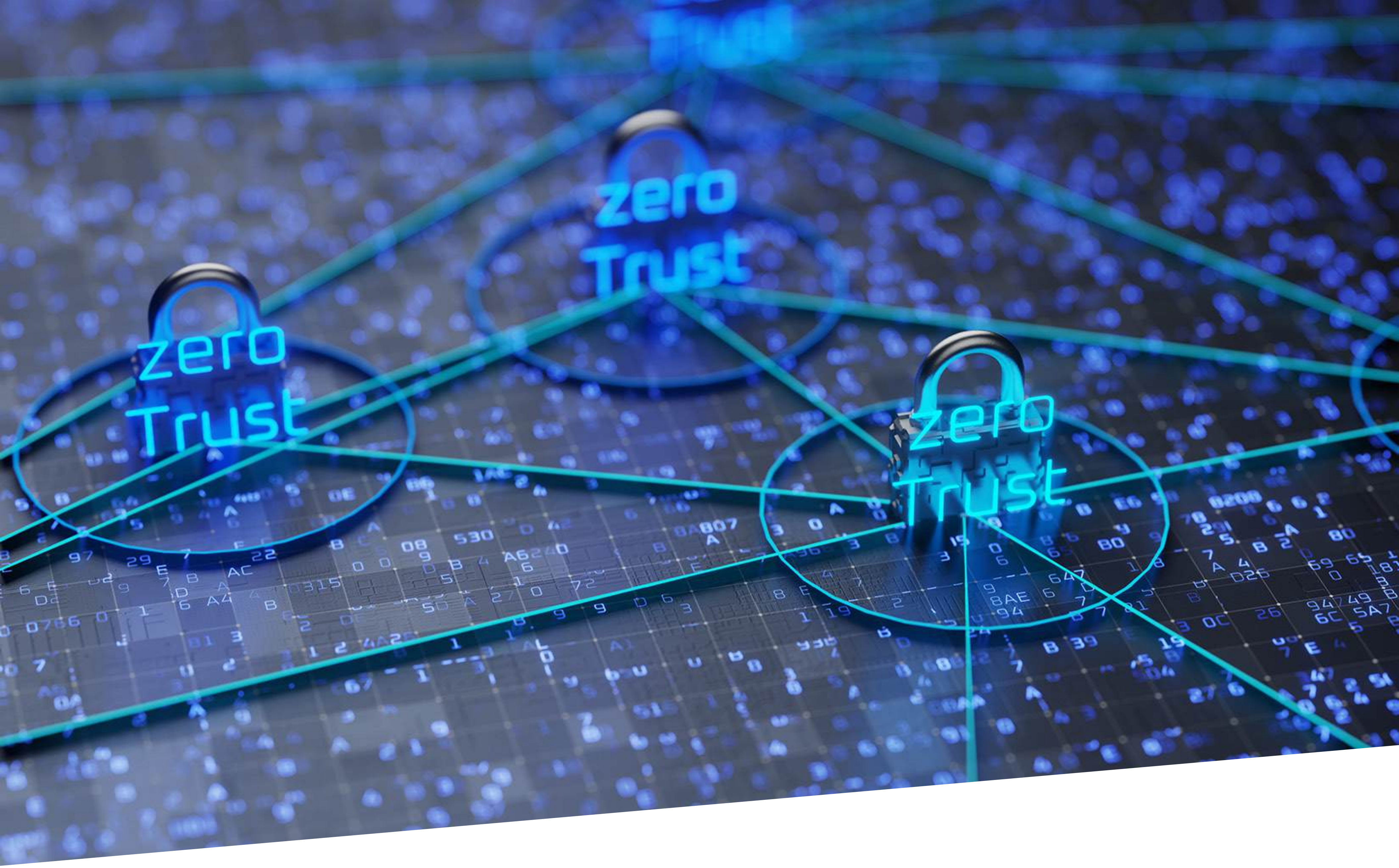
48.9%	Midsized enterprise (1,000 to 4,999)
35.1%	Large enterprise (5,000 to 19,999)
15.9%	Very large enterprise (20,000 or more)

Top industries

24.4%	Manufacturing
17.4%	Retail/Wholesale/Distribution
12.6%	Finance/Banking/Insurance
11.9%	Professional services
7.4%	Health care/Hospitals
5.9%	Construction
5.6%	Oil/Gas/Chemicals

Key Findings

- Only 35% of zero trust initiatives are completely successful
- Budget constraints and integration with existing infrastructure are top challenges
- In 44% of zero trust initiatives, the network infrastructure team is an equal partner to the cybersecurity group in leading the strategy
- Network performance and user experience are essential considerations in all aspects of zero trust – the network team are the experts here
- 96% of respondents believe network observability tools are important to zero trust success
- Most enterprises leverage DNS to optimize zero trust network segmentation and enhance threat detection
- 94% of organizations modernize their secure remote access technology for zero trust, and zero trust network access and secure access service edge are the most popular technologies for this modernization
- Public cloud and data center networks are the most popular targets for zero trust network segmentation
- Firewall appliances remain the most popular technology for implementing zero trust network segmentation



Foundations of Zero Trust Networking Strategy

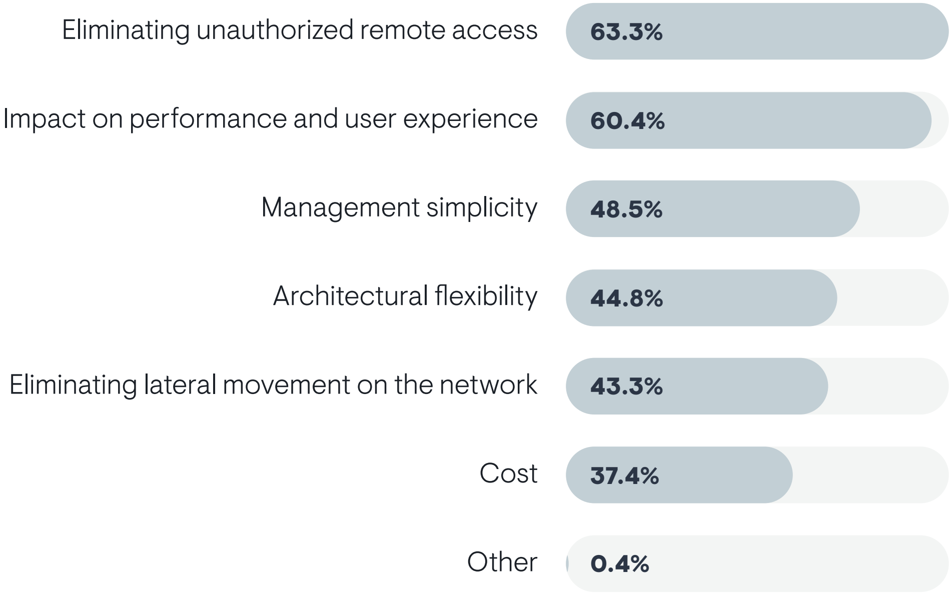
Essential Strategic Considerations

The twin pillars of strategic zero trust priorities point to the essentialness of the network team's participation. **Figure 3** shows that most enterprises are focused on eliminating unauthorized remote access with zero trust, but they are also very aware that they must avoid any impact on network performance and user experience as they execute on these efforts. Network performance has always been the north star for network engineering teams, and they are best equipped to know how zero trust architectures will impact it.

Less successful zero trust strategies correlated with a focus on eliminating unauthorized access, suggesting that enterprises should take a more expansive view of things. In fact, respondents with successful zero trust strategies made architectural flexibility a top priority.

Eliminating lateral movement on the network was a secondary priority, even though it is an essential pillar of zero trust concepts. However, lateral movement becomes more of a focus when a company has a hybrid cloud or multiple cloud providers. Impacts of performance and stopping unauthorized access are also bigger priorities for hybrid and multi-cloud enterprises. Cost is the lowest consideration for zero trust strategy, but enterprises that have not adopted public cloud services at all were more likely to select cost.

FIGURE 3. WHICH OF THE FOLLOWING FACTORS MOST INFLUENCE YOUR ORGANIZATION'S APPROACH TO EXECUTING ITS STRATEGY FOR ZERO TRUST SECURITY ON THE NETWORK?



Sample Size = 270

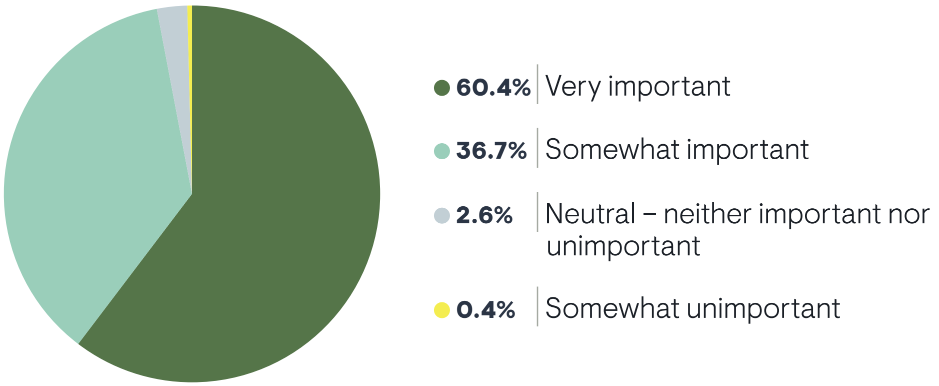
Network Performance and Zero Trust

Let's dive deeper into the consideration of network performance. We know it's a top consideration relative to other strategic factors, but how many consider it important overall? **Figure 4** reveals that 97% of IT professionals believe network performance is at least somewhat important to how they implement zero trust, with more than 60% saying it is very important. Respondents with completely successful zero trust strategies were even more likely (71%) to say network performance is very important.

97% of IT professionals believe network performance is at least somewhat important to how they implement zero trust.

Network performance was more essential to companies with hybrid cloud architecture and with multiple cloud providers. Respondents with a strong focus on network performance were also more likely to tell EMA that they have network observability tools that are effective at supporting their zero trust implementations. The research will explore this issue more in the following pages, but this correlation suggests that a focus on network performance leads to efforts to ensure that network tools can reveal how tools like secure remote access and network segmentation impact network experience.

FIGURE 4. WHEN IMPLEMENTING ZERO TRUST SECURITY ON YOUR NETWORK, HOW MUCH IS NETWORK PERFORMANCE A FACTOR IN HOW YOU PROCEED?

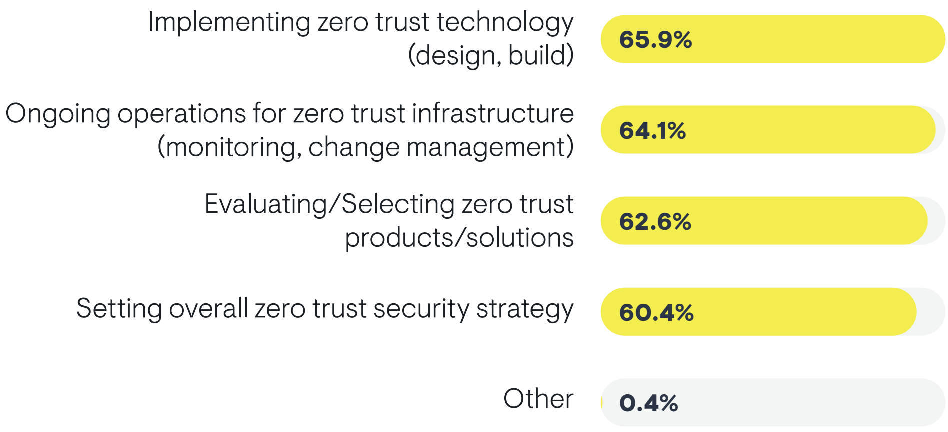


Sample Size = 270

The Network Team’s Role

Network teams clearly play a prominent role in any zero trust strategy. **Figure 5** reveals that the most common role is implementation of technology. They are often designing and building zero trust networks and installing and configuring secure remote access solutions and network segmentation tools.

FIGURE 5. WHAT ROLE DOES YOUR COMPANY'S NETWORK INFRASTRUCTURE/ ENGINEERING TEAM PLAY IN ZERO TRUST SECURITY STRATEGY?



Network teams are also usually responsible for ongoing operations of zero trust infrastructure and evaluating and selecting solutions. When the network team is involved in ongoing operations of zero trust infrastructure, a zero trust strategy is more likely to be successful. They are slightly less likely to be involved in setting overall strategy.

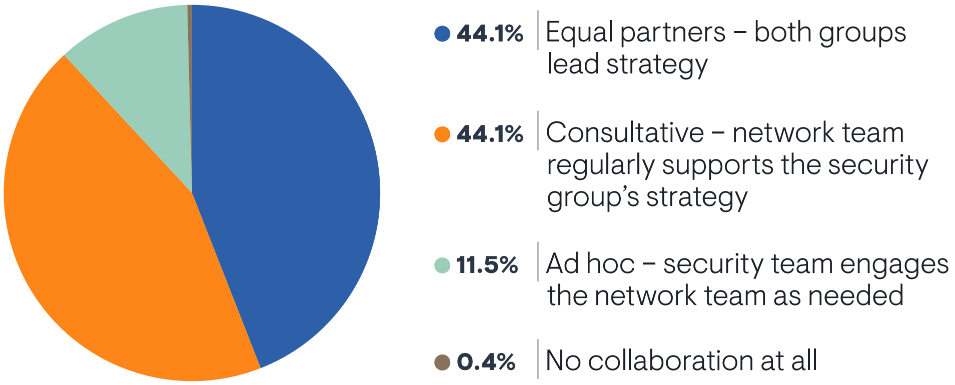
Network teams are more likely to be involved in all of these aspects of zero trust if an enterprise has a hybrid cloud architecture, suggesting that network teams get involved more in zero trust when IT is dealing with the complexity of a hybrid cloud environment.

Sample Size = 270

Partnerships with Cybersecurity

The cybersecurity team usually sets a zero trust agenda, but the previous chart makes clear the importance of the network team. **Figure 6** shows how these two groups work together. More than 44% of respondents told EMA that the cybersecurity team and the network team are equal partners who both lead zero trust strategy. Another 44% described the network team as a consultative partner who regularly supports cybersecurity's strategy. A smaller number told EMA that there is only ad hoc collaboration between the two groups.

FIGURE 6. TO WHAT EXTENT DOES YOUR COMPANY'S NETWORK TEAM AND CYBERSECURITY/IT SECURITY TEAM COLLABORATE ON ZERO TRUST SECURITY?



EMA found that network teams were more likely to be equal partners with the cybersecurity group if a company had a hybrid cloud architecture. Such partnerships were also more common if the network team had observability tools that were effective at supporting zero trust requirements.

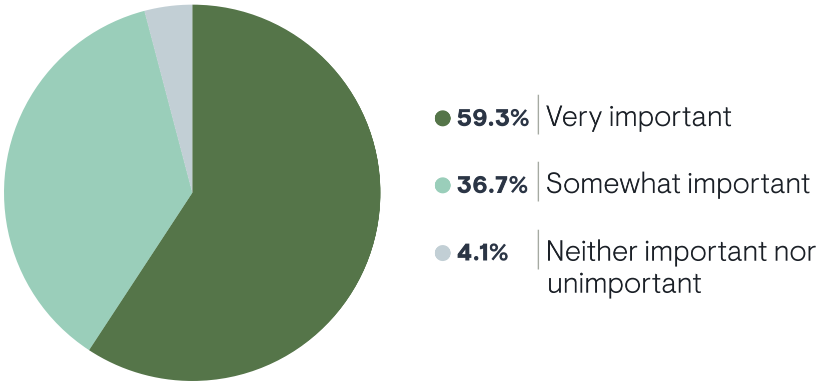
Sample Size = 270

Network Observability's Role

EMA believes that network observability tools are critical to a network team's ability to support zero trust strategies. Research respondents agree. **Figure 7** shows that 96% of respondents consider these tools to be important to zero trust enablement, with 59% saying they are very important. Midsized enterprises (1,000 to 4,999 employees) especially believe network observability is critical. Organizations with successful zero trust strategies were especially engaged with the importance of these tools.

The IT executive suite and network operations and security operations teams were most likely to call out network observability's importance. The network engineering team and IT architecture group were less enthused. The importance of network observability to zero trust increases as enterprises adopt more cloud providers.

FIGURE 7. HOW IMPORTANT ARE THE NETWORK TEAM'S NETWORK OBSERVABILITY/MONITORING TOOLS TO SUPPORTING A ZERO TRUST STRATEGY?



Sample Size = 270

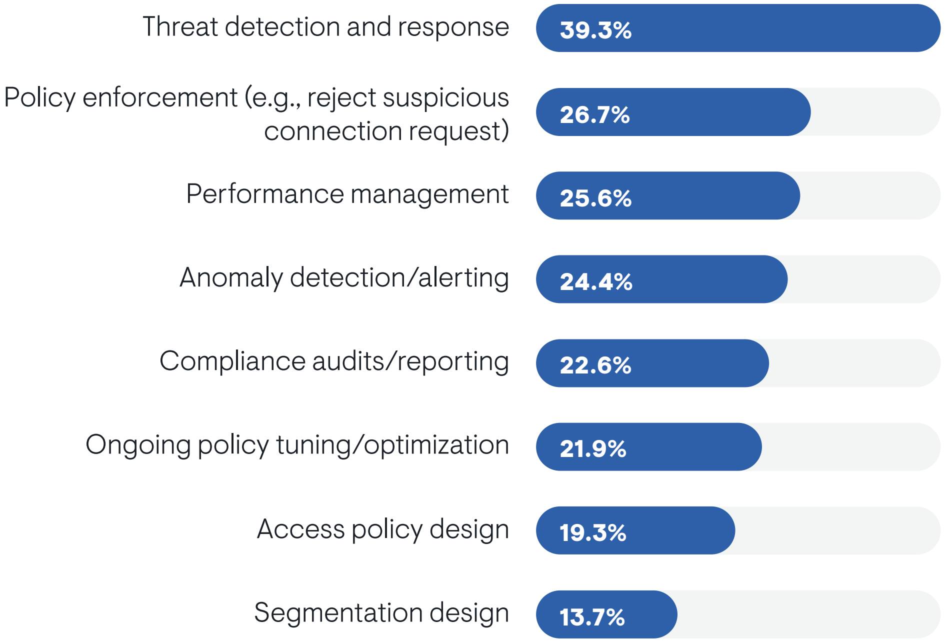
How Network Observability Helps Zero Trust Efforts

Figure 8 looks at how network observability best helps organizations with zero trust strategy. Ongoing monitoring with these tools is clearly critical to threat detection and response.

Policy enforcement, performance management, and anomaly detection are the top secondary opportunities. Policy enforcement is especially important to enterprises that are not using public cloud services.

Zero trust design is the lowest priority opportunity, both access policy design and segmentation design.

FIGURE 8. HOW DO NETWORK OBSERVABILITY/MONITORING TOOLS BEST SUPPORT YOUR ORGANIZATION'S ZERO TRUST STRATEGY?

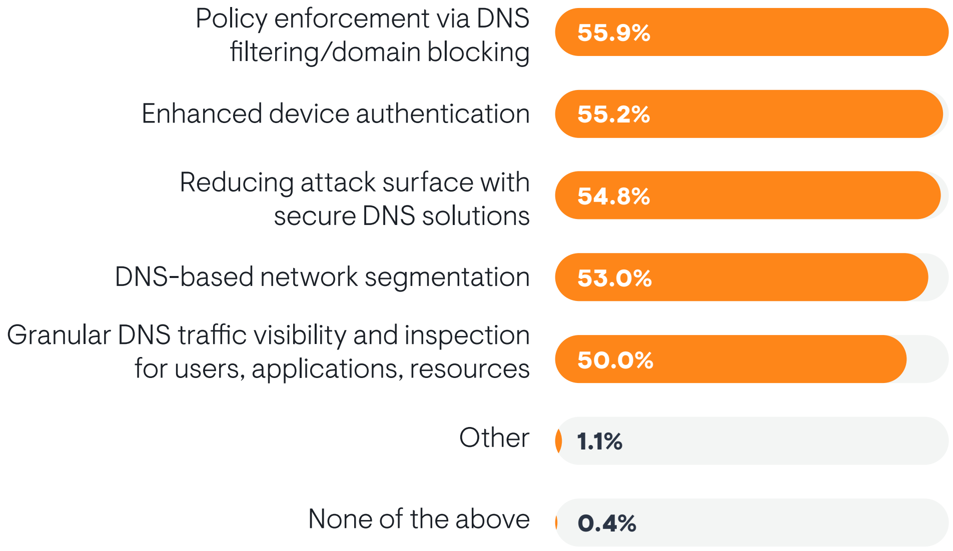


Sample Size = 270

The Role of DNS Tools and Technology

Network teams are traditionally the owners and operators of DNS infrastructure. Cloud migration fractured centralized ownership of DNS, with cloud and applications implementing their own DNS services without the network team's involvement. Still, network teams have the expertise and the enterprise-grade DNS solutions that can contribute to a zero trust security initiative. **Figure 9** reveals how IT pros believe DNS can support zero trust. Most see an opportunity to enforce policy via DNS filtering or domain blocking, and it is especially valuable to multi-cloud enterprises. Most respondents also see an opportunity to enhance device authentication and to reduce attack surfaces with secure DNS solutions.

FIGURE 9. WHAT ROLE DOES DNS PLAY IN YOUR ORGANIZATION'S ZERO TRUST STRATEGY?



Most also see the potential use of DNS as a network segmentation mechanism. However, this type of network segmentation was less popular among organizations with successful zero trust strategies.

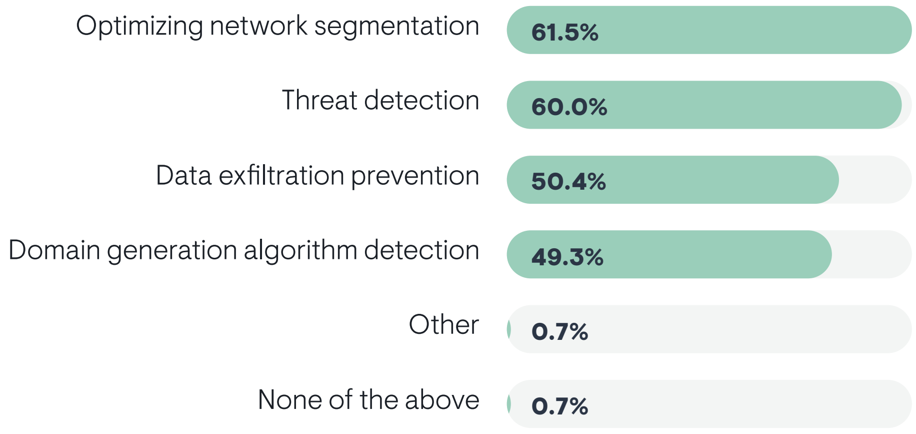
Sample Size = 270

Exactly half of respondents believe that DNS-based traffic visibility and inspection are valuable for zero trust. They were especially valuable to organizations that have hybrid cloud architecture and multi-cloud architecture.

The Value of DNS Monitoring

Figure 10 takes a deeper look at what organizations are seeking to do when they point their network observability solutions at DNS traffic in support of zero trust. Primarily, they are trying to optimize network segmentation and detect threats. Threat detection is especially important to operators of hybrid clouds and multi-cloud networks. Optimization of network segmentation is especially important to organizations that prioritize network performance when planning zero trust strategies, suggesting that DNS can help prevent network segmentation from impacting performance.

FIGURE 10. HOW MIGHT REAL-TIME ANALYSIS OF DNS TRAFFIC HELP SUPPORT YOUR ZERO TRUST SECURITY STRATEGY?



Secondarily, organizations are trying to prevent data exfiltration and detect domain generation algorithm activity.

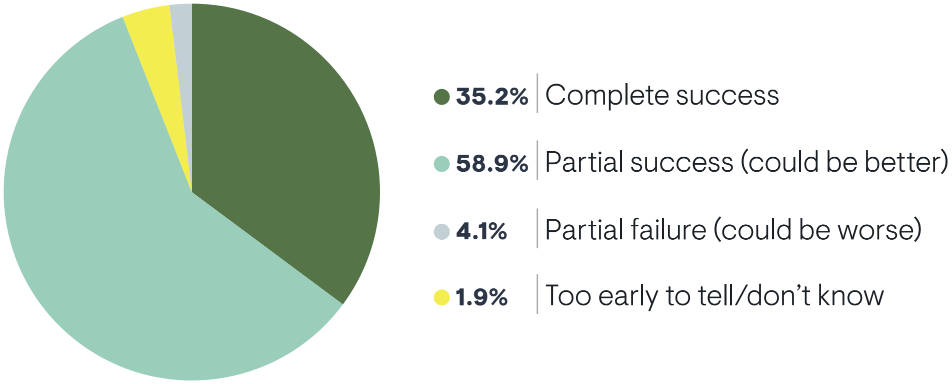
Sample Size = 270

Outcomes of Network Teams Aligning with Zero Trust

Zero Trust Success

Figure 11 reveals that only 35% of respondents believe they've been completely successful with zero trust so far. Nearly 59% see some room for improvement, 4% consider themselves failures, and only 2% say it's too early to tell.

FIGURE 11. TO WHAT EXTENT HAVE YOUR COMPANY'S EFFORTS TO IMPLEMENT A ZERO TRUST SECURITY STRATEGY BEEN SUCCESSFUL SO FAR?



Organizations that host their applications and data exclusively in data centers rather than the public cloud are experiencing the most success, suggesting that the cloud undermines zero trust efforts. On the other hand, organizations that use three or more cloud providers reported more success. EMA suspects that these organizations strive to reduce overall complexity by using third-party, end-to-end zero trust networking solutions rather than the native capabilities of individual providers. This may improve their overall outcomes when compared to other organizations that use the cloud.

Good support of zero trust by network observability correlated with success. Cybersecurity and security operations professionals were more pessimistic about success than network operations and IT architecture personnel.

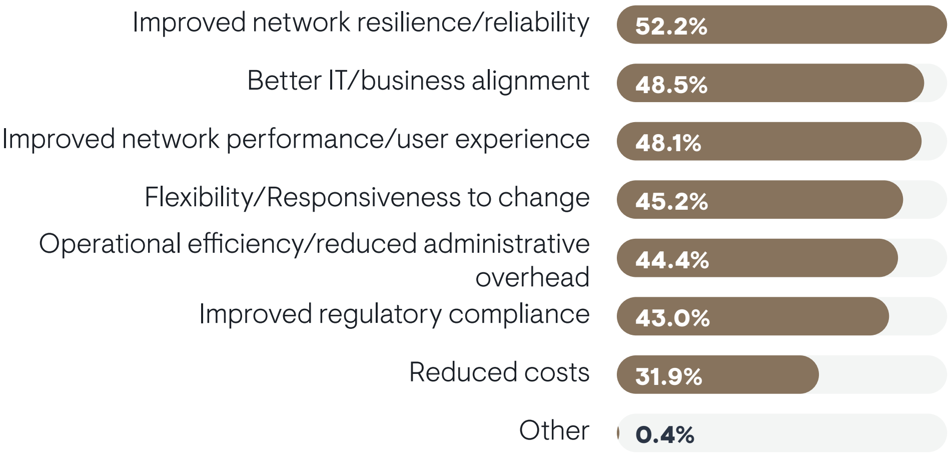
Sample Size = 270

Zero Trust Networking Benefits

Figure 12 Identifies how organizations benefit from a successful implementation of a zero trust network. EMA assumes that improved security is the ultimate benefit of these efforts, so we excluded it from consideration in this question. We asked respondents to identify the other benefits that follow it.

The top response was improved network resilience or reliability. Zero trust simply leads to less downtime. Operators of hybrid cloud architectures were more likely to cite this benefit. The IT executive suite perceived it more often than the cloud team.

FIGURE 12. ASIDE FROM IMPROVED SECURITY, WHAT OTHER BENEFITS DO YOU EXPECT YOUR ZERO TRUST SECURITY STRATEGY TO PROVIDE TO YOUR COMPANY?



Respondents also pointed to better alignment of IT with the business and improved network performance. The network engineering and network operations teams were most aware of improved IT and business alignment. Reduced cost is not a common benefit overall.

Operational efficiency is another secondary benefit, but organizations that experienced the most success with zero trust put it at the top of this list.

Sample Size = 270

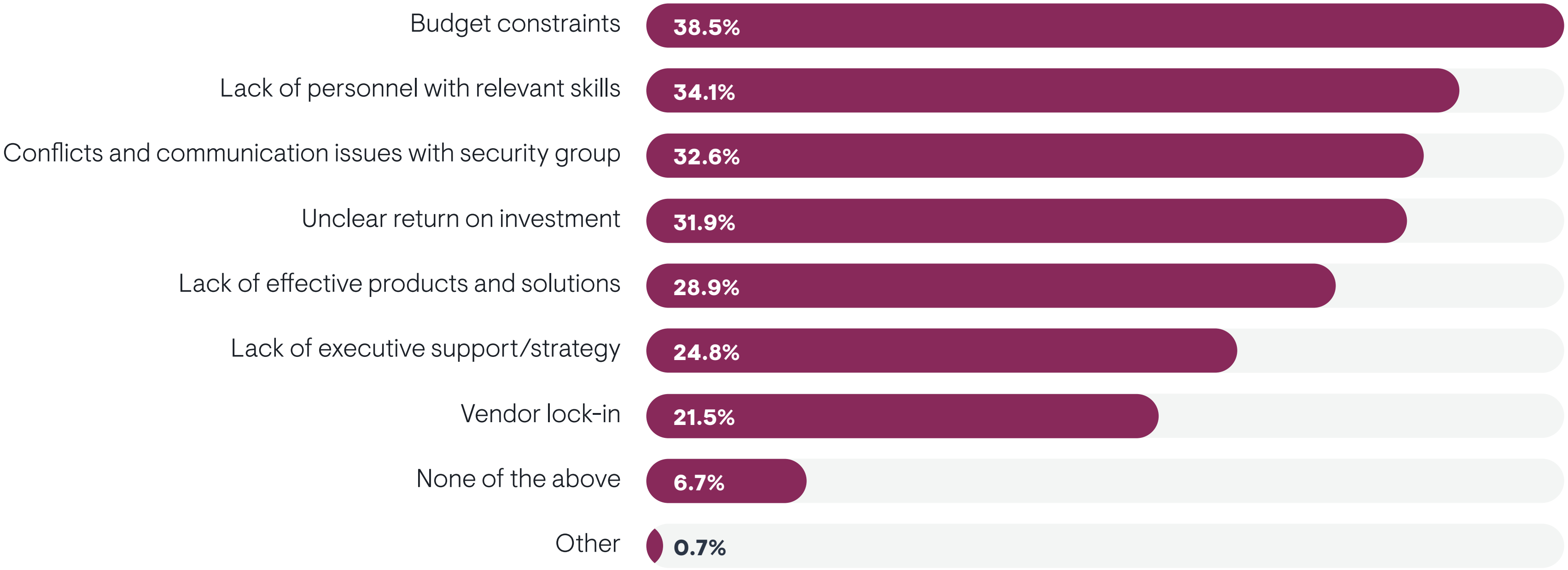
Zero Trust Sources of Pain

Figure 13 identifies the business challenges that undermine a network team's ability to support zero trust. The biggest challenge is budget. Organizations with less successful zero trust efforts were more likely to cite budget. It's also a bigger problem for Europeans than North Americans.

Many are also struggling with a lack of skilled personnel, conflicts and communication issues with security groups, and a lack of clarity on how zero trust delivers a return on investment (ROI). Like budget, unclear ROI was cited more often by less successful zero trust strategies. The network engineering team (who would know best about this issue) was more likely than the cloud team to cite conflicts with the security group as a major problem. These intergroup conflicts were also felt more often in large enterprises (2,500 to 10,000 employees).

A lack of effective solutions, a lack of executive support and strategy, and vendor lock-in were lesser issues. However, organizations that outright failed with zero trust were more likely to point to vendor lock-in and ineffective solutions.

FIGURE 13. WHICH OF THE FOLLOWING BUSINESS ISSUES ARE MOST CHALLENGING TO THE NETWORK TEAM'S EFFORTS TO SUPPORT YOUR ZERO TRUST STRATEGY?

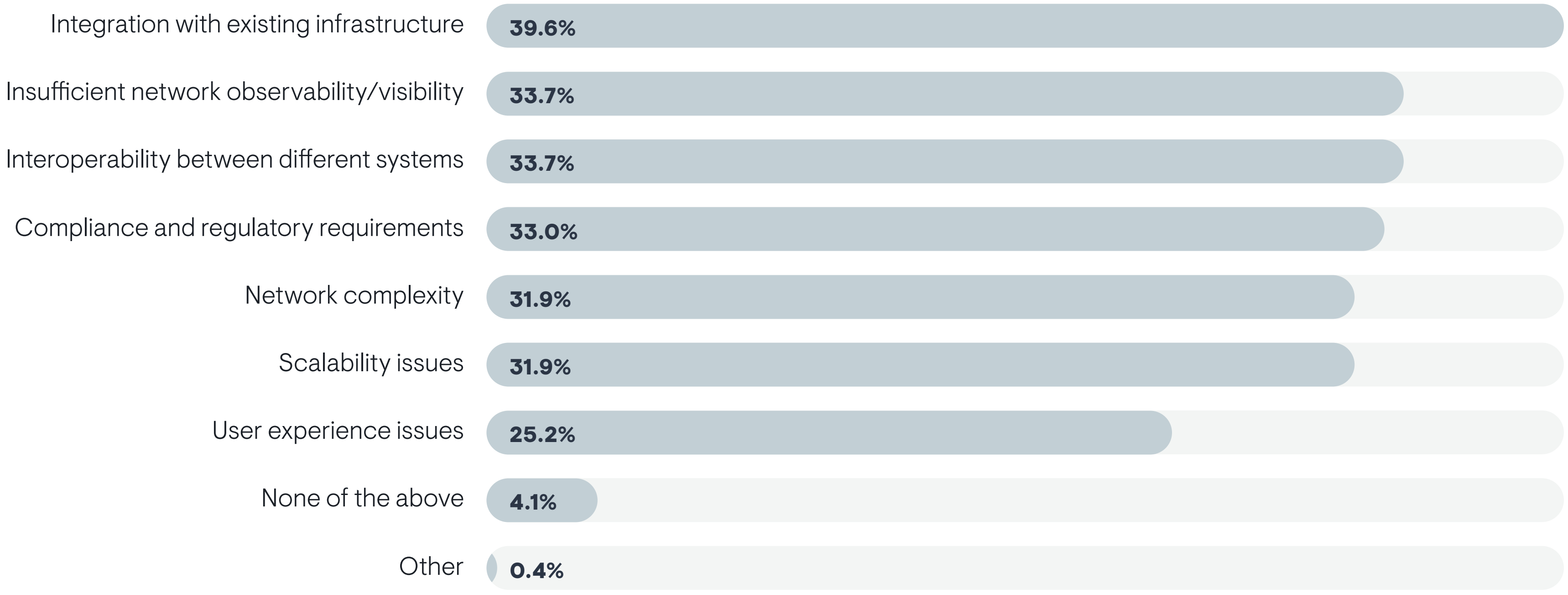


Sample Size = 270

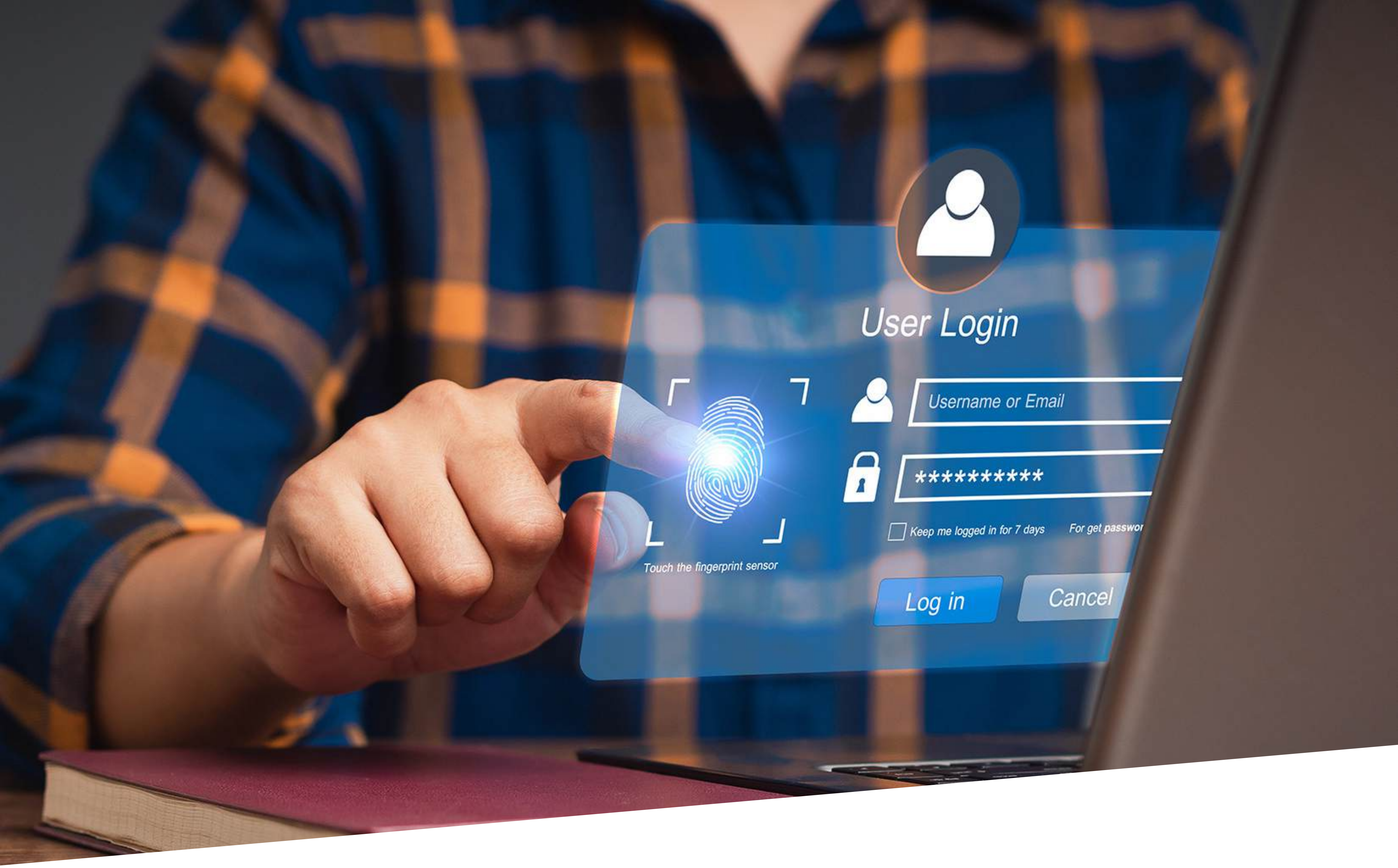
Figure 14 identifies the technical issues that undermine the network team's ability to support zero trust. The top issue is the effort to integrate existing infrastructure with zero trust architecture. Members of the network engineering team were more aware of this issue than people in the IT executive suite, suggesting that it is a bigger issue than even this chart reveals it to be.

Everything else is a secondary issue, with insufficient network observability and challenges with interoperability between different systems at the top of the list. Scalability was near the bottom of the list, but the cybersecurity team was more aware of this latter problem.

FIGURE 14. WHICH OF THE FOLLOWING TECHNICAL ISSUES ARE MOST CHALLENGING TO THE NETWORK TEAM'S EFFORTS TO SUPPORT YOUR ZERO TRUST STRATEGY?



Sample Size = 270



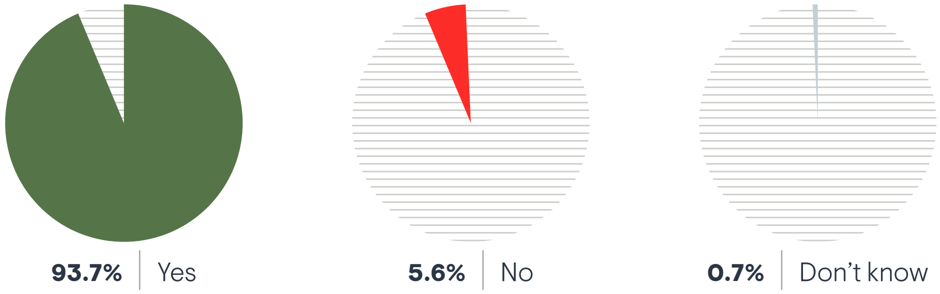
Zero Trust and Secure Remote Access

Secure Remote Access Modernization

In EMA's experience, enterprises usually have multiple secure remote access solutions, and the network team is usually responsible for many of them. For instance, the network team owns and operates VPN platforms, which are often implemented on network devices like routers or application delivery controllers. Any effort to modernize secure remote access will likely involve the network team. **Figure 15** reveals that nearly 94% of the companies in this research are modernizing remote access as part of their zero trust strategies.

This modernization is especially common among respondents who told EMA their zero trust strategies have been a complete success, while those who have failed with zero trust efforts are less likely to modernize remote access. EMA also found that enterprises with a hybrid cloud environment are also more likely to modernize remote access.

FIGURE 15. AS PART OF ITS ZERO TRUST STRATEGY, IS YOUR ORGANIZATION MODERNIZING OR PLANNING TO MODERNIZE THE TECHNOLOGY IT USES FOR SECURE REMOTE ACCESS (E.G., REPLACING LEGACY TECHNOLOGY)?



Sample Size = 270

Top Requirements for Zero Trust Secure Remote Access

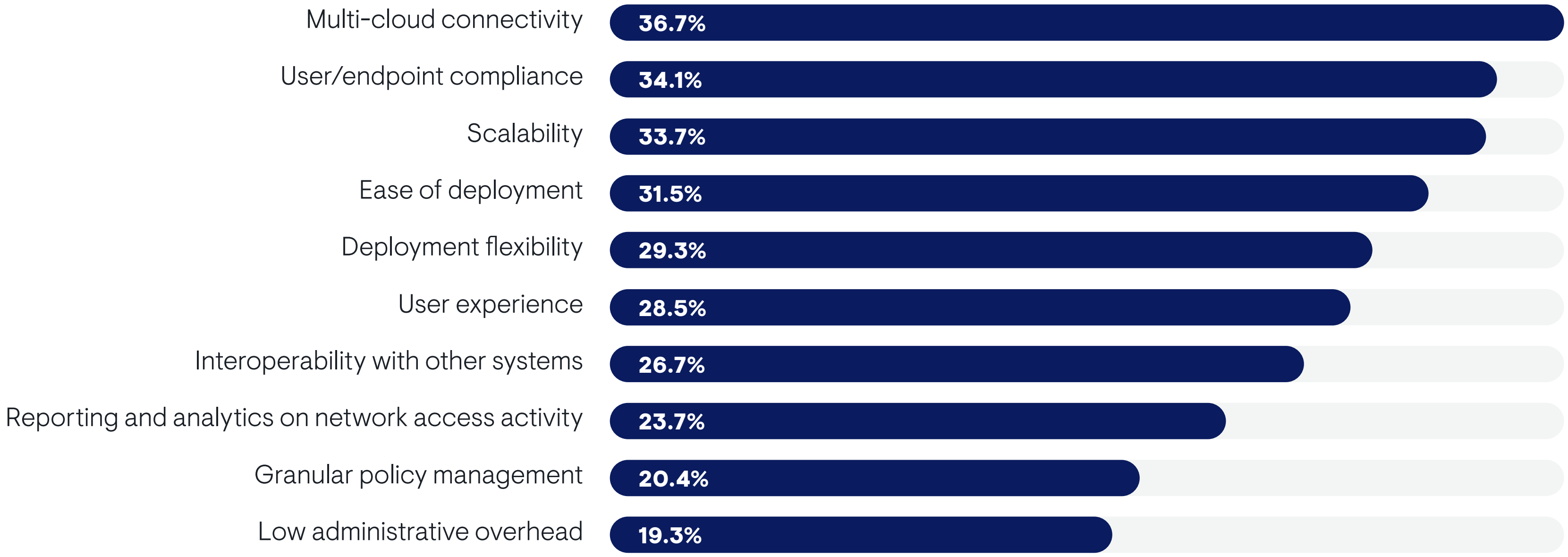
Figure 16 reveals the secure remote access solution requirements that enterprises prioritize when they embrace zero trust networking. Multi-cloud connectivity is the top consideration, suggesting that enterprises are looking for technology that can impose consistent secure access across different cloud providers.

Next, enterprises prioritize user/endpoint compliance, highlighting the need for a solution to validate users and make sure their devices comply with the access policies that an enterprise has set for its zero trust strategy. This requirement is especially important to enterprises with 1,000 to 10,000 employees and less important to larger companies.

Third, enterprises look for scalable solutions, which suggests that decision-makers know they need to support growing populations of end users with their remote access solutions,

Deployment flexibility and interoperability with other systems were two tertiary requirements that were high priorities for large enterprises (10,000 or more employees). Granular policy management was a low-priority requirement and was especially less important to organizations that reported greater success with zero trust strategies.

FIGURE 16. WHICH OF THE FOLLOWING ARE THE MOST IMPORTANT REQUIREMENTS OF A SECURE REMOTE ACCESS SOLUTION THAT SUPPORTS YOUR ZERO TRUST GOALS?



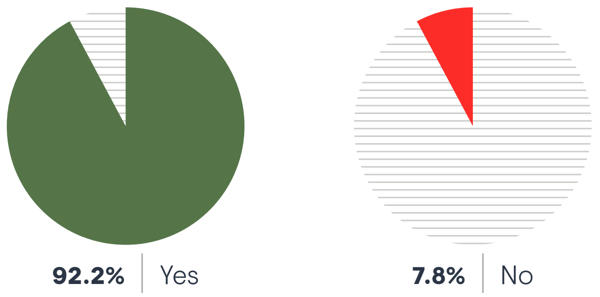
Sample Size = 270

Unifying Local and Remote Access

Hybrid work has created a new source of architectural complexity. With so many employees splitting their work week between the office and home, IT organizations are recognizing inefficiency in maintaining multiple technologies to manage network access. **Figure 17** reveals this complexity in stark terms. More than 92% of respondents want to unify or integrate the technology they use for on-premises network access control and secure remote access. Vendors have introduced solutions in the last few years that address this requirement, labeling them as "universal access" or "universal ZTNA" solutions.

Organizations that describe their zero trust strategies as a complete success are more likely to pursue this unification of access control. Hybrid cloud enterprises are also more prone to it.

FIGURE 17. DOES YOUR ORGANIZATION INTEND TO UNIFY OR INTEGRATE THE TECHNOLOGY IT USES FOR ON-PREMISES NETWORK ACCESS CONTROL AND SECURE REMOTE NETWORK ACCESS?

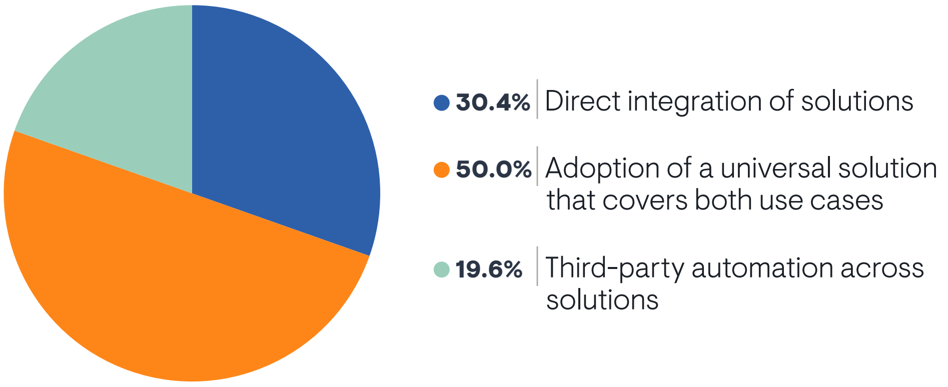


Sample Size = 270

Unification Approach

Figure 18 reveals how organizations intend to achieve this unification of access solutions. The most popular strategy is the adoption of a universal solution that covers both use cases, secure remote access and on-premises access control. Direct integration between two solutions is the second-most popular path. Fewer respondents reported plans to achieve this unification through third-party automation tools. The use of third-party automation tools was most popular among organizations with failed zero trust strategies, suggesting it is a worse practice.

FIGURE 18. WHAT IS THE BEST APPROACH TO UNIFYING ON-PREMISES NETWORK ACCESS CONTROL AND SECURE REMOTE ACCESS?



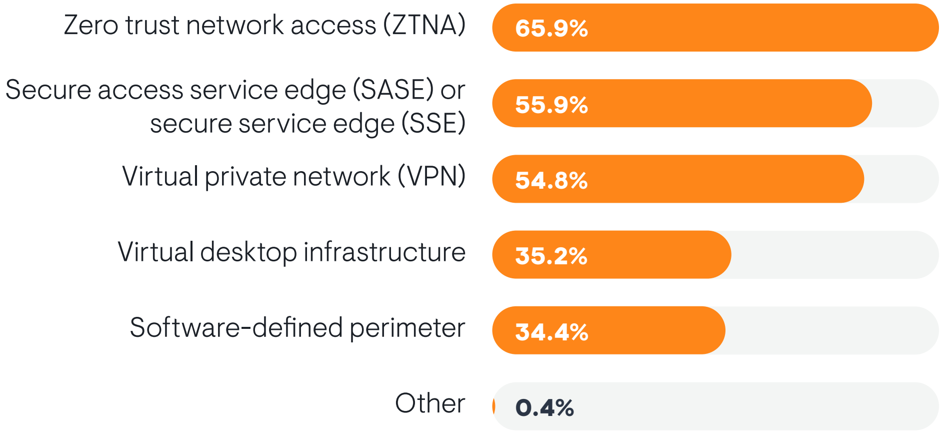
Sample Size = 270

Picking a Secure Remote Access Solution for Zero Trust

Figure 19 reveals that enterprises identified zero trust network access (ZTNA) technology as the best solution for addressing their zero trust requirements for secure remote access. Secure access service edge (SASE) is also very popular, as is a traditional VPN technology.

Fewer respondents selected virtual desktop infrastructure or software-defined perimeter (SDP) solutions as viable zero trust solutions. SDP was more popular among enterprises that host their applications exclusively in data centers and not the public cloud. Meanwhile, ZTNA and SASE were perceived as better solutions among enterprises that have hybrid cloud or 100% public cloud footprints. Respondents were more likely to select ZTNA if they considered network performance to be an important consideration when implementing zero trust solutions for secure remote access.

FIGURE 19. WHICH OF THE FOLLOWING TECHNOLOGIES WOULD BEST SUPPORT YOUR ORGANIZATION'S REQUIREMENTS FOR A ZERO TRUST SECURE REMOTE ACCESS SOLUTION?



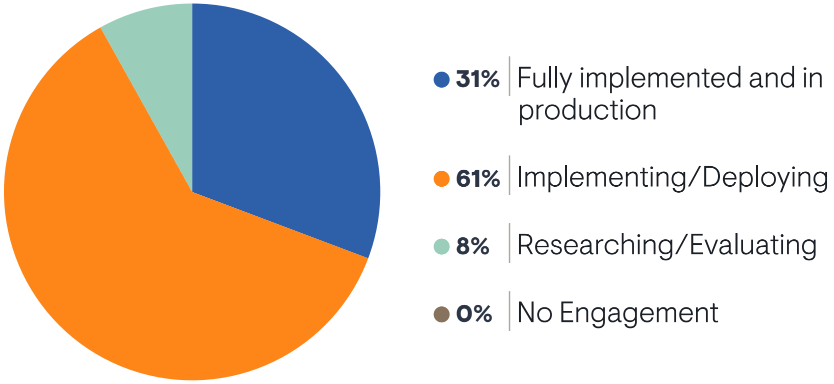
Sample Size = 270

100% of the enterprises represented in this research are engaged with ZTNA in some way.

ZTNA Engagement

This research established that most enterprises regard ZTNA as the best solution for applying zero trust to secure remote access. **Figure 20** reveals that 100% of the enterprises represented in this research are engaged with ZTNA in some way, with nearly 31% already using the technology, more than 61% implementing the technology, and 8% researching and evaluating it for potential adoption.

FIGURE 20. WHICH OF THE FOLLOWING DESCRIBES YOUR CURRENT ENGAGEMENT WITH ZERO TRUST NETWORK ACCESS (ZTNA) SOLUTIONS?

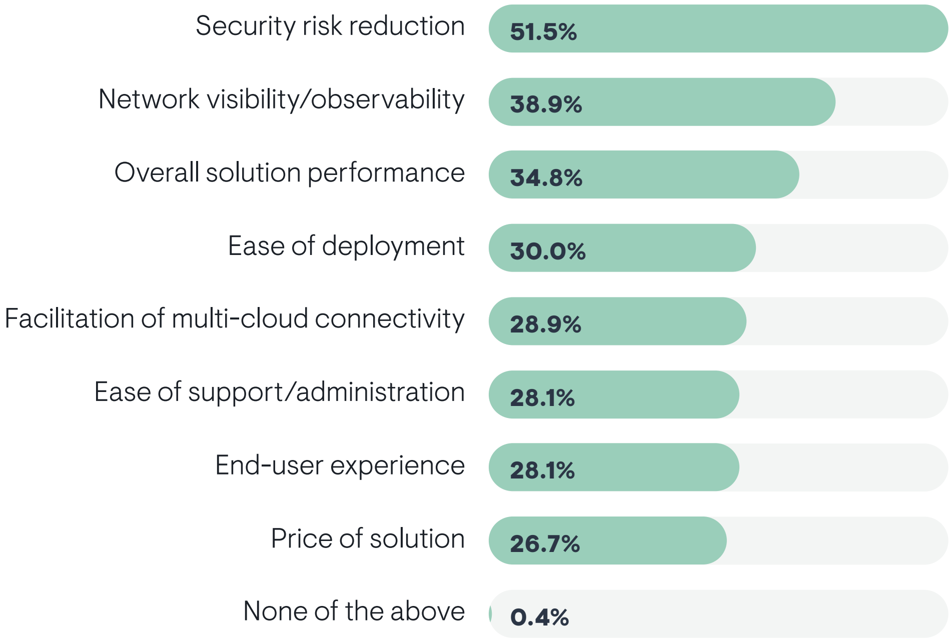


Sample Size = 270

ZTNA Technology Sentiment

Figure 21 reveals the aspects of ZTNA technology that respondents are most satisfied with today. Research participants were allowed to make up to three selections from the items listed in the chart. Overall, most were happy with ZTNA's ability to reduce security risk. Next, many were satisfied with the network visibility or observability ZTNA technology offers and overall solution performance. All other options were secondary. Respondents from very large companies (10,000 or more employees) were less likely to express satisfaction with observability, but they were more likely to be happy with overall performance.

FIGURE 21. WITH WHICH ASPECTS OF ZTNA TECHNOLOGY ARE YOU MOST SATISFIED?



Sample Size = 270

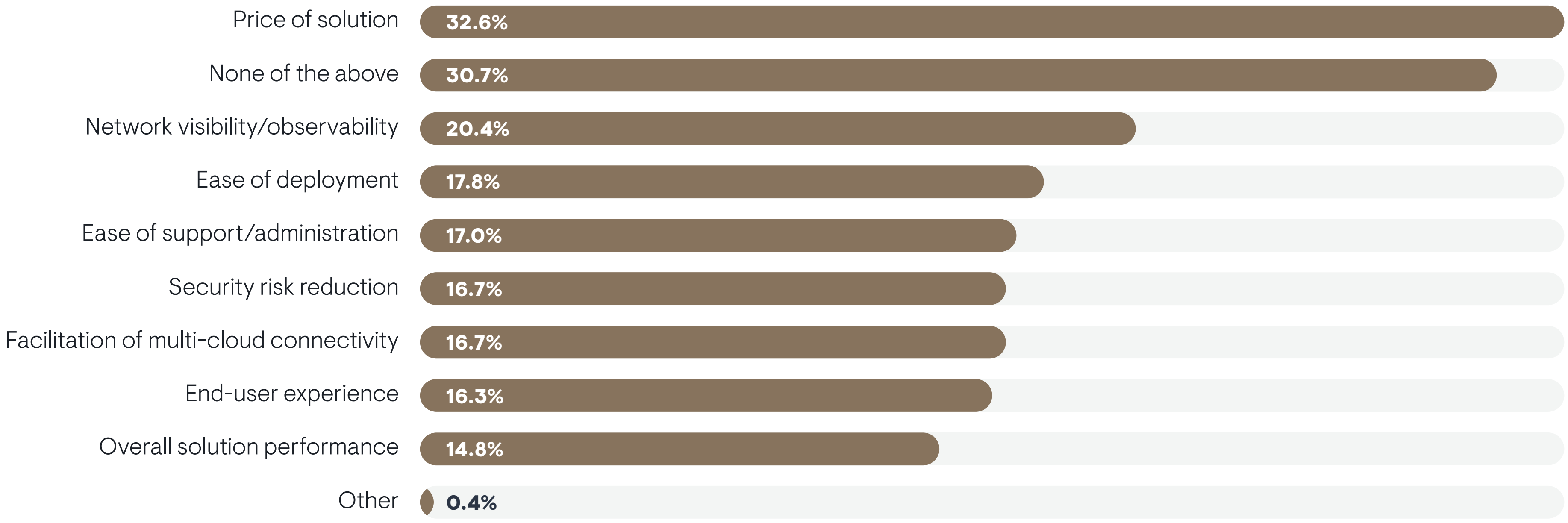
Figure 22 shows the flipside of ZTNA sentiment, revealing the aspects of the technology with which respondents are least satisfied. The top complaint was solution pricing. Nearly one-third of respondents are unhappy with the cost of a ZTNA product. Respondents who reported less success with their zero trust strategies were more likely to complain about pricing, suggesting that budget issues may be playing a role here.

Note that the second-most popular response to this question was “none of the above.” Nearly 31% claim that there is no aspect of ZTNA technology that has them dissatisfied. Respondents who reported the most zero trust success were more likely to make this selection.

Secondarily, many found fault with the observability capabilities of their ZTNA solutions, and ease of deployment edged out the rest of this list as the third-biggest issue.

Ease of deployment and ease of support were less problematic for most, but members of the network operations team were more likely to complain. Also, there was a significant gap in dissatisfaction with security risk reduction between members of the IT executive suite (9%) and members of cybersecurity (24%), network operations (28%), and network engineering (25%), suggesting that IT executives may be unaware of security risk issues that technical teams have detected with ZTNA.

FIGURE 22. WITH WHICH ASPECTS OF ZTNA TECHNOLOGY ARE YOU LEAST SATISFIED?



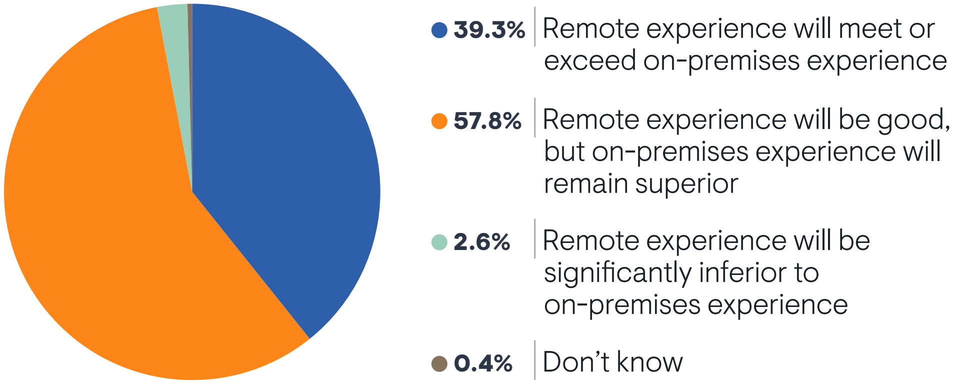
Sample Size = 270

User Experience in Focus

Expectations for User Experience

Figure 23 examines the expectations that organizations have for the experience of users who connect to their networks remotely. Only 39% believe it's possible that this remote user experience can be comparable or superior to the experience of people who work on-premises. Instead, most believe remote user experience can be good, but not equal to on-premises experience. Members of IT architecture and network operations groups are more likely to have higher expectations for user experience, while members of the IT executive suite, network engineering, and cybersecurity are more pessimistic. These expectations should guide decision-makers as they modernize their secure remote access solutions during their zero trust implementations. However, EMA found that organizations with successful zero trust strategies expect an experience that meets or exceeds on-premises experience.

FIGURE 23. TO WHAT EXTENT DO YOU THINK IT IS POSSIBLE TO DELIVER A DIGITAL EXPERIENCE TO REMOTE USERS THAT IS COMPARABLE TO THE EXPERIENCE THEY MIGHT HAVE WHEN WORKING ON-PREMISES IN YOUR CORPORATE SITES?



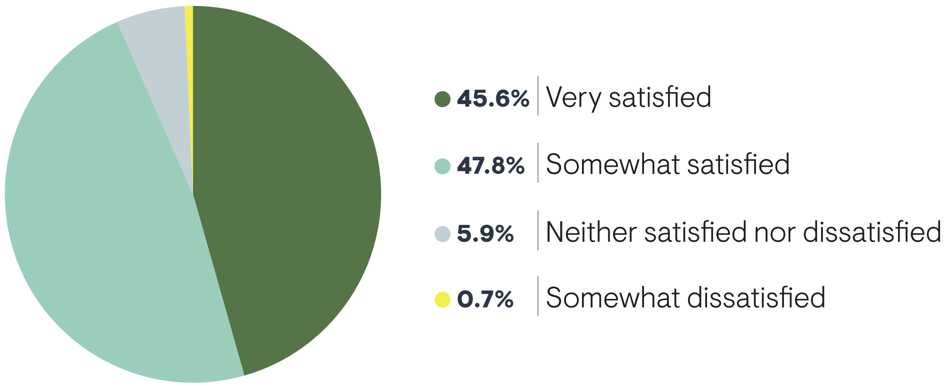
Sample Size = 270

Respondents at organizations that host all their digital resources in data centers have higher expectations for remote user experience than respondents who use public cloud services. Also, respondents who are satisfied with how their network observability tools support zero trust have higher expectations.

Satisfaction with Current User Experience

Figure 24 reveals how satisfied respondents are with the network performance and user experience associated with their secure remote access solutions. It reveals that nearly 46% are completely satisfied while another 48% see some room for improvement. Fewer than 1% are outright dissatisfied. Respondents who are the most successful with their zero trust strategies reported the most satisfaction. Satisfaction was higher among enterprises that have three or more public cloud providers. It was also higher among people who had network observability tools that were effective at supporting a zero trust strategy, suggesting that strong observability can help with designing and operating effective remote access solutions.

FIGURE 24. HOW SATISFIED ARE YOU WITH THE OVERALL NETWORK PERFORMANCE/USER EXPERIENCE OF YOUR CURRENT SECURE REMOTE ACCESS SOLUTION?



Sample Size = 270

Zero Trust Network Segmentation

Network segmentation has been around for a long time. In a zero trust architecture, IT organizations often implement more sophisticated and granular network segmentation schemes to limited lateral movement by malware and malicious actors.

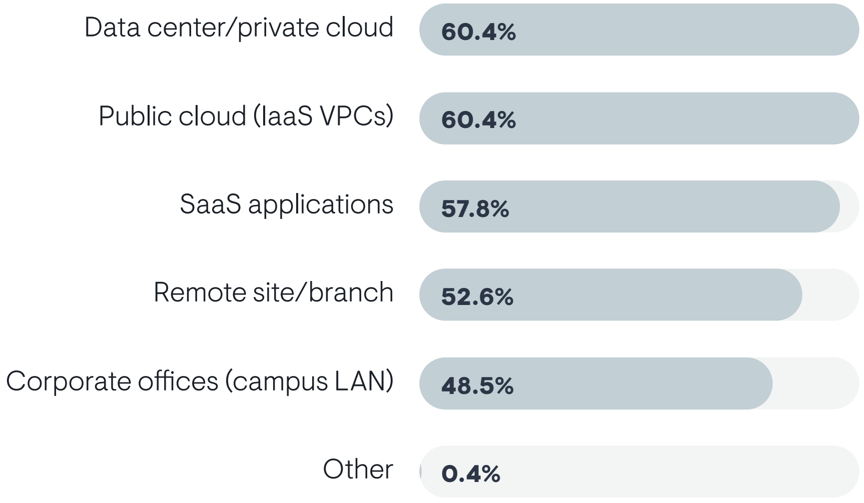
Zero Trust Segmentation Focus: Public Cloud, Data Centers, and SaaS Applications

Figure 25 reveals where organizations are concentrating their efforts to impose zero trust network segmentation. The two big focal points are the public cloud and the data center. Public cloud network segmentation is a major focus for enterprises that use three or more cloud providers.

Many are also trying to segment SaaS applications. Segmentation of SaaS applications is more common in midsized enterprises (1,000 to 2,500 employees).

Segmentation of remote sites and large campus networks is less common.

FIGURE 25. ON WHICH PARTS OF THE NETWORK IS YOUR ORGANIZATION APPLYING ZERO TRUST SEGMENTATION?



Sample Size = 270

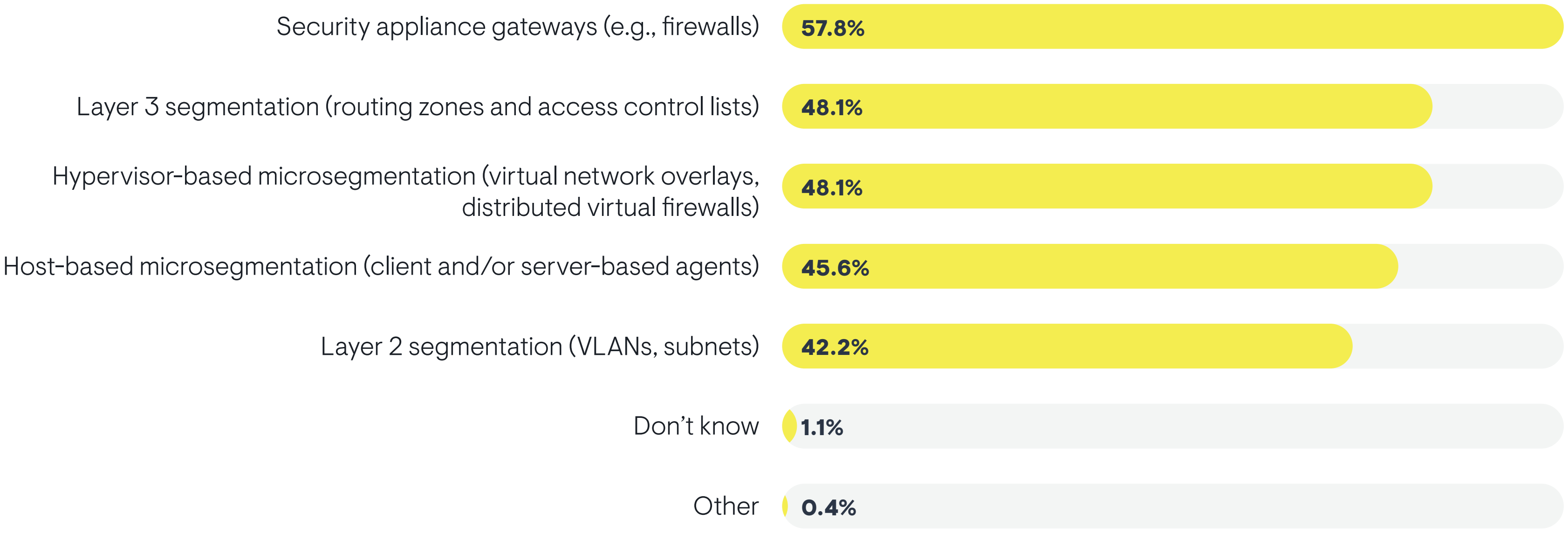
Segmentation Technologies

Figure 26 explores which technologies enterprises use to impose zero trust segmentation. The most popular approach is the use of security appliances, like firewalls. This legacy strategy involves the redirection of all traffic through a central point for the application of security policies that define network segments. The IT executive suite, the IT architecture group, and cybersecurity favored security appliances more. Cloud engineering, network engineering, and network operations personnel were less likely to favor them. These appliances were also popular among enterprises that have a hybrid cloud architecture. This approach can add inefficiencies to network traffic by adding latency and a single point of failure. Many enterprises try to mitigate these negative impacts by creating a distributed network security appliance architecture with multiple firewalls deployed throughout the network.

Other segmentation strategies were secondarily popular. Layer 2 and Layer 3 segmentation are legacy approaches implemented in network devices. They are typically less granular. Respondents who believe that network performance impacts should be a very important consideration when implementing zero trust favor Layer 3 segmentation.

Hypervisor- and host-based microsegmentation solutions are newer approaches, and they typically offer the most granular options for segmenting a network. The network engineering team favored hypervisor solutions and the network operations team favored host-based solutions.

FIGURE 26. HOW DOES YOUR ORGANIZATION PLAN TO IMPLEMENT ZERO TRUST NETWORK SEGMENTATION?



Sample Size = 270

Conclusion

This research demonstrates that network infrastructure teams are essential partners to the cybersecurity teams that are pursuing a zero trust strategy. There are a couple of reasons why the network team is so integral to these efforts. First, network engineers and architects are experts on the foundational technologies of zero trust. They know the weaknesses of legacy VPN solutions and they know how to evaluate, implement, and manage modern secure remote access solutions, like ZTNA and SASE. They are also experts on network segmentation and will be essential to translating legacy segmentation tools like firewall rules and VLANs to modern microsegmentation technologies based on hypervisor overlays or host-based agents.

The other reason why network teams need to be involved in zero trust is network performance. Most research respondents made it extremely clear that network performance and end-user experience are essential considerations when pursuing a zero trust strategy. They want to ensure that changes made to secure remote access solutions and network segmentation schemes do not degrade network experience. Network teams have the expertise and the observability tools that are needed to execute on this priority.

Cybersecurity teams lack the knowledge and the tools to protect an enterprise from potential adverse performance impacts with zero trust. EMA believes a poor user experience can make or break a zero trust strategy. If users realize that modernized secure remote access solutions are killing productivity, they will find a workaround that will undermine security. It will be the network team's job to ensure balance between performance and security.

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 4465.112224