Enterprise Zero Trust Networking Strategies: Secure Remote Access and Network Segmentation

By Shamus McGillicuddy
An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Research Report Summary
October 2020

Sponsored by:

Pulse Secure®

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Enterprise Zero Trust Networking Strategies: Secure Remote Access and Network Segmentation

Table of Contents

Executive Summary 1
Introduction 1
Demographics Overview 2
Zero Trust Networking Strategies 4
- Defining Zero Trust Networking 4
- The State of Zero Trust 5

The Zero Trust Networking Team 6
- Bringing Together Network and Security Experts 6
- Essential Areas of Networking and Security Collaboration 7
- Collaboration Roadblocks 8

Zero Trust Networking Success 9
- Benefits of Zero Trust Networks 10

Policy Design and Management for Zero Trust Networking 11
- Policies for IoT and Other Unmanaged Devices 11
- Dynamic Zero Trust Policy Engines 13

Secure Remote Access and Zero Trust 14
- Remote Access Requirements 14
- Zero Trust Remote Access Solutions 16
- Remote Access Solution Requirements 18

Network Segmentation and Zero Trust 20
- Zero Trust Segmentation Footprint 20
- Segmentation Technology 21
- Segmentation Management and Control 22
- Microsegmentation 23

Unifying Zero Trust Network Segmentation and Remote Access 25
Impacts of the COVID-19 Pandemic 26
- The Pandemic Accelerated Zero Trust 26
- Work From Home is the New Normal 27

Conclusion 29

EMA

Enterprise Zero Trust Networking Strategies: Secure Remote Access and Network Segmentation

Executive Summary

This summary of an Enterprise Management Associates (EMA) research report explores how IT organizations are using network technologies to support a Zero Trust security model. It is based on a survey of 252 enterprise technology professionals with direct and relevant experience with these efforts. EMA focused its investigation primarily on secure remote access, network segmentation, and microsegmentation technologies.

Introduction

Zero Trust is a network security model that minimizes risk by applying granular policies and controls to network access and network communications. Rather than establishing trust, the Zero Trust model is constantly verifying the legitimacy of network communications even inside the network perimeter. Changes in location, device state, security state, behavior, and more can initiate a reauthentication process.

The technologies that enable a Zero Trust model are often network-based. They include network segmentation and microsegmentation architecture and secure remote access solutions. These technologies need centralized policy management and control to coordinate authentication, authorization, and change management in a Zero Trust environment. These solutions may also integrate with parts of the security stack, like identity and access management and threat analysis, to enhance Zero Trust policy engines.

This research explores how network technology is the foundation of Zero Trust networking. It identifies key technical requirements of Zero Trust networking solutions, the organizational strategies enterprises establish to support Zero Trust with network and security teams, and the best practices they are establishing. The research also explores how the COVID-19 pandemic has impacted Zero Trust networking initiatives.

Demographics Overview

In August 2020, EMA surveyed 252 technology professionals who are directly engaged with applying network segmentation and secure remote network access solutions to a Zero Trust strategy.

Figure 1 offers an overview of who these research participates are. A large minority are executives in a technical organization, such as a CIO or CISO. A majority of them are in middle management, either a manager, supervisor, or director in an IT or security group.

Functional Groups Represented

- 43% Executive IT leadership (CIO or CISO's office)
- 19% Security architecture/engineering
- 14% SecOps
- 10% Network architecture/engineering
- 7% Data center operations
- 7% NetOps

Job Titles

- 34% CIO/CTO/CISO
- 27% IT or security manager/supervisor
- 19% IT or security director
- 6% IT or security VP
- 6% Architect
- 4% Engineer
- 4% Project manager

Figure 1. Departments and job titles

Figure 2 offers a profile of the enterprises that these people work for. The vast majority work for large or very large enterprises, but EMA also collected a significant sample from midsized enterprises. The majority are located in North America. The rest are in Europe, primarily in France, Germany, and the United Kingdom.

Company Size (Total Employees)
• 27% Midsized enterprise (250 to 999) • 54% Large enterprise (1,000 to 9,999) • 19% Very large enterprise (10,000+)
Geography
• 63% North America • 37% Europe
Industry
• 18% Professional services • 16% Manufacturers • 14% Software • 13% Retail/Wholesale/Distribution • 13% Finance/Banking/Insurance • 4% Utilities/Energy • 4% Healthcare/Pharmaceutical/Medical • 4% Construction • 3% Government

Figure 2. Corporate profiles

Zero Trust Networking Strategies

Defining Zero Trust Networking

EMA asked these 252 subject matter experts to weigh in on what defining characteristics of Zero Trust networking are most critical to them. **Figure 3** shows that a majority of enterprises believe it is critical that Zero Trust controls can take additional action after initial access has been granted to an authenticated user or device. Fifty-six percent said a Zero Trust system must be able to force users and devices to reauthenticate at any time, based on policies and observed activity.

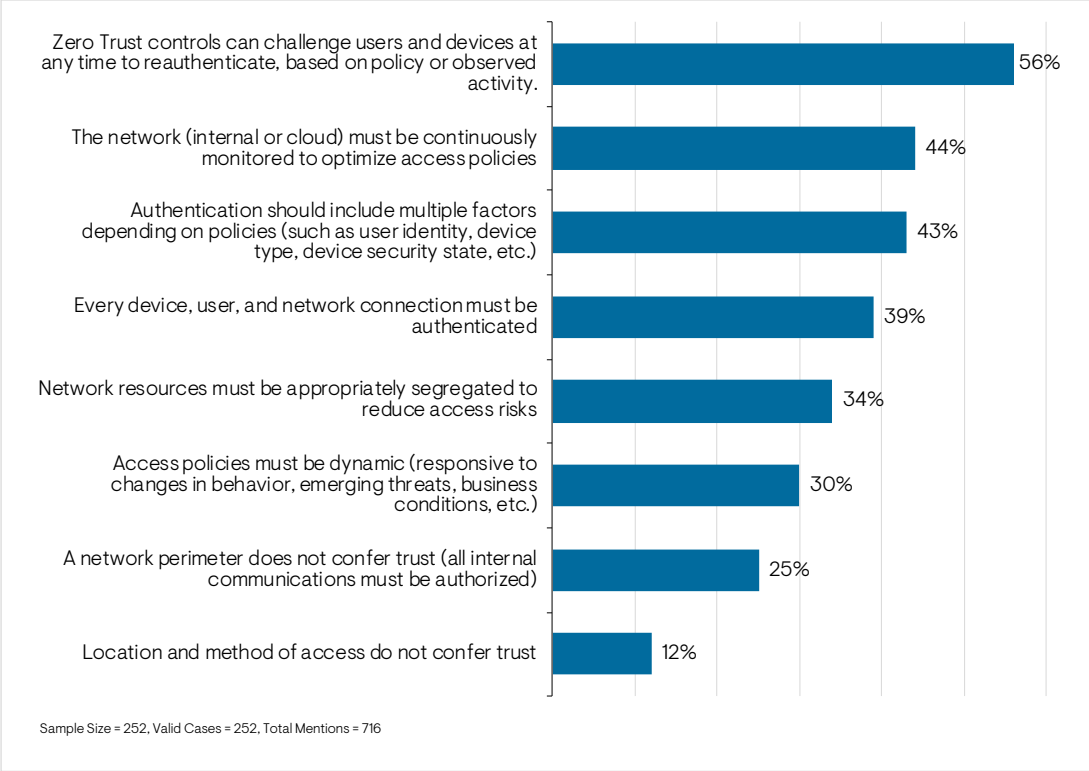

Figure 3. Concepts most fundamental and important to Zero Trust networking implementation

The survey identified three secondary principles that, taken together with the ability to reauthenticate, can serve as the overall definition of Zero Trust networking in the context of this research.

- Zero Trust controls must be able to challenge connected devices and users to reauthenticate at any time
- The network must be continuously monitored to optimize access policies
- Authentication must be based on multiple factors, depending on policy design
- Every device, user, and network connection must be authenticated

The State of Zero Trust

EMA's goal with this research was to survey enterprises that are engaged with Zero Trust networking. EMA used a series of qualifying questions to weed out people who lacked timely experience with the concept. As **Figure 4**, reveals, anyone who admitted to having no Zero Trust activity in their organization was dropped. Among those that have some sort of Zero Trust engagement, most (85%) have a defined Zero Trust initiative, although only half of those have received added budget to support this initiative. Healthcare, software, non-IT manufacturing, professional services, and retail organizations were all more likely to have added budget.

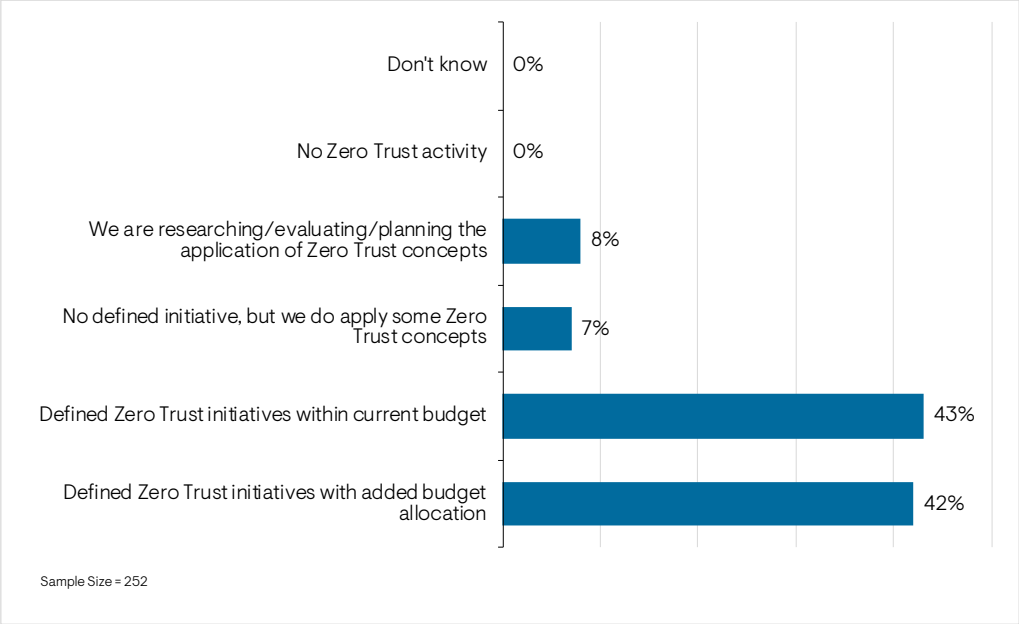

Figure 4. What is the state of Zero Trust security in your organization?

A very small percentage take an ad hoc approach, in which they have no formal initiative but apply some Zero Trust concepts to their environment. Very large enterprises (21%) are the most likely to adopt this ad hoc approach. Another small percentage are mostly researching and evaluating Zero Trust.

Enterprises that have defined Zero Trust initiatives with added budget are more likely (61%) to be successful with Zero Trust networking projects. Meanwhile, only 29% of organizations that take an ad hoc approach to Zero Trust reported success with Zero Trust networking.

Enterprises that have defined Zero Trust initiatives with added budget are more likely (61%) to be successful with Zero Trust networking projects.

The Zero Trust Networking Team

Bringing Together Network and Security Experts

EMA remains confident in saying that Zero Trust network projects continue to be multidisciplinary, with strong contributions from the security and networking teams. **Figure 5** examines the nature of this collaboration.

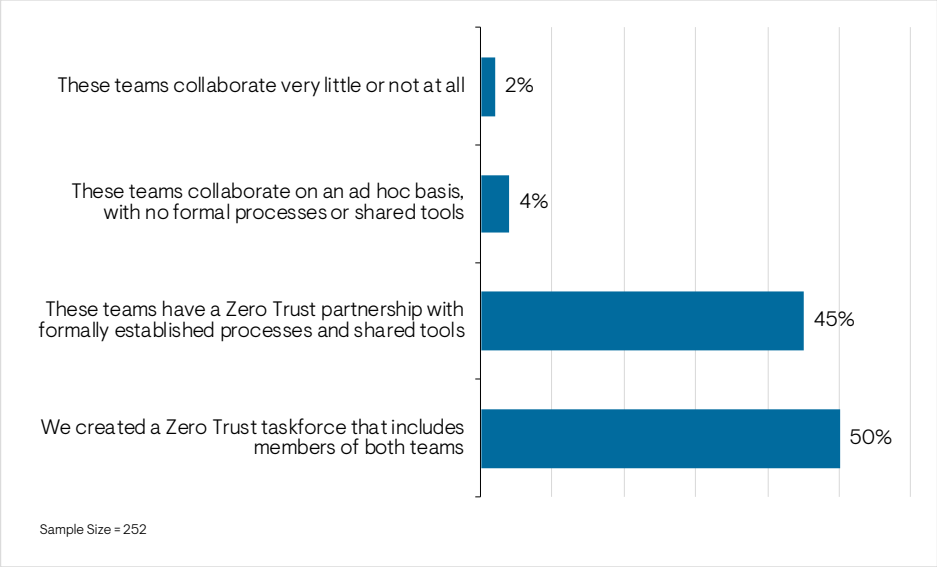

Figure 5. The nature of Zero Trust collaboration between network and security teams

Half of enterprises have formed a Zero Trust taskforce that draws on both the network and security teams for personnel. Organizations that added to their IT budgets in support of a Zero Trust initiative are more likely (68%) to have a taskforce. Taskforces are also preferred by organizations that are successful with Zero Trust (62%). Healthcare, software, professional services, and retail companies all have an affinity for taskforces.

Another 45% have established a formal partnership between networking and security, with shared tools and processes. Ad hoc collaboration is rare, and only a handful claim to have little to no collaboration at all. Construction, finance, government, manufacturing, oil and gas, and utility companies all prefer partnerships between the two groups.

Half of enterprises have formed a Zero Trust taskforce that draws on both the network and security teams for personnel.

Essential Areas of Networking and Security Collaboration

Figure 6 reveals how networking and security professionals need to collaborate, regardless of whether they're working within a taskforce or as part of a partnership between these teams. The top priority is coordinating access security controls across multiple systems. At the highest level, the network team might implement and operate most of a company's segmentation solutions, while the security team might be responsible for remote access. At a lower level, a security team might own a host-based network segmentation solution, while the network team might be responsible for Layer 2 segmentation through VLANs.

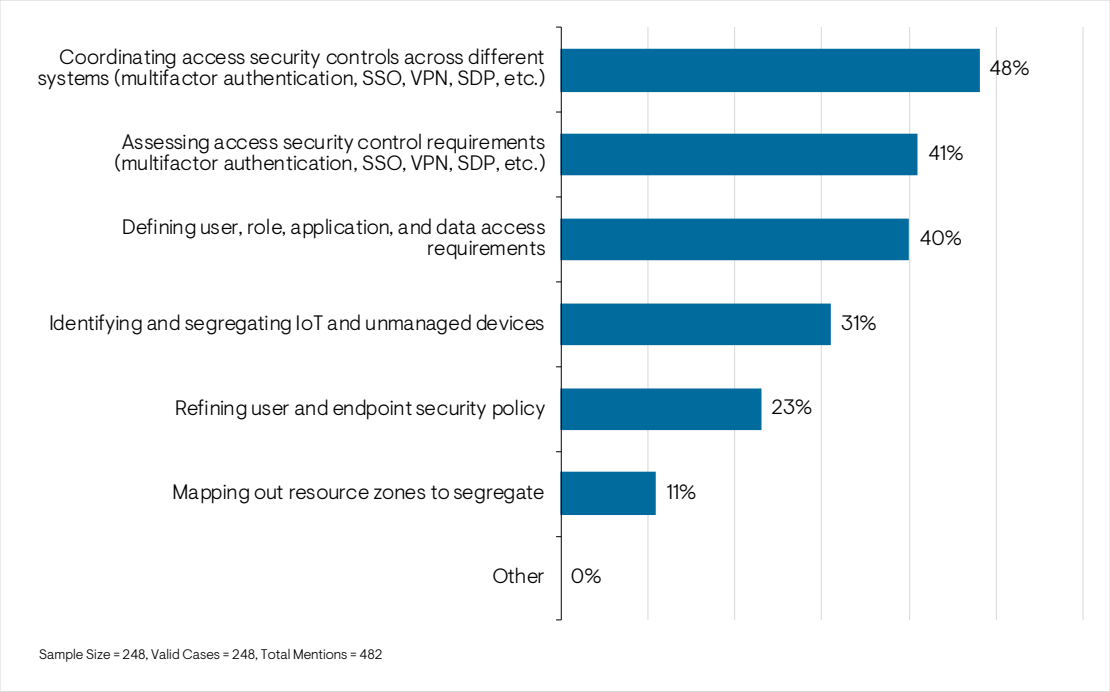

Figure 6. Most important areas of Zero Trust collaboration between network and security teams

Collaboration Roadblocks

Network and security teams are not natural allies, even when they share a common Zero Trust goal. The network team's core mission is to provide a healthy, high-performing network connection to anyone and anything that needs it. The security team is usually driven to limit connectivity as much as possible.

Figure 7 explores the kinds of conflicts and challenges that can derail cooperation between these groups when they are trying to execute a Zero Trust network. The good news is that 15% claim to have no significant challenges at all. The bad news is that the other 85% are dealing with at least two significant issues.

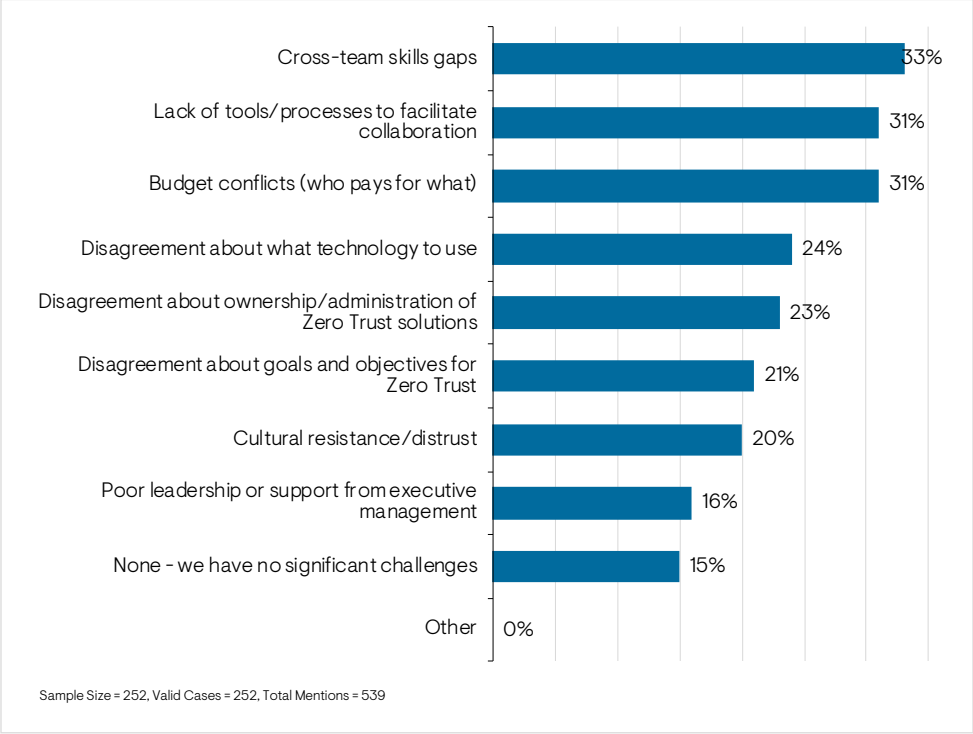

Figure 7. Leading challenges to Zero Trust-related collaboration and project execution between network and security teams

Companies are primarily struggling with cross-team skills gaps, a lack of tools and processes to facilitate collaboration, and conflicts over whose budget pays for what. The lack of collaborative tools and processes is particularly common among somewhat successful Zero Trust networking initiatives (39%), while less common among successful projects (25%). This finding suggests that a lack of collaborative tools and processes can derail a project.

Disagreements about Zero Trust goals and objectives and disagreements about ownership of Zero Trust solutions are some of the least challenging issues enterprises are facing. However, both of these problems are very common within companies that lack a formal Zero Trust initiative. Less successful Zero Trust strategies are also more likely to struggle with conflicts over who owns the solutions.

Zero Trust Networking Success

Figure 8 reveals how successful research participants are with their Zero Trust networking efforts. EMA finds that technologists are rarely willing to give their initiatives a failing grade. Thus, EMA focuses on enthusiasm, distinguishing between those who claim success and those who claim to be only somewhat successful. The differences between these two groups can reveal best practices.

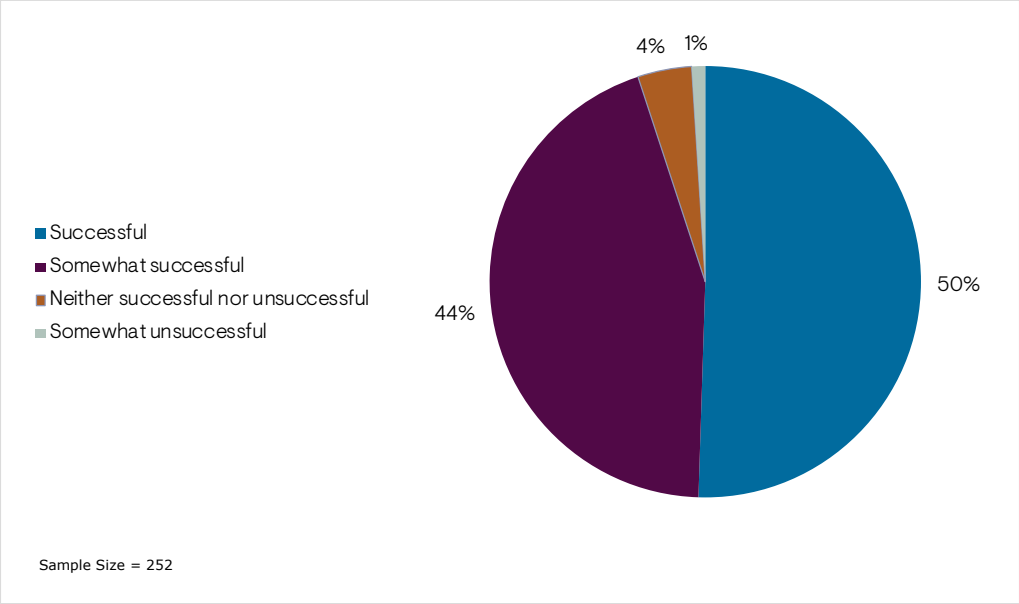

Figure 8. Overall success with applying network technology to the Zero Trust security model

In this case, half of survey participants claim that their application of network technology to Zero Trust has been fully successful. Forty-four percent revealed that they have been only somewhat successful. IT executives have a sunnier outlook (60% claimed success). Europeans were less likely to claim full success (37%).

Half of survey participants claim that their application of network technology to Zero Trust has been fully successful.

Benefits of Zero Trust Networks

Any technology investment must be justified by some kind of return. EMA asked survey participants to identify the top business benefits they have experienced or anticipate from their Zero Trust networking projects. **Figure 9** reveals that IT operations agility is the biggest Zero Trust opportunity.

IT operations agility is the biggest Zero Trust opportunity.

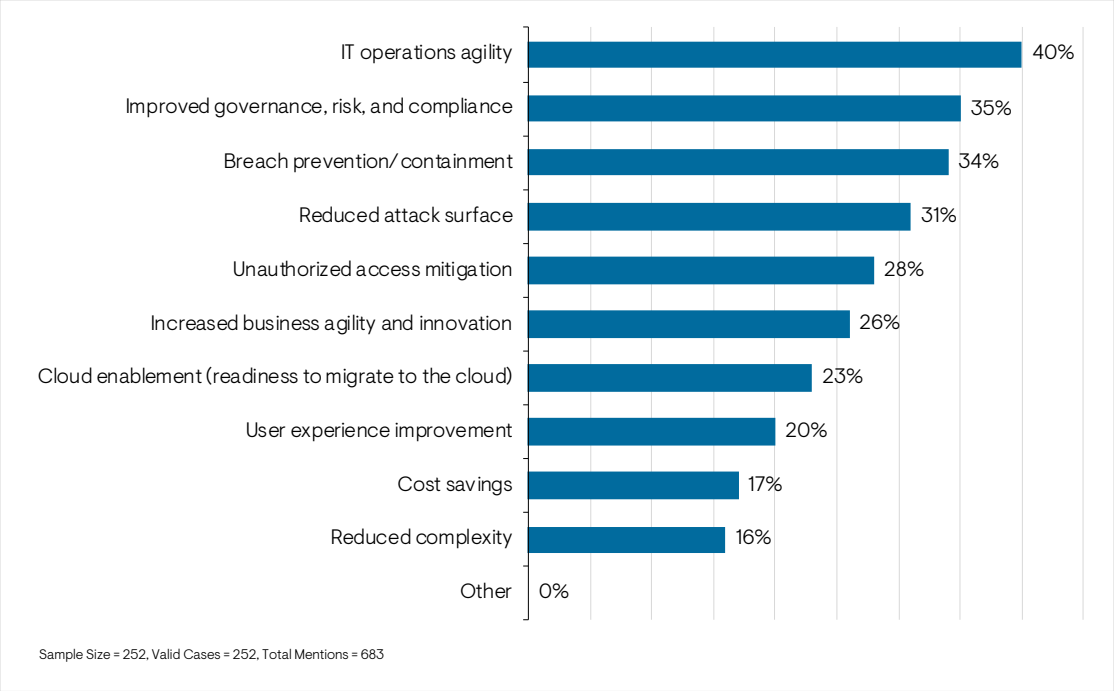

Figure 9. Most valuable business benefits experienced or anticipated via Zero Trust networking

Secondarily, enterprises improve governance, risk, and compliance (GRC), improve breach prevention and containment, and reduce their overall attack surface. Very large enterprises are more likely to target reduced attack services, but less likely to target GRC and breach prevention. Financial companies are more focused on GRC.

Policy Design and Management for Zero Trust Networking

This section explores how enterprises design and manage the policies that drive their Zero Trust network solutions.

Policies for IoT and Other Unmanaged Devices

User identity is the foundation of many Zero Trust policy strategies. Identity and access management systems contain information on what access privileges users should have. This information can help a Zero Trust solution determine whether a network connection should be allowed. However, if a device has no user associated with it, the Zero Trust controls require an alternative way to authenticate connection requests. Thus, IoT and other unmanaged devices present a challenge to Zero Trust networking policy design.

Figure 10 reveals how enterprises prefer to determine network access privileges for devices without an associated user identity. The most popular strategy, but by no means the majority view, is to create tailored access privileges based on the functions and characteristics of individual devices or classes of devices. These tailored policies will require deep visibility into the devices themselves so that Zero Trust solutions can authenticate them. This policy design strategy is less popular within very large enterprises with 10,000 or more employees (23%), possibly because these larger companies are dealing with too much complexity and too many devices to create such granular policies.

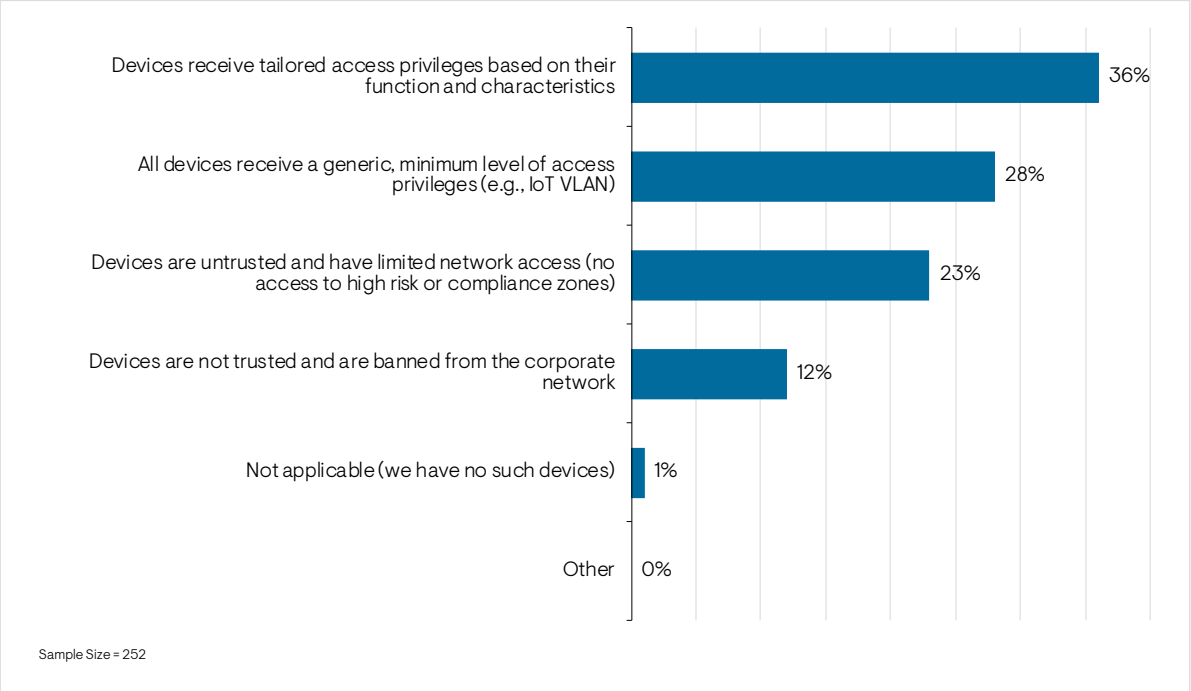

Figure 10. Preferred method for determining network access privileges for devices without an associated user identity

The next most popular policy strategy is to establish a generic, minimum level of access privilege for these devices, such as an IoT VLAN. This strategy is popular among government agencies (50%) and healthcare organizations (55%).

Fewer than one-quarter of organizations prefer to treat such devices as untrusted, with limited access. Finally, only 12% claim that these devices are banned from the corporate network altogether.

EMA asked the 91 survey participants who prefer to create tailored access policies for unmanaged devices to reveal which attributes are most important to determining those access privileges. Device security status is the top parameter by a large margin. Executive respondents (63%) are especially focused on security status, while middle management respondents are less likely to favor it (39%).

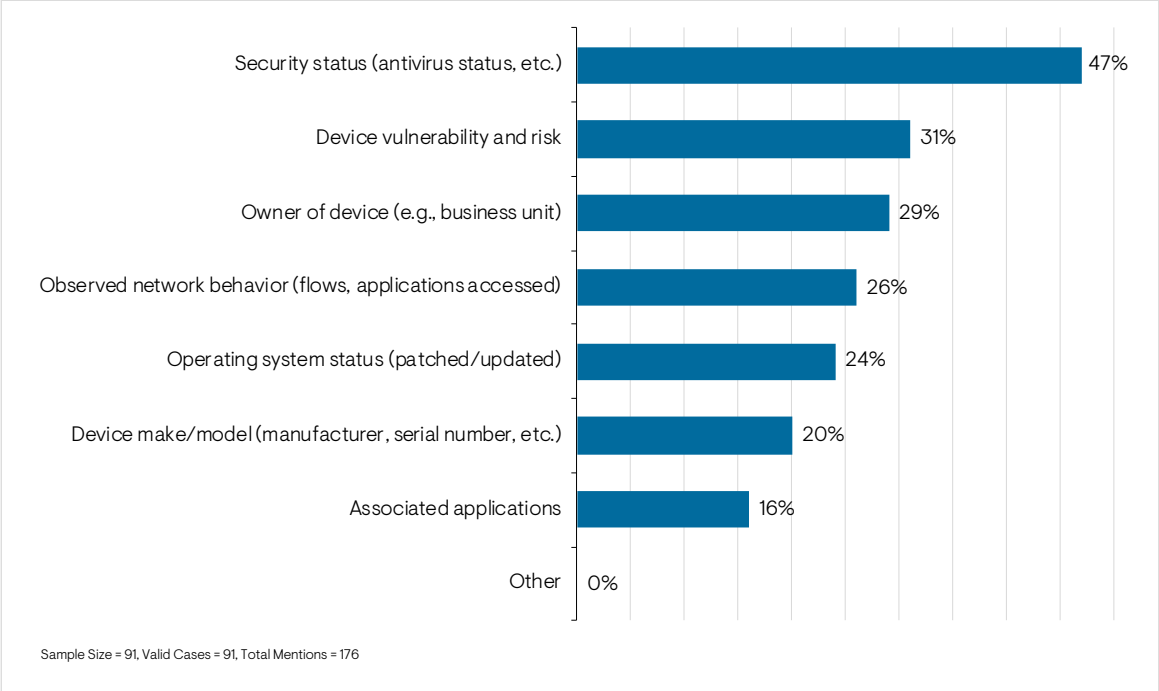

Figure 11. Most important parameters for determining access privileges of unmanaged devices

Device vulnerability and risk, device owner, observed behavior, and operating system status are all secondary attributes. Device make and model and associated applications are the least essential. However, midmarket enterprises are much more likely to use associated applications as an attribute (32%).

Dynamic Zero Trust Policy Engines

Earlier in this report, EMA defined Zero Trust by reviewing the conceptual principles of the model that are most important to survey respondents. Figure 3 revealed that a dynamic Zero Trust policy model is essential to 30% of enterprises. This requires a dynamic policy engine that can apply adaptive polices based on changing conditions, such as threat intelligence, user state, and device state.

More than half of these enterprises have fully implemented a dynamic policy engine, and only 2% have absolutely no plans to do so.

Figure 12 reveals that more than half of these enterprises have fully implemented a dynamic policy engine, and only 2% have absolutely no plans to do so. Organizations that have added new budget specifically to support a Zero Trust networking initiative are more likely (69%) to have fully implemented dynamic policy, while ad hoc Zero Trust projects are much less likely (35%).

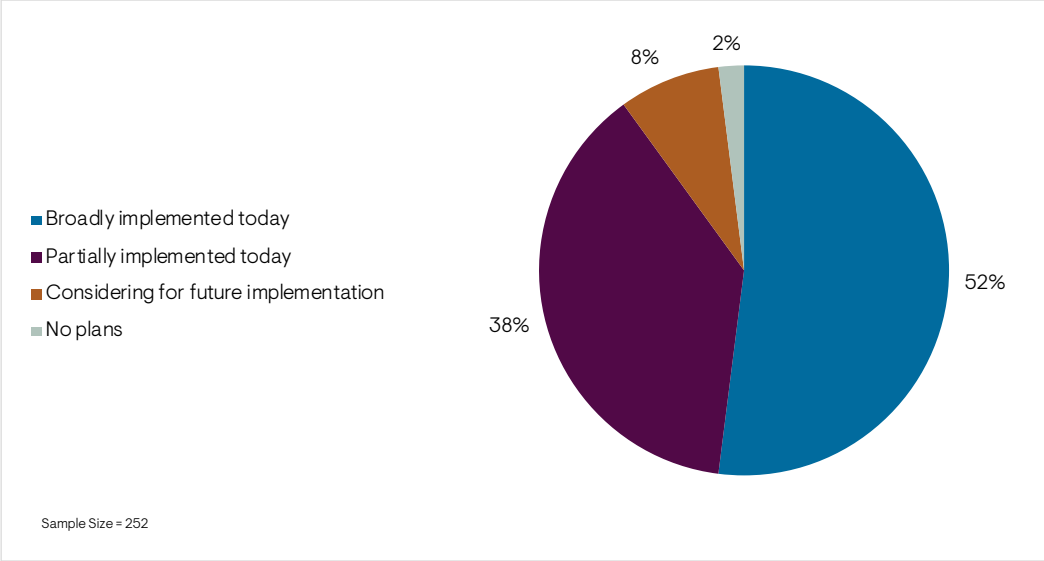

Figure 12. Status of Zero Trust dynamic policy engine adoption

Dynamic policy engine adoption also correlates with Zero Trust success. Seventy-two percent of successful initiatives have fully implemented dynamic engines, but only 32% of somewhat successful initiatives have done so.

Secure Remote Access and Zero Trust

This section reviews how enterprises are adapting and applying their secure remote access solutions to their Zero Trust networking strategy. It explores technology requirements and adoption plans.

Remote Access Requirements

Figure 13 reveals the general remote access requirements that enterprises in this study have today. Cloud access is the highest priority. In particular, 62% need secure remote access to SaaS applications. Half of them need access to both public and private cloud resources and applications. Corporate network access is a secondary priority, with Layer 3, Layer 4, and Layer 7 network access drawing interest from small minorities of enterprises.

62% need secure remote access to SaaS applications. Half of them need access to both public and private cloud resources and applications.

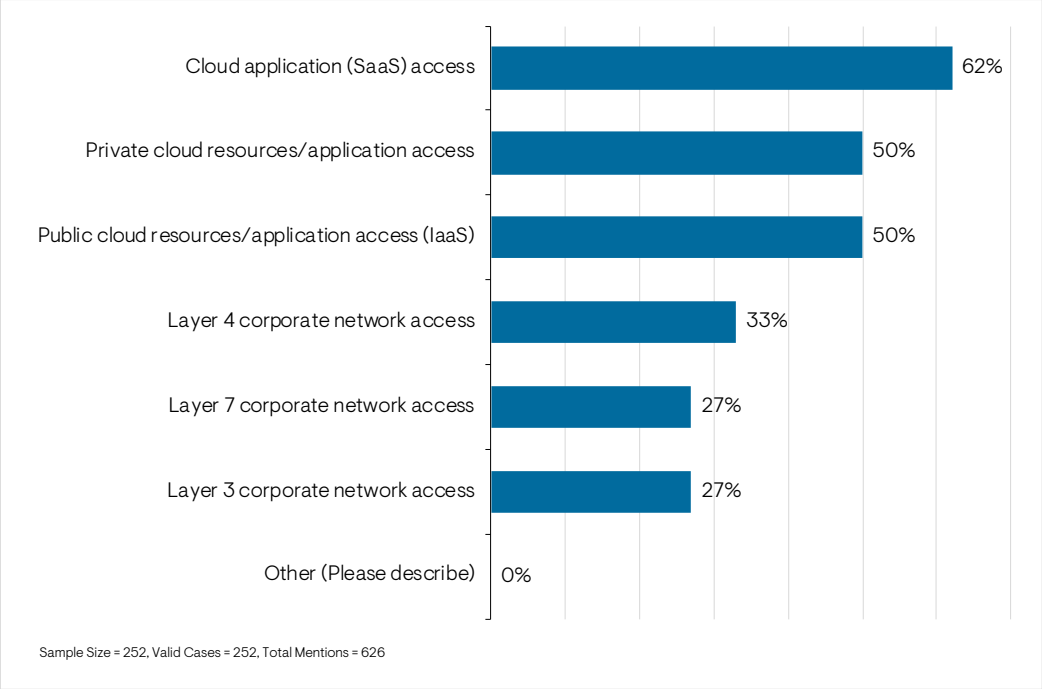

Figure 13. The general remote access requirements enterprises have today

When enterprises have a mix of on-premises and external cloud access requirements, the question that emerges is this: Should you establish hybrid access with a solution that can manage access across both domains? **Figure 14** shows that 41% of enterprises want a central platform that controls access across corporate assets and cloud-based assets. Only 28% want siloed platforms that specialize in one or the other. Another 32% say they need a combination of both platforms, suggesting that they are taking a multi-layered approach to hybrid remote access. Successful Zero Trust strategies are more likely (49%) to require a unified hybrid access platform, while somewhat successful strategies are less likely (34%) to require it.

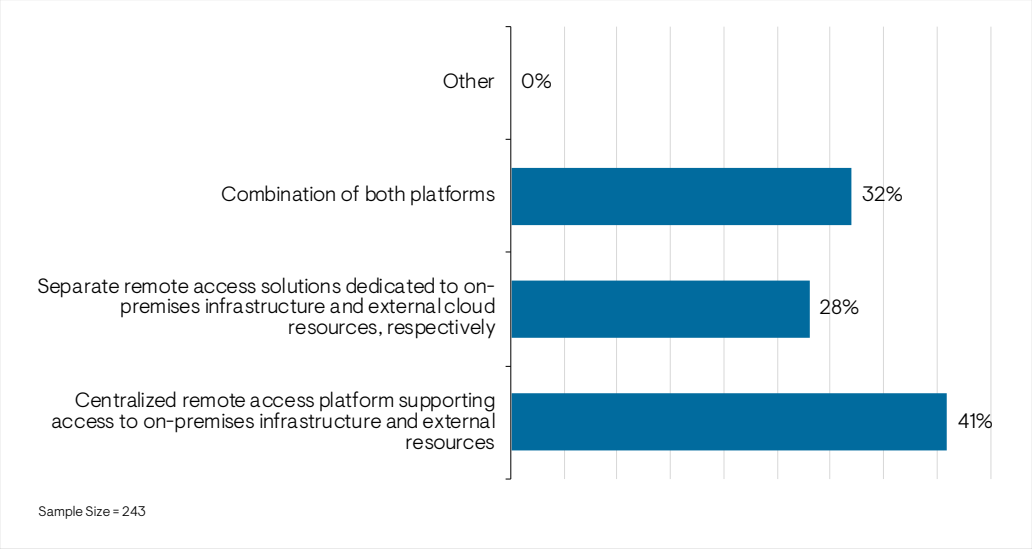

Figure 14. Preferences for providing Zero Trust remote access to external cloud and on-premises assets

Zero Trust Remote Access Solutions

Figure 15 reveals the types of remote access products that enterprises are using to support their Zero Trust networking requirements. The chart shows what enterprises are using today and what they plan to use or investigate for use within the next 18 months. The chart shows high adoption of legacy VPN technology and remote access protocols, but both will decline slightly by 2022. Use of SD-WAN for Zero Trust remote access will remain flat. Virtual desktops will decline. Secure access service edge (SASE) use will increase significantly, and software-defined perimeters (SDPs) will grow modestly.

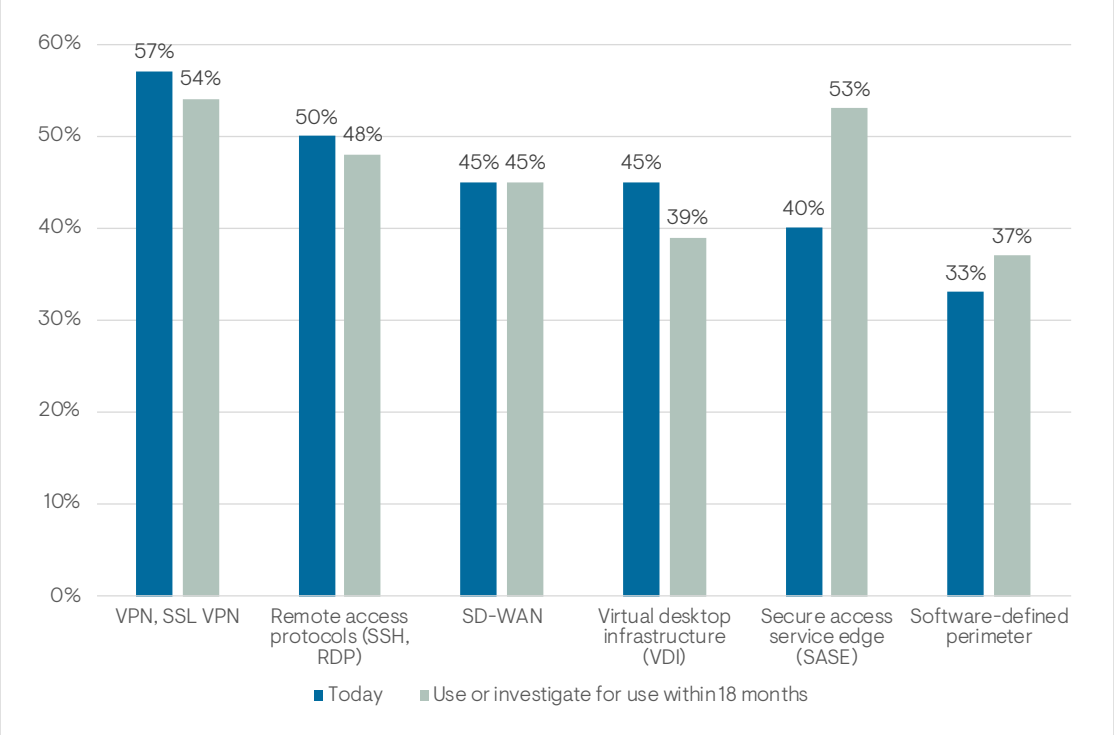

Figure 15. Remote access solutions applied to Zero Trust networking

EMA believes that the high rate of adoption today for SASE (40%) is inflated by misleading marketing. SASE is a very new product category that combines SD-WAN, remote user access, and cloud-based security into a unified platform. While many vendors have started marketing SASE solutions, particularly SD-WAN and cloud security vendors, very few have a complete and fully integrated solution. Many of the respondents in this research may believe they have SASE implemented, but they have been oversold or misled by their vendors. EMA has observed similar inflated adoption numbers with other hyped technologies, most recently SD-WAN and AIOps.

The shift to Zero Trust networking will disrupt installed remote access solutions. **Figure 16** reveals that 69% of enterprises will replace their legacy remote access technology within the next 12 months to support Zero Trust, including 27% that have already done so. Only 4% believe that their existing remote access solutions can fully enable Zero Trust, and 22% will use legacy technology and new technology together to achieve Zero Trust.

69% of enterprises will replace their legacy remote access technology within the next 12 months to support Zero Trust.

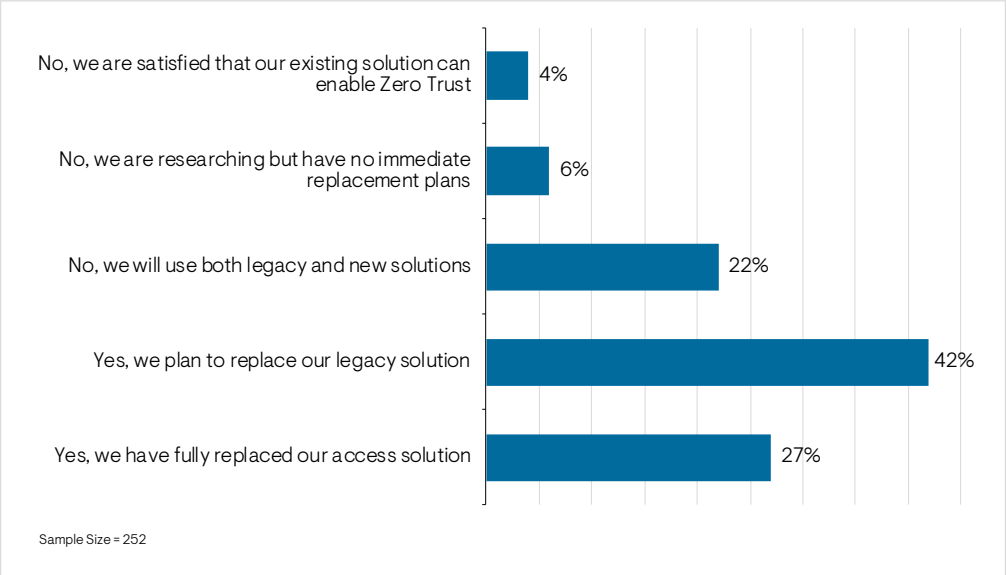

Figure 16. As part of your Zero Trust strategy, do you expect to replace your legacy secure remote access solution within the next 12 months?

Remote Access Solution Requirements

This section explores some of the technical requirements of a Zero Trust remote access solution. First, **Figure 17** reveals that 96% of enterprises require a central controller for policy management and access authorization. Sixty-three percent consider this capability critical to their Zero Trust network. Very large enterprises are more likely (77%) to say this is critical, as are government agencies, software companies, retailers, and utility companies.

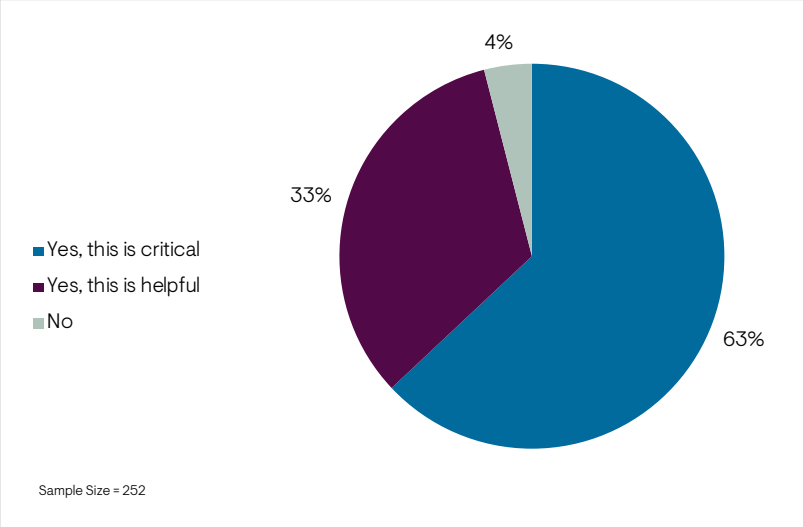

Figure 17. Does your organization's Zero Trust network strategy require a secure remote access solution with a central controller that manages policy and authorizes access requests?

EMA asked respondents to rank the importance of seven product characteristics, with 1 being the most important and 7 being least important. The mean responses are charted in **Figure 18**. The results show that enterprises consider performance and scalability to be the most important measures of a solution. Access visibility and analytics and hybrid IT support are also top priorities.

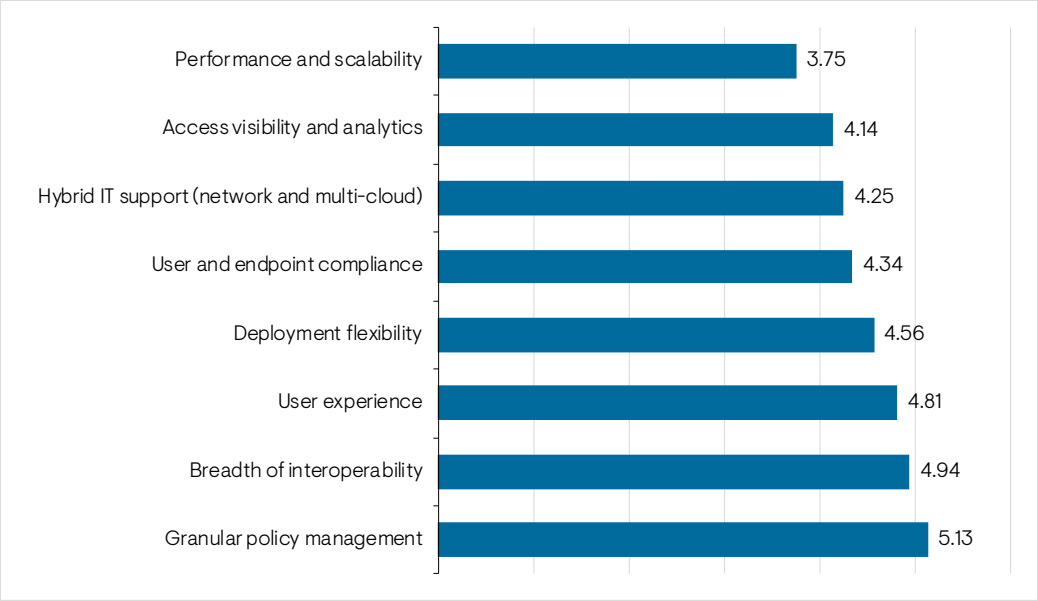

Figure 18. Mean responses: "Rank the following characteristics of Zero Trust remote access, with 1 being most important and 7 least important."

Network Segmentation and Zero Trust

This section reviews how enterprises are applying network segmentation and microsegmentation to their Zero Trust networking strategy. It explores technology requirements and adoption plans.

Zero Trust Segmentation Footprint

EMA asked respondents to identify where they have implemented Zero Trust network segmentation on their networks. **Figure 19** reveals that application infrastructure is the primary focus. Large majorities have introduced Zero Trust segmentation to their data centers and/or private clouds and their public cloud environments. Very large enterprises (83%) are very likely to have Zero Trust segmentation in their data centers and private clouds, and less likely (51%) to have it in the public cloud.

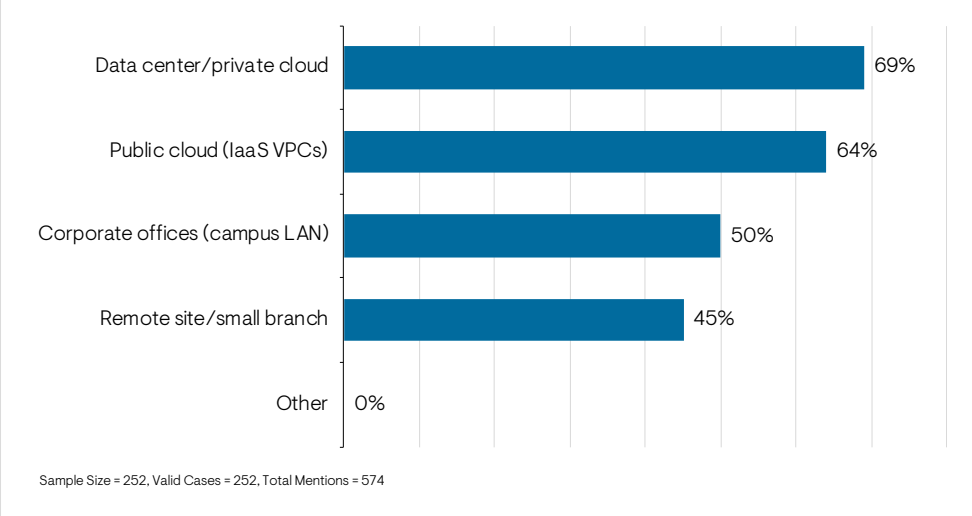

Figure 19. Network domains in which Zero Trust network segmentation is applied

Exactly half of enterprises have implemented some form of Zero Trust segmentation in corporate offices, and a smaller number have extended it to remote sites and small branches. Manufacturers of IT products reported a higher rate (60%) of Zero Trust segmentation in remote sites and small branches.

Segmentation Technology

Enterprises have a variety of techniques available to them when implementing Zero Trust network segmentation. One option is to use a security appliance as a gateway, where all traffic between segments is routed through the appliance like a firewall. Policies on the firewall can allow or disallow traffic. This method is effective, but it can create a bottleneck in environments with large volumes of east-west traffic. Some IT organizations will have to make a significant investment in an appliance with enough capacity to support the number of network flows that might pass through the device.

Another option is to configure segments on the network using Layer 2 or Layer 3 features, such as VLANs or routing zones. These methods are usually reliable, but they can be limited by issues of scale and network management complexity.

Finally, enterprises can use newer software solutions for segmentation. Hypervisors in a data center or cloud can provide a foundation for software-based segmentation schemes through virtual network overlays or distributed virtual firewalls. Some vendors also support segmentation by installing agents on hosts and enforcing segmentation between each host.

Figure 20 reveals what enterprises are using to enforce segmentation boundaries today. The most popular technique is a secure appliance gateway. Hypervisor solutions, such as network overlays, are used by a majority. Security professionals (43%) are less likely than infrastructure professionals (57%) to favor this technique. Host-based and Layer 3-based solutions are used by less than half of companies. Layer 2 techniques are the least popular.

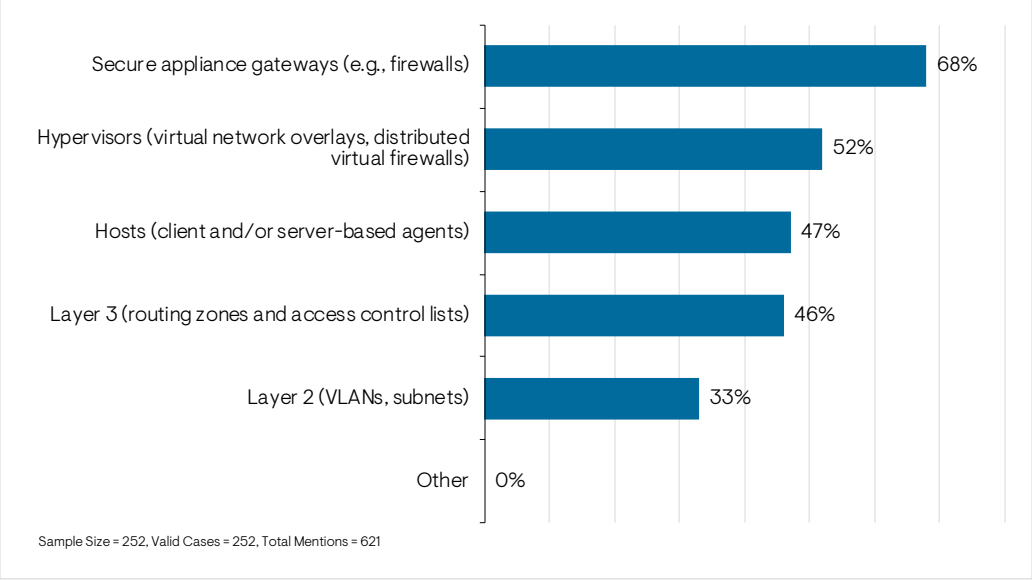

Figure 20. Technologies used to enforce Zero Trust network segmentation boundaries

Segmentation Management and Control

Like Zero Trust remote access solutions, Zero Trust segmentation technology requires a policy framework to govern whether network communication is allowed. That policy engine can live on the enforcement point, such as a firewall appliance. However, if a segmentation scheme uses multiple enforcement points, a central policy engine can improve scale and reduce complexity. In this research, EMA found that 91% of enterprises require a central policy engine for their Zero Trust segmentation. **Figure 21** shows that 54% of enterprises consider this policy engine to be critical to their success.

91% of enterprises require a central policy engine for their Zero Trust segmentation.

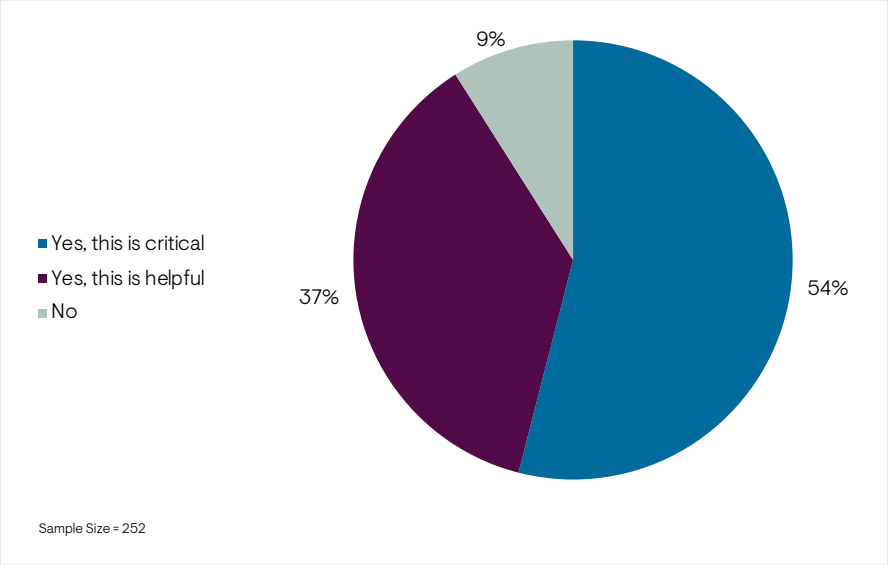

Figure 21. Do you require a central policy engine for your Zero Trust network segmentation solution to determine whether communications are allowed or disallowed?

Microsegmentation

Microsegmentation is a newer, more granular approach to network segmentation. It is often implemented by hypervisor-based or cloud-native segmentation technologies in data centers and cloud environments. Microsegmented network zones are often as small as an individual workload on a virtual machine or container. This level of granularity significantly reduces the ability for malicious activity to propagate on a network.

EMA asked survey participants whether they consider any of the Zero Trust segmentation in their network to be microsegmentation. **Figure 22** reveals that slightly more than half have microsegmentation in their networks today, and nearly 40% plan to have it in the future. Very large enterprises (66%) are the most likely to have this implemented already.

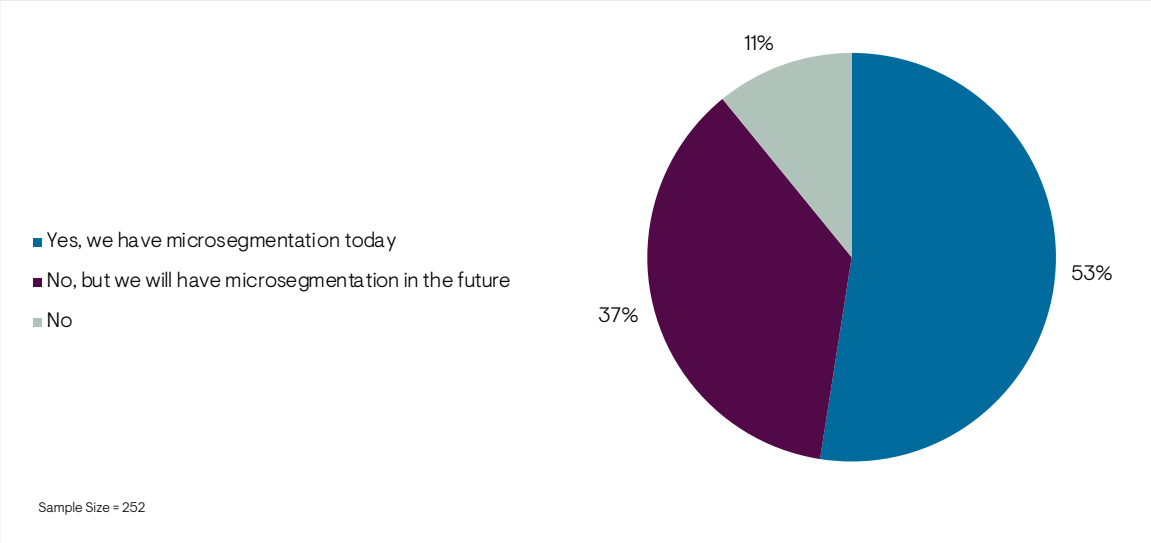

Figure 22. Do you consider any of the segmentation in your network to be microsegmentation?

Only 11% of enterprises have no microsegmentation plans, but this number is much higher among organizations that have taken an ad hoc Zero Trust networking (33%). Successful Zero Trust networking strategies are most likely (60%) to have microsegmentation implemented already, versus only 46% of somewhat successful strategies. Microsegmentation also appears to be a major factor in determining Zero Trust success.

Only 11% of enterprises have no microsegmentation plans.

Organizations that adopt hybrid cloud or multi-cloud architecture may need a microsegmentation solution that can span multiple environments. This will allow them to unify network and security operations across these architectures. **Figure 23** reveals that 92% of enterprises want this capability, and 58% consider it to be critical to their success.

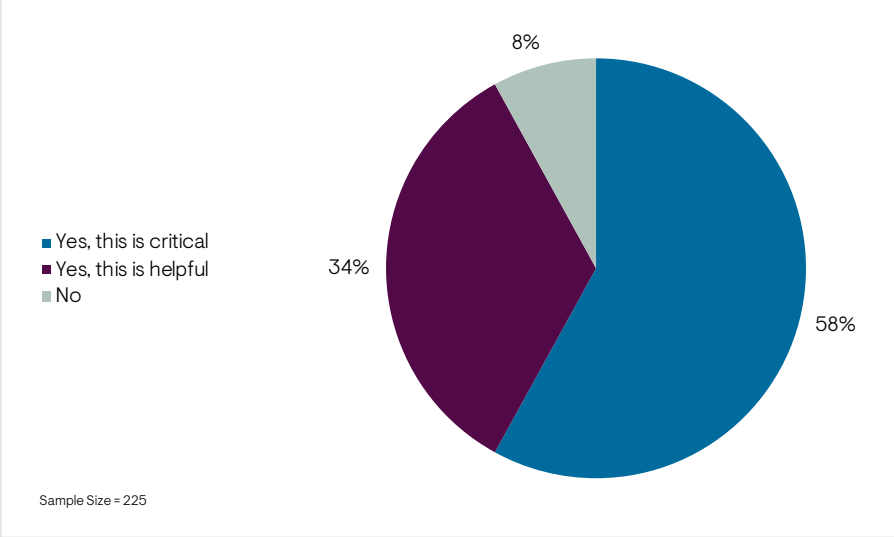

Figure 23. Do you require microsegmenation technology that can span multiple environments (e.g. On-premises data center and public cloud?

Successful organizations (70%) are the most likely to consider multi-domain microsegmentation critical, versus only 50% of somewhat successful organizations.

Unifying Zero Trust Network Segmentation and Remote Access

In most enterprises, the technology used to facilitate secure remote access is distinct from the tools and technology used to segment the network. In many cases, the teams responsible for these capabilities are separate as well. The engineers that manage the remote VPN solution are not the same as the engineers who implement microsegmentation in a private cloud. However, enterprises see value in the ability to unify these solutions.

Figure 24 reveals that 92% of enterprises want their remote access and network segmentation solutions to be integrated for coordinated Zero Trust control. Forty-nine percent say this is a critical requirement. Enterprises with successful Zero Trust networks are more likely (57%) to call this a critical need. Engineers and architects (62%) are also highly likely to consider this critical, versus 37% of executives.

92% of enterprises want their remote access and network segmentation solutions to be integrated for coordinated Zero Trust control.

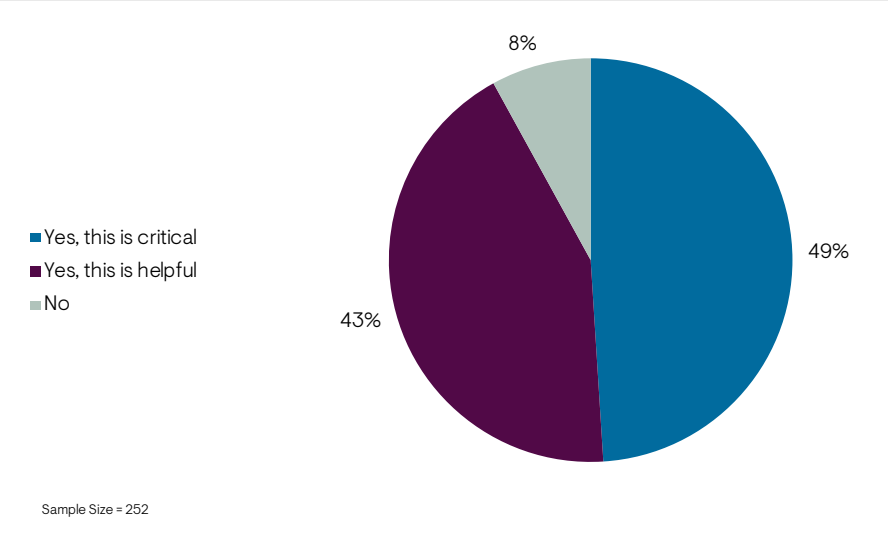

Figure 24. Does your organization require your network segmentation technology to integrate with your remote access solutions for more coordinated Zero Trust control?

Impacts of the COVID-19 Pandemic

At the time this survey was conducted (August 2020), the global COVID-19 pandemic was still severely affecting day-to-day business operations. As of the publication of this report, it remains so. EMA wanted to understand how the pandemic has affected Zero Trust networking initiatives, and we wanted to identify whether Zero Trust can help an enterprise mitigate the impacts of a pandemic.

The Pandemic Accelerated Zero Trust

Figure 25 reveals that the majority of enterprises accelerated their Zero Trust networking initiatives in response to the pandemic. Very few organizations actually slowed down their projects. However, enterprises that lacked a formal Zero Trust initiatives and took an ad hoc approach to implementation were the least likely to have accelerated their efforts during the pandemic (35%). Instead, they were more vulnerable to having to actually slow down their projects (35%), which presents a lost opportunity. Without a formal initiative, these organizations were sidetracked by other issues during the pandemic crisis.

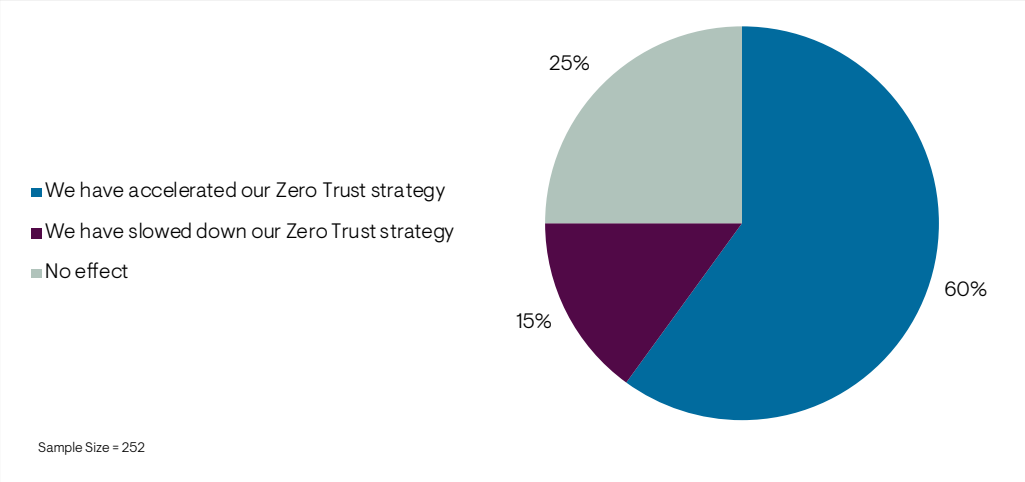

Figure 25. Did COVID-19 accelerate or slow down Zero Trust initiatives?

EMA believes that the best response to this pandemic is to be more aggressive with Zero Trust networking. Successful organizations were the most likely (69%) to have accelerated their projects.

Work From Home is the New Normal

It is self-evident that the pandemic has forced millions of people to work from home in order to maintain social distancing. EMA asked survey participants to measure this issue inside their organizations. They revealed how many of their end users had been connecting to their networks remotely prior to the pandemic, then how many are connecting remotely today. On average, the number of end users connecting remotely has nearly doubled during the pandemic to 62% of users, according to Figure 26.

On average, the number of end users connecting remotely has nearly doubled during the pandemic to 62% of users.

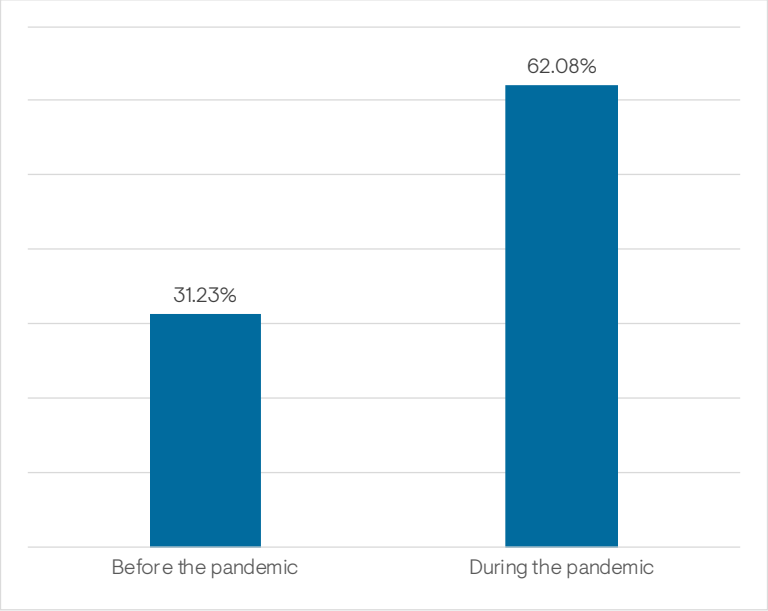

Figure 26. Percentage of end users who were primarily using secure remote access to connect to corporate networks and applications, before the pandemic versus now

The industries that saw the biggest increase in remote workers are education, finance, government, healthcare, professional services, and nonprofits.

Figure 27 reveals that larger populations of remote workers will remain even as pandemic restrictions ease. Only 42% of enterprises expect to return to pre-pandemic levels of remote work. More than half expect remote workforces to remain larger, with 27% saying it will remain much higher than it was.

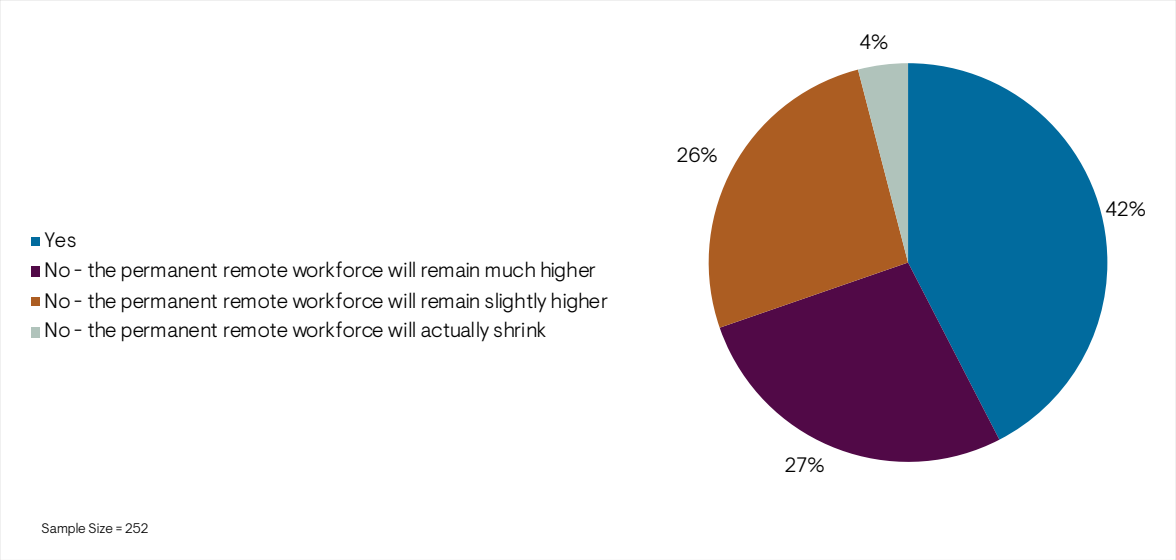

Figure 27. As pandemic precautions and work restrictions ease, will the size of your organization's remote workforce return to pre-pandemic levels?

Conclusion

This research reveals that the concept of Zero Trust network architecture has matured considerably, but it is not without its challenges. Budget and leadership are fundamental issues. EMA repeatedly found indications that enterprises are more successful when they add new line items to their budgets to support Zero Trust, rather than try to implement Zero Trust within existing budgets. Also, an informal Zero Trust initiative is more effective than an ad hoc approach, in which architects and engineers apply Zero Trust concepts on the fly when they can find time and resources. For instance, it appears that many ad hoc Zero Trust strategies were derailed by the COVID-19 pandemic, while formal initiatives with buy-in from IT executives were more likely to accelerate and enable the business during this pandemic.

EMA also found that Zero Trust networking is a partnership between networking and security. Both groups contribute budget to the endeavor, and the most successful projects are led by Zero Trust taskforces that pull experts from both groups. Successful enterprises indicated that one of the most important areas of Zero Trust collaboration is the coordination of access security controls across different systems, since security and networking teams often own complementary security technologies. EMA also found that the IT service management group contributes to Zero Trust budgets and that these budgets are expected to grow in 2021.

Remote access solutions and network segmentation solutions are both foundational to a Zero Trust network, and the majority of enterprises are investing in new technology to support this effort, while many will also retain their legacy solutions for a multi-layered approach to Zero Trust. EMA found considerable interest in secure access service edge (SASE) and microsegmentation as enablers of Zero Trust networks. Adoption of software-defined perimeter (SDP) solutions will also tick upward in the coming years.

Finally, the research revealed the following **best practices**:

- Adopt a dynamic policy engine that can respond to changing conditions and observed activity.
- Secure remote access to the public cloud is essential.
- Layer 7 remote corporate network access solutions are useful.
- Do not sweat legacy assets for too long. Successful enterprises are more willing to replace legacy secure remote access technology.
- Establish a central policy engine for segmentation.
- Be aggressive with microsegmentation if you have a requirement for it. It gives you more granular control inside the perimeter.
- Look for opportunities to integrate your segmentation and secure remote access solutions.
- Do not pause Zero Trust during the pandemic. These technologies will enable your business during adverse conditions.

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 or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
www.enterprisemanagement.com

4035.100720