



Enterprise Strategy Group | Getting to the bigger truth.™

ESG Research Insights Paper

Zero Trust Impact Report

How Organizations Prioritizing Zero Trust Segmentation Achieve Better Business and Security Outcomes

By John Grady, ESG Senior Analyst; and Adam DeMattia, Director of Research

June 2022

This ESG Research Insights Paper was commissioned by Illumio and is distributed under license from TechTarget, Inc.

Contents

Executive Summary	3
Even As Cyber Risk Widens, Many Do Not Treat Being Breached as Definitive.....	4
An “Assume Breach” Mindset May Be Lacking But Zero Trust Interest Continues to Grow	7
With So Much to Focus On, Prioritizing Where to Begin Can Be Difficult.....	7
The Criticality of Zero Trust Segmentation	8
Assessing Zero Trust Segmentation Maturity.....	8
Benefits Pioneers See Across the Stages of Zero Trust Segmentation.....	11
Visibility	11
Containment.....	12
Protection	13
The Bigger Truth	14
Appendix I: Research Methodology and Demographics.....	15
Appendix II: Survey Questions Used to Evaluate Zero Trust Segmentation Maturity.....	17

Executive Summary

The hyperconnectivity created by digital transformation among users, applications, data, and things massively expands the attack surface and increases risk. Seeking to exploit these trends, attackers use a variety of methods to compromise targets, often causing significant business disruption. To address these threats, many organizations have begun to implement Zero Trust architectures to modernize their cybersecurity programs and attempt to limit the impact of attacks.

Yet, despite the prevalence of Zero Trust and likelihood of suffering an attack, nearly half of organizations (47%) do not operate under the assumption that they will be breached. Further, the breadth of tools supporting Zero Trust can make it difficult to determine where to begin and correctly focus on these initiatives. This has led to important practices that prevent attackers from having unfettered access to corporate resources when compromises inevitably occur, such as segmentation, to become overlooked and points to a clear disconnect between the need, interest, and proper application of Zero Trust.

Despite the prevalence of Zero Trust and likelihood of suffering an attack, nearly half of organizations do not operate under the assumption that they will be breached.

To gain insight into how organizations are faring with their Zero Trust initiatives and, specifically, how the maturity of an organization's approach to Zero Trust Segmentation impacts both security and business objectives, Illumio commissioned the Enterprise Strategy Group (ESG) to conduct a global research survey of 1,000 organizations located in North America, Europe, and Asia Pacific and Japan. Based upon the research conducted in this study, ESG concludes that organizations that have progressed further down the path of Zero Trust Segmentation enjoy the following benefits:

- **Improved visibility across hybrid multi-cloud environments.** Understanding the assets across the environment, how they relate, and where the greatest risks reside is foundational to Zero Trust. Mature organizations were 4.3 times more likely to say they have comprehensive visibility into traffic across their environment and five times more likely to have comprehensive visibility into traffic across all types of application architectures.
- **Significantly lower annual downtime costs.** Attacks are bound to occur. Ensuring the response to these incidents is fast and accurate is critical. Mature organizations were twice as likely to have avoided a critical outage due to an attack over the last 24 months and boasted a 68% faster mean time to recover (MTTR). By avoiding critical outages and recovering more quickly when attacks do occur, these organizations enjoy a \$20.1 million advantage in the annual cost of downtime.
- **Better operational results.** Mature organizations were able to translate success with Zero Trust Segmentation into broader business results. These organizations will move 14 production applications to the cloud over the next year that they otherwise wouldn't due to a lack of confidence in their security. They also report freeing up an average of 39 person-hours per week in their security teams due to increased operational efficiencies enabled via Zero Trust.
- **Confidence in preventing cyber disasters.** Following an attack, seconds can mean the difference between an inconvenience and a disaster. Mature organizations were 2.7 times more likely than their counterparts to have highly effective attack response processes. As a result of better visibility, faster response and containment, and more Zero Trust success, mature organizations are more than twice as likely to feel prepared to handle cyberattacks and reported preventing an average of five cyber disasters annually.

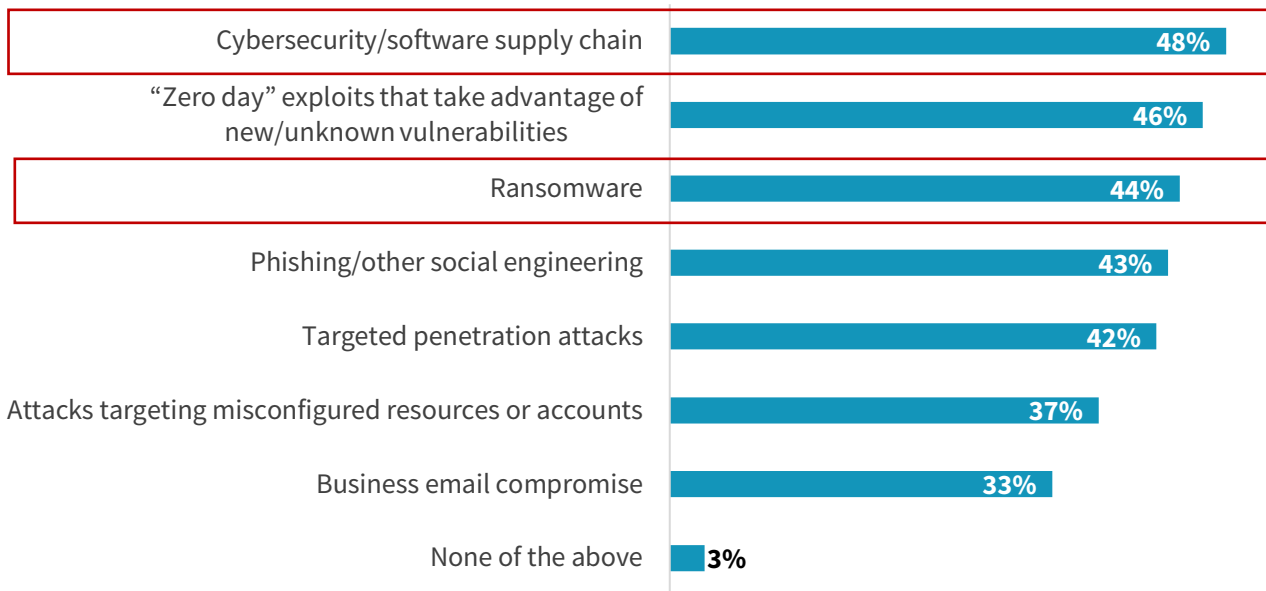
Even As Cyber Risk Widens, Many Do Not Treat Being Breached as Definitive

Digital transformation (DX) continues to be a top IT priority for many organizations. Yet, while DX initiatives can help drive greater operational efficiency, foster improved collaboration, and provide better customer experiences, they often result in greater environmental complexity. Specifically, DX creates hyperconnectivity among users, applications, and things across on-premises data centers, cloud infrastructure, and remote locations. The result is a hybrid, multi-cloud architecture that expands the attack surface and ultimately increases risk to the organization.

Attackers seek to exploit the complexity these hybrid environments create and have a variety of tools at their disposal with which to do so. Traditional attacks using malware, targeting misconfigurations, and exploiting stolen credentials continue to pose problems. However, software supply chain, zero-day exploits, and ransomware attacks have become increasingly concerning due to both their frequency and significant impact across organizations of all types (see Figure 1).

Figure 1. Most Concerning Types of Attacks

Regardless of the malicious activity you have seen over the last 24 months, which type of attacks are you personally most concerned about moving forward? (Percent of respondents, N=1,000, multiple responses accepted)



Source: ESG, a division of TechTarget, Inc.

Respondents are experiencing these types of attacks, with 66% having reported experiencing at least one supply chain attack over the past 24 months, and 76% at least one ransomware attack over the same timeframe. Ransomware incidents are particularly challenging as they test an organization’s cyber, and thus business, resilience. The compromise of business-critical data or the unavailability of mission-critical systems can result in loss of revenue, impact to brand reputation, and potential societal implications. The decision on whether to pay the ransom can be difficult and

More than one-third of respondents indicated a ransomware attack resulted in their data and systems being held hostage; 82% ultimately paid the ransom, the average of which was \$495,000.

must balance the financial implication of the payment itself, the cost of not paying, the potential of “rewarding” attackers and being exploited again, and the public perception that can follow a ransom payment. More than one-third of respondents indicated a ransomware attack resulted in their data and systems being held hostage. Among those who had

data and systems held hostage, 82% ultimately paid the ransom (42% directly and 40% via cyber insurance), the average of which was \$495,000. All these factors have pushed ransomware into the mainstream, with executives, board members, and the government all taking a more active role in ransomware prevention, response, and recovery planning.

Regardless of the type of attack, there are substantial impacts that follow. Typically, successful attacks result in systems becoming unavailable. Amazingly, 43% of respondents reported that they typically suffer unplanned downtime of a business-critical application due to a cyberattack at least monthly. The cost of these outages makes that finding even more noteworthy, with respondents indicating that the average hourly cost of downtime for a typical business-critical application due to lost revenue and productivity was \$251,000.

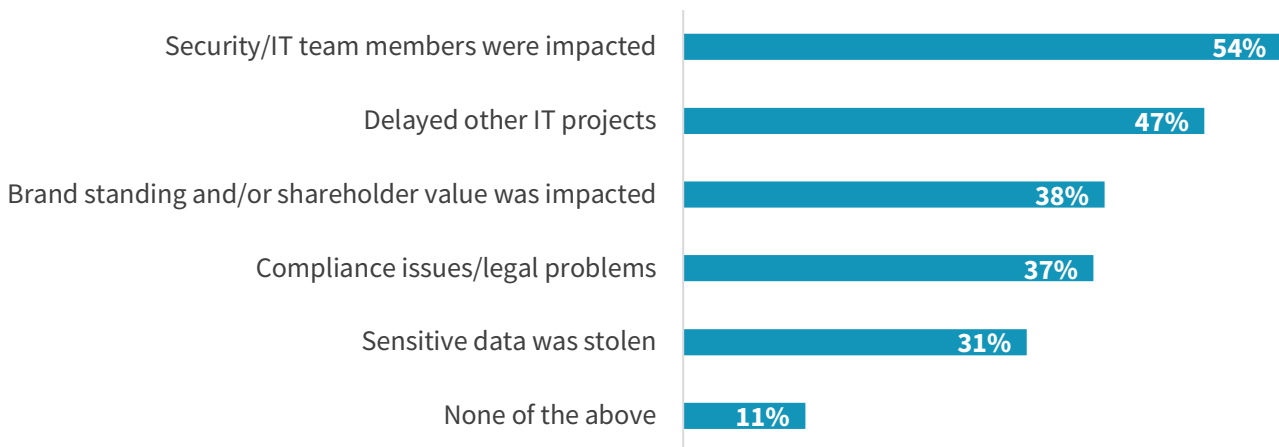
43% of respondents reported that they typically suffer unplanned downtime of a business-critical application due to a cyberattack at least monthly.

Additionally, substantial personal and business impacts can result (see Figure 2). These impacts can affect:

- **People.** Over half of respondents (54%) reported security or IT team members were impacted, which could range from having their workload increase due to an attack, to having their responsibilities changed, up to reassignment or termination.
- **IT.** Nearly half of respondents (47%) noted other IT projects were delayed. Attacks force teams to focus on the tactical rather than the strategic and can lead to delays.
- **Business.** Thirty-eight percent of respondents noted that brand standing or shareholder value was impacted following an attack, while 37% reported compliance or legal issues.

Figure 2. Attack Impacts

Beyond the direct cost of downtime, in what other ways has your business been impacted by ransomware, software supply chain, or other attacks experienced over the last 24 months? (Percent of respondents, N=1,000, multiple responses accepted)



Source: ESG, a division of TechTarget, Inc.

Perhaps due to the range of impacts they may face following an attack, many respondents are pessimistic about their organization’s resiliency in the event of an attack. When asked of their mindset when a cyberattack is discovered by the

security team, less than one in five (19%) feel their organization is prepared to handle the impacts of the incident. Further, more than half (52%) indicated they believe a cyberattack is likely to be a disaster for their organization (see Figure 3).

Figure 3. More than Half of Respondents Believe a Cyberattack is Likely to Be a Disaster



Source: ESG, a division of TechTarget, Inc.

An expanding attack surface, high likelihood of being attacked, and the negative impacts an attack can create have resulted in significant cyber risk for most organizations. However, nearly half of respondents (47%) do not operate with an “assume breach” mindset (see Figure 4). This indicates that most organizations have neglected to build enough cyber resilience to deal with the inevitability of a cyberattack, instead putting their hope in anonymity and keeping their fingers crossed that attackers will pass them over—an unlikely expectation.

Figure 4. Nearly Half of Respondents Do Not Operate With an “Assume Breach” Mindset



Source: ESG, a division of TechTarget, Inc.

An “Assume Breach” Mindset May Be Lacking But Zero Trust Interest Continues to Grow

In large part because of the erosion of the perimeter due to digital transformation and the resulting expansion of the attack surface, many organizations are turning to Zero Trust strategies. At its core, the Zero Trust model calls for denying access to applications, resources, and data by default and relies on three core principles: all entities are untrusted until verified, least privilege access is enforced, and comprehensive security monitoring is implemented. Among the study’s respondents, 85% said they had implemented or were in the process of implementing Zero Trust at their organization. More tellingly,

90% of respondents indicated that advancing Zero Trust is one of their organization’s top three cybersecurity priorities.

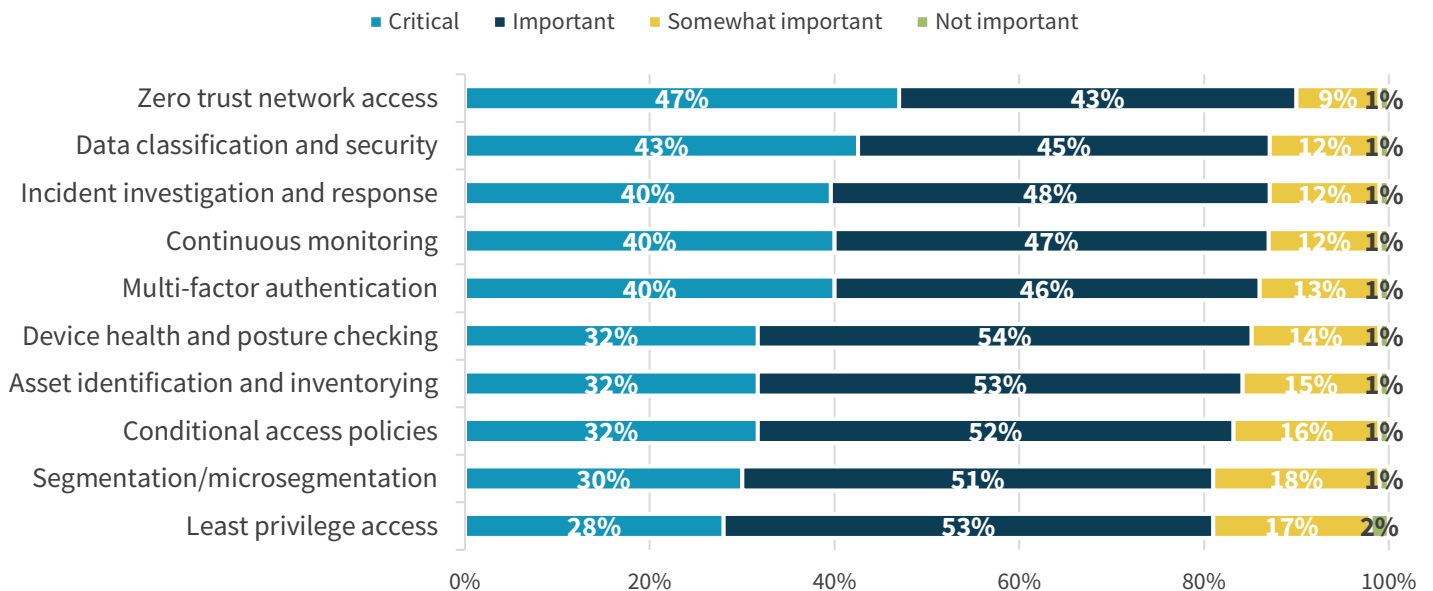
nearly all see this as a critical cybersecurity initiative. Specifically, 39% of organizations’ forward-looking annual budgets for security controls are aimed at advancing Zero Trust initiatives and 90% of respondents indicated that advancing Zero Trust is one of their organization’s top three cybersecurity priorities, with 33% citing it as their top cybersecurity priority.

With So Much to Focus On, Prioritizing Where to Begin Can Be Difficult

While Zero Trust should be thought of as a strategy or framework upon which to base a cybersecurity program, tools are required to support the initiative. Because Zero Trust is a broad initiative touching on a variety of disciplines, many tools have become associated with the strategy. While not an exhaustive list, Figure 5 shows how respondents rate specific tools and practices with regard to supporting Zero Trust. Because everything seems to be important, organizations can struggle to prioritize and focus on the appropriate areas. For example, 30% of respondents rated segmentation as critical to their Zero Trust initiative. If the purpose of Zero Trust is ultimately to prevent attackers from having unfettered access to corporate resources when compromises inevitably occur, this would seem to be a massive disconnect and potentially a consequence of organizations failing to operate under an “assume breach” mindset. Perhaps as a result, less than half of the respondents surveyed (46%) ultimately graded their organization’s Zero Trust initiative as very successful.

Figure 5. Importance of Technologies and Practices to Zero Trust

How important are each of the following technologies or practices to your organization when it comes to supporting zero trust initiatives? (Percent of respondents, N=1,000)



Source: ESG, a division of TechTarget, Inc.

The Criticality of Zero Trust Segmentation

Proper segmentation of resources is an important aspect of security independent of Zero Trust but is foundational to ensuring that entities are isolated from one another and only allowed to communicate when allowed by corporate policy. Yet moving from open to highly segmented is not something most organizations accomplish overnight. Rather, there should be a focus on specific actions which helps move an organization from a reactive stance to a proactive posture and down a path of fast wins and quick value before ultimately achieving Zero Trust Segmentation. These include:

- **Visibility** – The first step in defending a highly heterogeneous and distributed environment is understanding what comprises it. Comprehensive visibility across all application types, locations, and endpoints is the first step but must be put in the context of risks from open ports, unnecessary communication between applications, and other factors.
- **Containment** – Attacks will happen, so the ability to pivot quickly to response and prevent attackers from moving laterally and infecting additional systems is critical. This requires integrations with SIEM and SOAR tools to plug into existing workflows, as well as tools and processes able to serve as an emergency response mechanism in the event of ransomware attacks by quickly closing the ports used to propagate attacks, quarantining infected systems, and isolating unaffected systems.
- **Protection** – The first step in moving from reactive to proactive is ensuring that unrelated environments are separated (such as development from production and IT from OT). Expanding these capabilities across the entire environment to apply segmentation to all applications, ring-fence high-priority resources, and prevent lateral movement anywhere in the environment in the event of an attack protects sensitive data and limits the impacts of an attack.

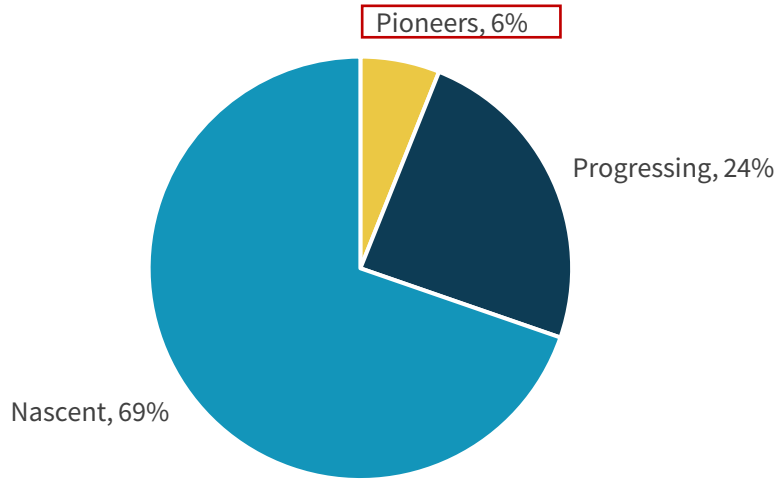
Assessing Zero Trust Segmentation Maturity

Respondents were asked five questions to assess their segmentation technology and practices relative to integrations with SIEM and SOAR solutions, separation of development and production environments, ability to block ports to stop the command and control traffic used to spread infections, consistency of policy enforcement across cloud and on-prem environments, and consistency of policy enforcement across different application architectures. Based on their responses, organizations were grouped into one of three cohorts based on Zero Trust Segmentation maturity (see Figure 6):

- **Nascent** – Organizations in the Nascent cohort use segmentation solutions that deliver very good capabilities across 0-2 areas (or the organization does not have a solution in place). A strong majority of organizations (69%) were grouped as Nascent. These organizations may still have work to accomplish with regard to Zero Trust Segmentation, but understanding the benefits the approach provides and best practices Pioneers employ can help them to prioritize areas of focus to refine their Zero Trust Segmentation approach over time.
- **Progressing** – Those grouped as Progressing use segmentation solutions that deliver very good capabilities across 3-4 areas. Roughly one-quarter (24%) of our respondents were Progressing toward Zero Trust Segmentation. These organizations are typically already seeing the benefits based on their work and have a solid foundation from which to continue to build.
- **Pioneers** – Pioneers are the most mature with regard to Zero Trust Segmentation and use segmentation solutions that deliver very good capabilities across all 5 areas. Unsurprisingly, few organizations have reached the third stage of Zero Trust Segmentation maturity, with only 6% able to be accurately described as Pioneers. Those identified as Pioneers can use this report within their organization to validate the advantages they can expect to see based on the benefits others in their group have seen.

Figure 6. Distribution of Zero Trust Segmentation Maturity

Respondents by Zero Trust Segmentation Maturity (Percent of respondents, N=1,000)



Source: ESG, a division of TechTarget, Inc.

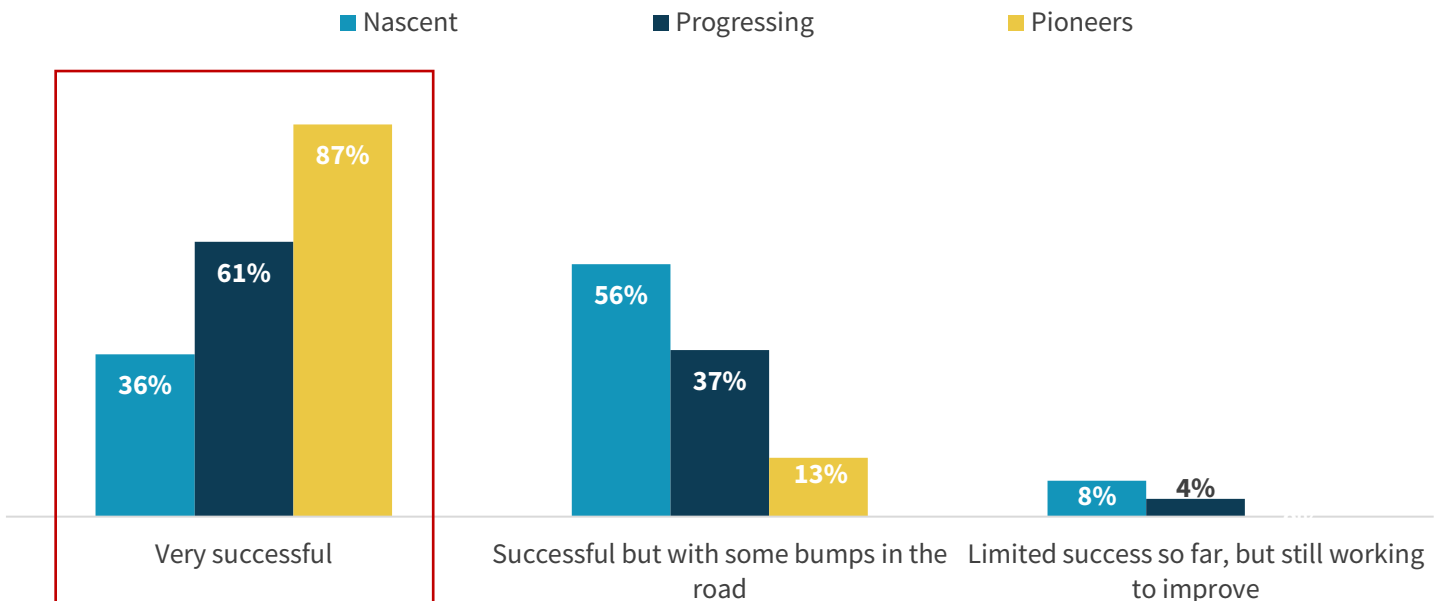
We will explore in depth the specific benefits those organizations that have prioritized Zero Trust Segmentation are seeing.

Yet at a high level, one of the first questions should be: Do organizations that are considered Zero Trust Segmentation Pioneers see more success with Zero Trust initiatives overall? In fact, they do. Specifically, Zero Trust Segmentation Pioneers were 2.4 times more likely than Nascent organizations to rate their Zero Trust initiatives very successful (see Figure 7).

Pioneers were 2.4 times more likely than Nascent organizations to rate their Zero Trust initiatives very successful.

Figure 7. Zero Trust Segmentation Pioneers Are More Successful with Zero Trust

Overall, how would you rate your organization’s level of success to-date with zero trust? (Percent of respondents)



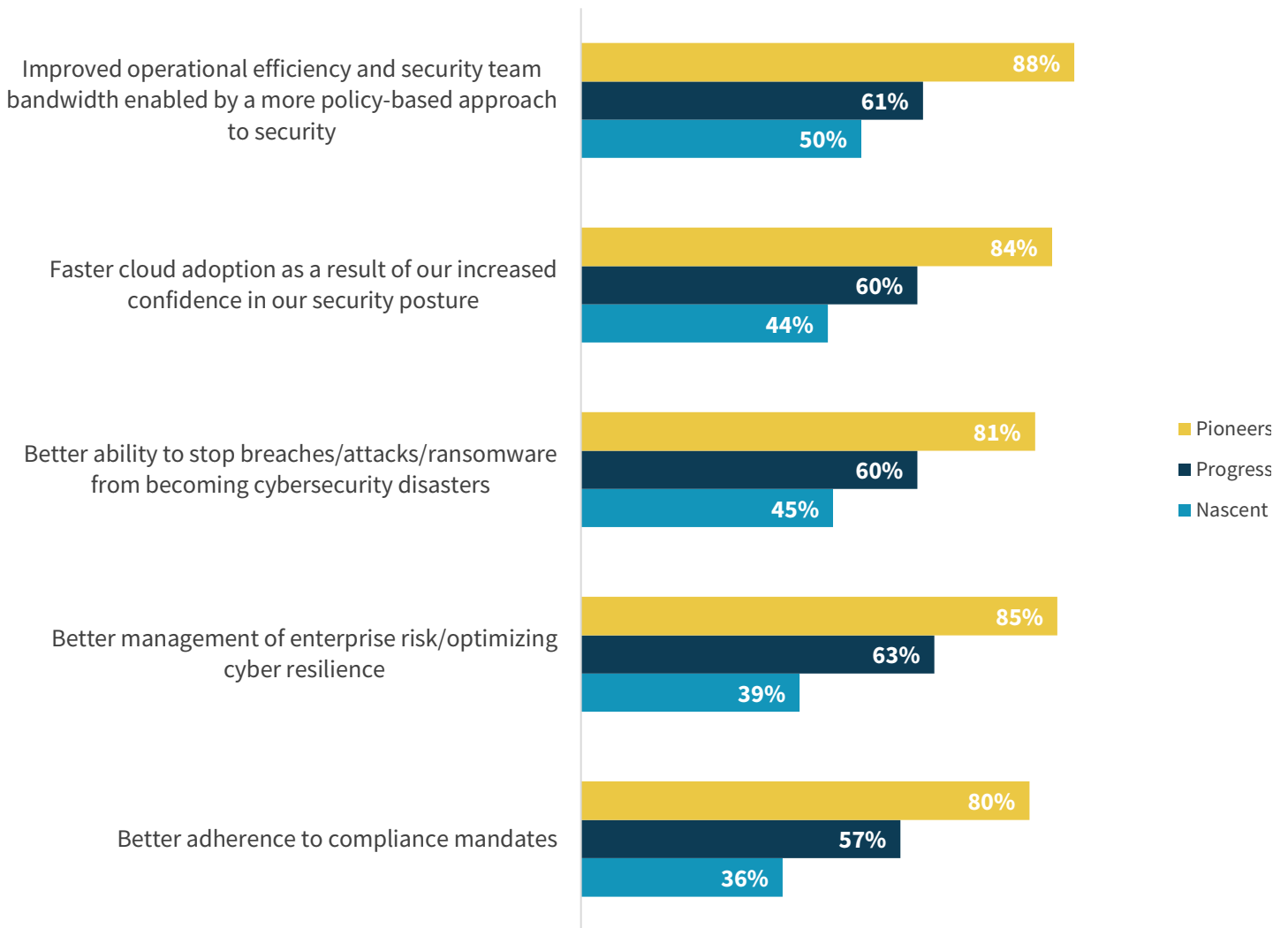
Source: ESG, a division of TechTarget, Inc.

More specifically, respondents made a clear connection between the application of segmentation in the environment and both the business and security benefits derived from Zero Trust (see Figure 8). Zero Trust Segmentation Pioneers were much more likely than their Nascent counterparts to indicate that investments in segmentation were critical to improving operational efficiency, accelerating cloud adoption, improving cyber resiliency, and meeting compliance mandates. Perhaps most importantly, 81% of Pioneers said their investments in segmentation were critical in helping them prevent breaches from becoming cyber disasters, compared to only 45% of their Nascent counterparts.

Perhaps most importantly, 81% of Pioneers said their investments in segmentation were critical in helping them prevent breaches from becoming cyber disasters, compared to only 45% of their Nascent counterparts.

Figure 8. Zero Trust Segmentation Pioneers Say Segmentation Has Helped Achieve Benefits

To what degree has your organization’s progress implementing segmentation/microsegmentation impacted broader zero trust benefits your organization has seen? (Percent of respondents selecting "Critical")



Source: ESG, a division of TechTarget, Inc.

Benefits Pioneers See Across the Stages of Zero Trust Segmentation

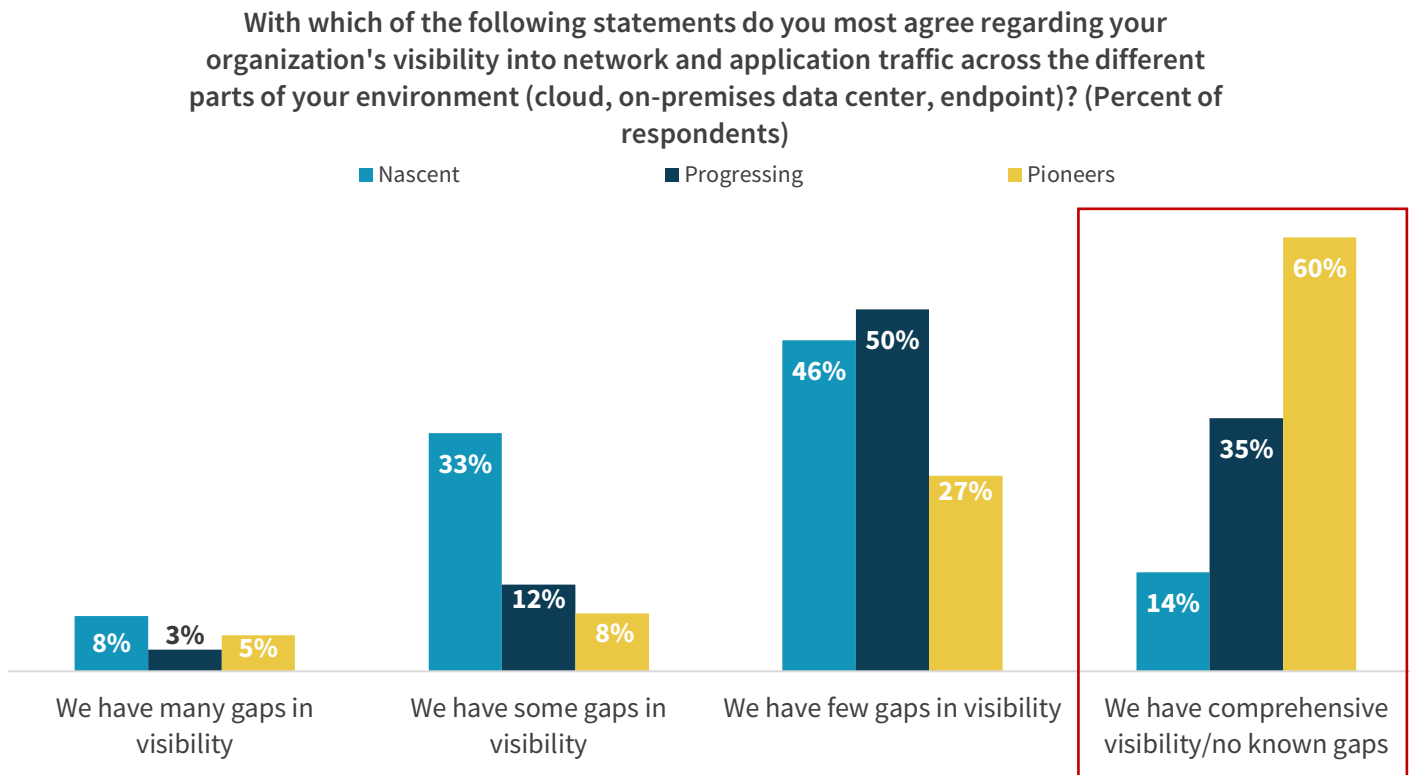
Organizations identified as Pioneers in our study saw clear and definitive benefits from their prioritization of segmentation across the stages of visibility, containment, and protection. Pioneers were at least 4.3 times more likely to report comprehensive visibility across their environment, reported a 68% faster mean time to recover, and saw a \$20.1 million annual cost of downtime advantage. As a result, Pioneers were 2.7 times more likely than Nascent organizations to feel prepared to handle cyberattacks and reported preventing an average of five cyber disasters annually. Put simply, Zero Trust Segmentation Pioneers are seeing success where much of the industry continues to struggle with adversity.

Pioneers were 2.7 times more likely than Nascent organizations to feel prepared to handle cyberattacks and reported preventing an average of five cyber disasters annually.

Visibility

Understanding the assets across the environment, how they relate, and where the greatest risks reside is foundational to Zero Trust. This has become both more important and more difficult with the shift to the cloud and adoption of cloud-native application architectures. Among our respondents, Zero Trust Segmentation Pioneers were 4.3 times more likely to report comprehensive visibility into traffic across their environment (see Figure 9). Similarly, Pioneers were 5 times more likely to have comprehensive visibility into traffic across all the types of application architectures in their environment. The confidence this visibility generates can have a tangible impact on broader IT initiatives as well. Among the Pioneer cohort, respondents expect to be able to move, over the next year, an incremental 14 production applications to the cloud that they wouldn't otherwise have had the confidence to do without Zero Trust.

Figure 9. Visibility Across Cloud, On-premises, and Endpoints



Source: ESG, a division of TechTarget, Inc.

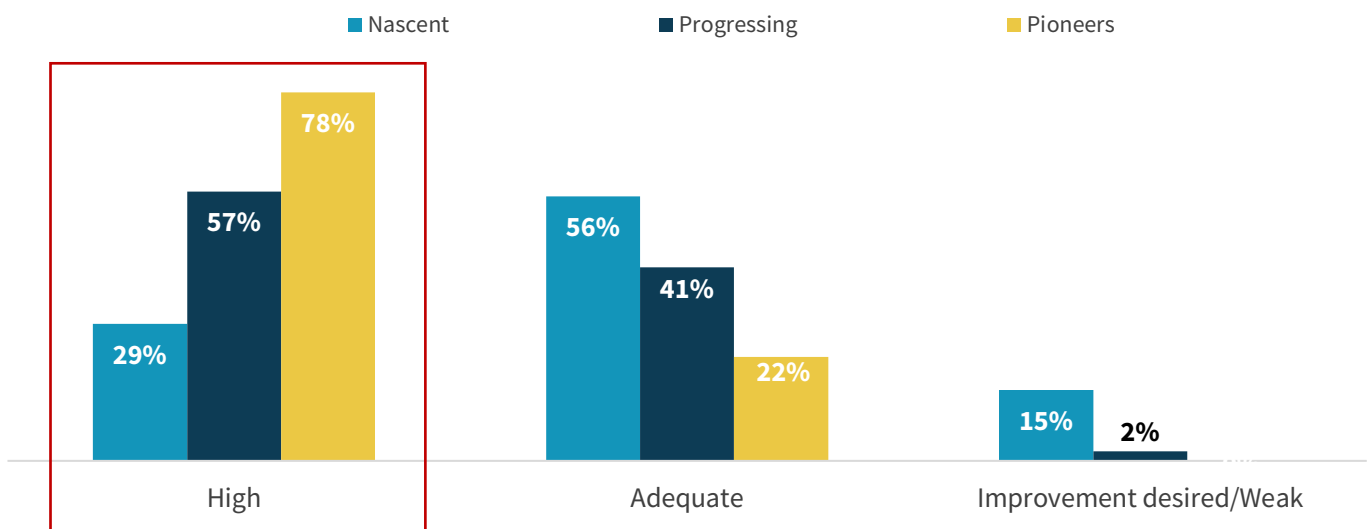
The assumption may be that Pioneers are bringing a multitude of tools to bear to achieve this type of success. Yet, in actuality, many are relying on a single tool for visibility insights. Specifically, 51% of Pioneer organizations use a single tool or primarily one tool for visibility across different parts of the environment and application architectures. This is two times more than their Nascent counterparts (25%). One benefit of this approach is the ability to democratize the insights derived from these insights across the organization more efficiently. Nearly two-thirds (65%) of Pioneers reported that application owners have their own views from the same visibility tool the security team uses, compared to only 36% of Nascent organizations. This ultimately supports a more proactive model when application owners are able to use these visibility insights to ensure their applications are secure earlier in the development cycle.

Containment

With attacks as common as they are, and the substantial personal and business impacts that often follow, fast and efficient response is critical. Our research found that Zero Trust Segmentation Pioneers were more than 2.7 times more likely to rate their attack response process as highly effective (see Figure 10). More objectively, we are able to validate how effective Pioneers are at containing cyberattacks through additional metrics they provided. With regard to mean time to recover, these mature organizations reported a 68% faster response than Nascent organizations, which helped them to avoid significant downtime. Specifically, Pioneers were 2.1 times more likely to have avoided a critical outage over the last 24 months. Most importantly, by averaging less downtime and recovering faster when incidents do occur, Pioneers ultimately see significant savings relative to the total annual cost of downtime, with a \$20.1 million advantage over their Nascent counterparts.

Figure 10. Effectiveness of Attack Response

In the event that an attack is detected at your organization, how would you describe the effectiveness in the process of quarantining systems, blocking lateral movement, and shutting down command and control communication paths? (Percent of respondents)



Source: ESG, a division of TechTarget, Inc.

A variety of considerations determine an organization’s ability to quickly respond to incidents when they occur. However, one of the most critical factors is the degree to which at least parts of the response are automated. The ability to instantaneously quarantine systems, shut down command and control communication paths by closing open ports, and ultimately prevent lateral movement gives responders a significant advantage against cyber-adversaries. Our research

found that 73% of Pioneers had highly automated attack response workflows, which was 2.5 times more likely than their less mature counterparts.

Protection

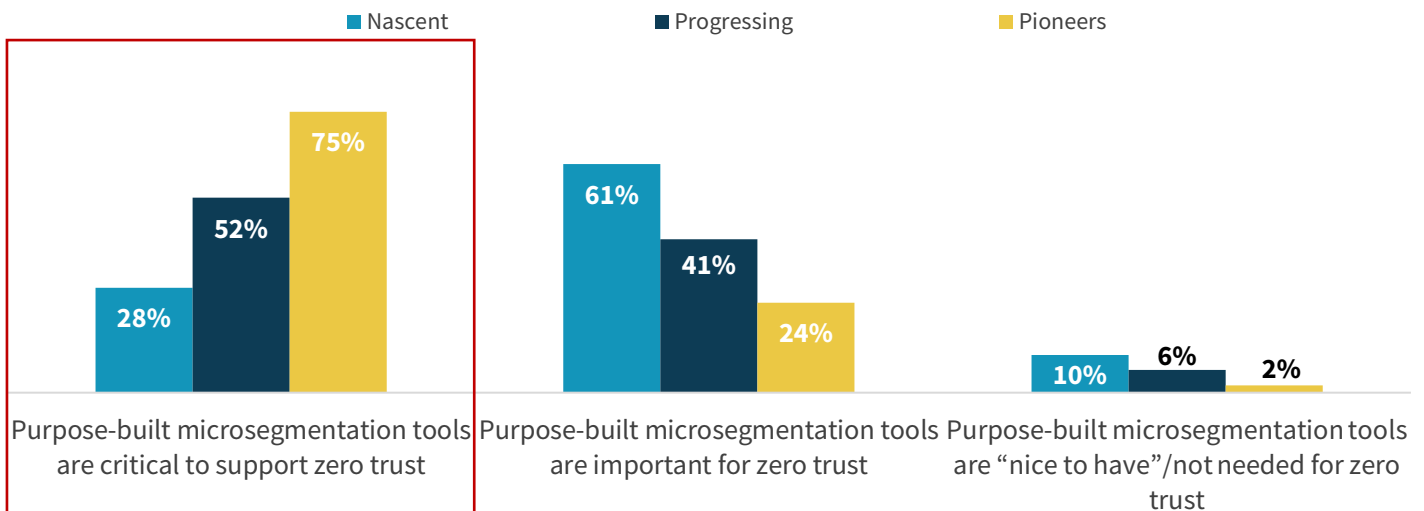
After achieving visibility and the ability to quickly respond to and contain incidents when they occur, the final stage on the Zero Trust Segmentation journey is achieving a proactively protective posture. This entails segmenting different parts of the environment and ensuring segmentation is applied to critical applications. As one would expect, Pioneers fared better than their Nascent counterparts in this area as well. Nearly all Pioneers (95%) rated their ability to separate their IT environment from their OT environment as very good. Conversely, only 38% of Nascent organizations felt this way. At an application level, Pioneers reported that 68% of their critical applications were ring-fenced, and 72% of their total applications were properly segmented. In both cases, this was a 26% advantage over Nascent organizations.

The knowledge that these key systems and applications are logically separated from other parts of the environment helps create confidence in the organization’s resiliency. This leads Pioneers to be 2.7 times more likely to feel prepared to handle a cyberattack than Nascent organizations. Further, Pioneers estimate that they avert 5 cyber disasters annually due to their Zero Trust Segmentation initiative. This confidence also generates greater efficiency, with Pioneers reporting an average of 39 person-hours per week freed up due to Zero Trust, nearly a full-person equivalent.

While applicable to each stage of the Zero Trust Segmentation journey, the use of purpose-built tools appears to play a significant role in an organization’s ability to achieve positive Zero Trust outcomes. From a broad Zero Trust perspective, only 4% of respondents voiced a preference for technologies that are part of a unified and integrated platform from a single vendor. Nearly half (49%) prefer purchasing tools and controls with best-of-breed capabilities from vendors with technology alliances and ecosystems, while 47% prefer purchasing best-of-breed tools even if they come with limited integrations. When it comes to Zero Trust Segmentation, these findings are even more pronounced, with 75% of Pioneers indicating that purpose-built microsegmentation tools are critical to Zero Trust (see Figure 11). The successes seen by these organizations begin to make sense in this context.

Figure 11. Preference for Purpose-built Microsegmentation Tools

With which of the following statements do you most agree with regarding the use of purpose-built microsegmentation tools (i.e., tools that are not part of a larger solution platform) to support a zero trust initiative? (Percent of respondents)



Source: ESG, a division of TechTarget, Inc.

The Bigger Truth

In some ways, the success of Zero Trust has bred fatigue for the term. Said another way, when everything is Zero Trust, is anything really Zero Trust? This is unfortunate because the core tenets of the approach are not only critical but fairly simple in reality: Never trust, always verify; continuously monitor; assume breach. The last point was clearly identified in our research as a major gap among many organizations and, in some ways, is the simplest to address: When organizations act as if a breach will occur, the objective should be to make it as hard as possible for attackers to move about the environment with impunity until they find valuable information. This quite clearly requires segmentation.

Beyond the logic of implementing segmentation because it is part and parcel of Zero Trust, our research has shown that organizations that have prioritized the practice and achieved Zero Trust Segmentation maturity are faring much better than those that have not across a multitude of security and business metrics. These mature organizations have more confidence, are more agile, and ultimately are more resilient in the face of adversity. This is not to say that segmentation has to be all or nothing. Simply by beginning the journey and gaining better visibility across the environment, organizations just getting started can begin to see benefits and build critical momentum toward expanding their capabilities and progressing toward maturity.

Appendix I: Research Methodology and Demographics

To gather data for this report, ESG conducted a comprehensive online survey of information security and IT professionals knowledgeable about their organization’s security priorities, technologies, and strategies. More than half of respondents (58%) held senior IT or security titles (i.e., CIO, CISO, VP of IT/IS or equivalent) while the remainder held middle management and staff titles. Respondents were distributed across North America (36%), Europe (32%), and Asia Pacific and Japan (33%). Respondents were employed at organizations with 500 or more employees. Specifically, 39% were employed at large midmarket organizations (i.e., those with 500 to 2,499 employees), and 61% at enterprise organizations (i.e., those with 2,500 or more employees). Respondents represented numerous industry and government segments, with the largest participation coming from manufacturing (27%), financial services (14%), technology (13%), retail/wholesale (12%), communications and media (7%), and healthcare (6%).

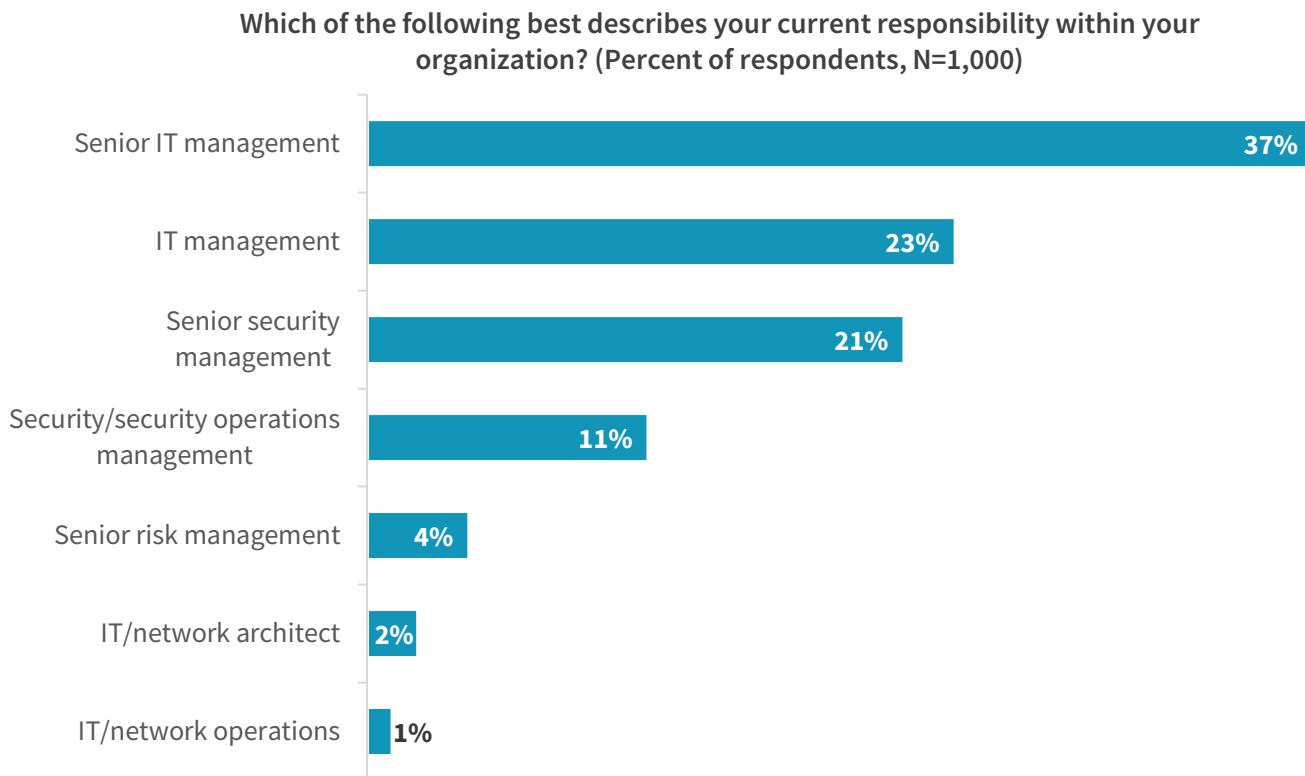
The survey was fielded in February 2022.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 1,000 respondents remained.

All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents. Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

Figures 12-14 detail the demographics of the respondent base: individual respondents’ roles, as well as respondent organizations’ total number of employees, annual revenue, and primary industry.

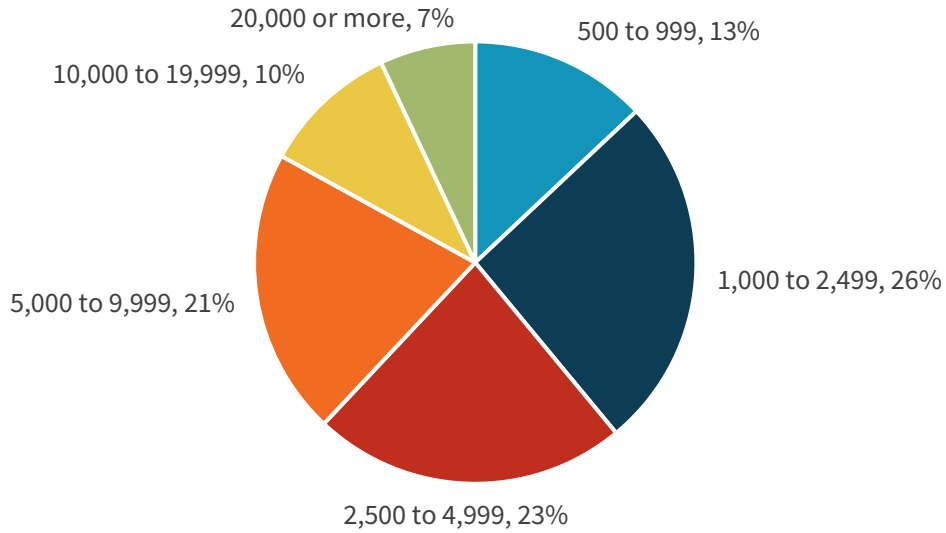
Figure 12. Survey Respondents, By Role



Source: ESG, a division of TechTarget, Inc.

Figure 13. Survey Respondents, by Company Size (Number of Employees)

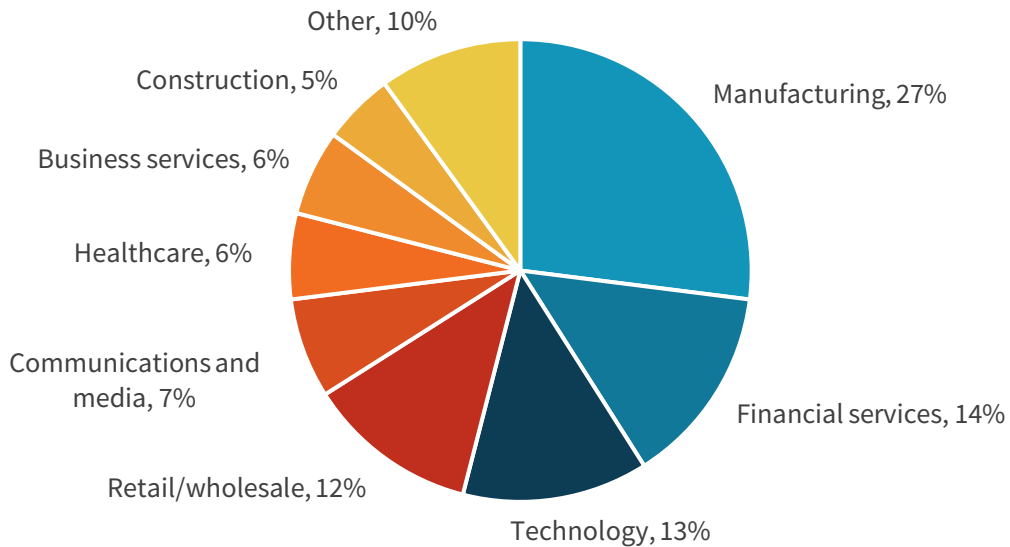
How many total employees does your organization have worldwide? (Percent of respondents, N=1,000)



Source: ESG, a division of TechTarget, Inc.

Figure 14. Survey Respondents, by Industry

What is your company's primary industry? (Percent of respondents, N=1,000)



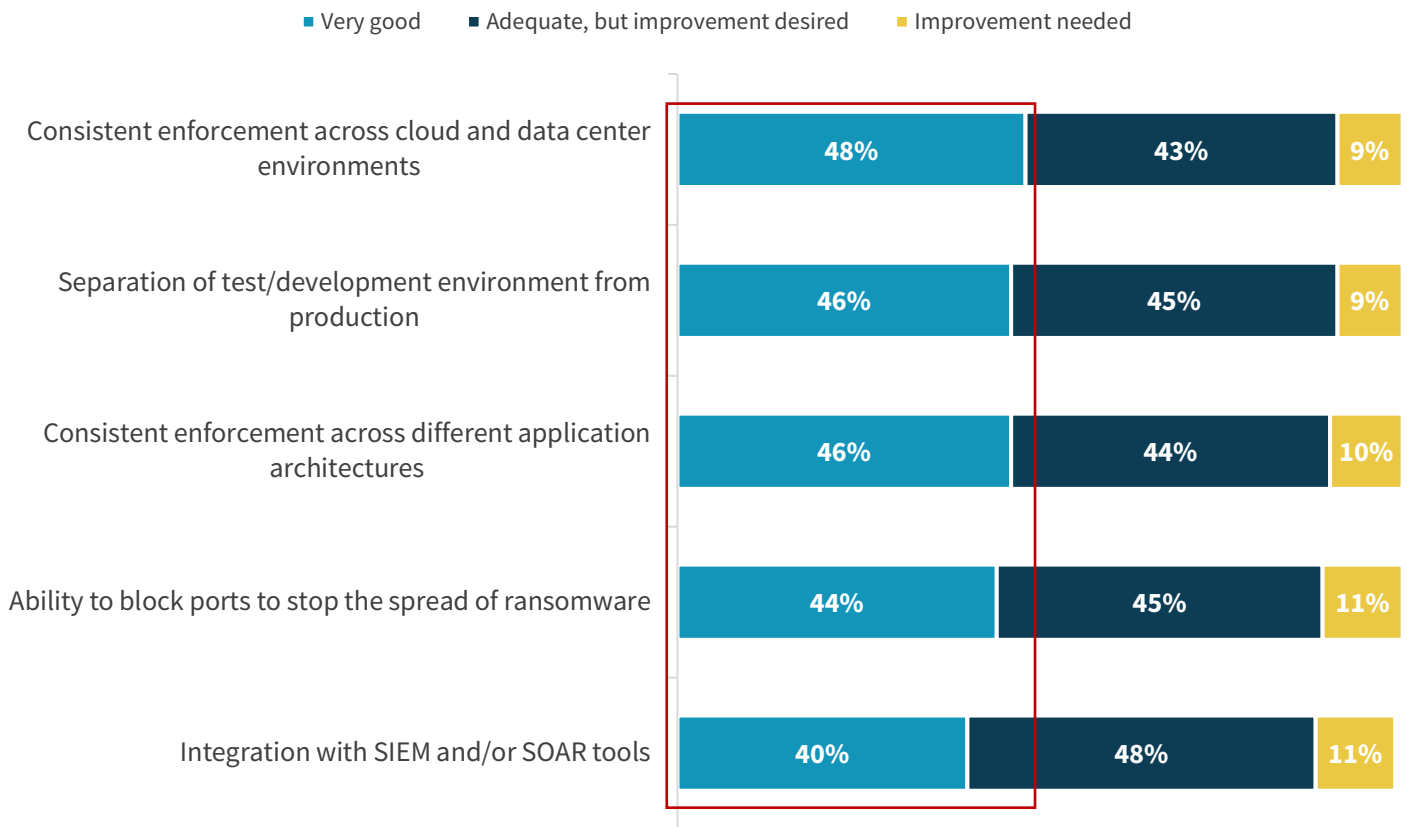
Source: ESG, a division of TechTarget, Inc.

Appendix II: Survey Questions Used to Evaluate Zero Trust Segmentation Maturity

ESG assessed the Zero Trust Segmentation maturity of organizations participating in the research survey based on their responses to five key questions about their segmentation tools and practices. Figure 15 details these questions, and the highlighted responses indicate those that ESG evaluated as most mature.

Figure 15. Zero Trust Segmentation Maturity Characteristics

Thinking about your organization’s segmentation/microsegmentation tools and practices, how would you rate its ability to support each of the following? (Percent of respondents, N=768)



Source: ESG, a division of TechTarget, Inc.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.


This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.



Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 508.482.0188