FORRESTER®

Trusting Zero Trust

Targeted Investment In Microsegmentation Fortifies Security In Clouds, Data Centers, And Workloads

A FORRESTER CONSULTING THOUGHT LEADERSHIP PAPER COMMISSIONED BY ILLUMIO, JANUARY 2022

Table of Contents

Project Director:
Vanessa Fabrizio,
Market Impact Consultant

Contributing Research:
Forrester's Security & Risk research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

Executive Summary

Companies are adopting Zero Trust (ZT) to strategically secure growth and digitally transform in the increasingly cloud-centric, work-from-anywhere world. During the past two years, organizations have turned to ZT to better navigate the "new normal" that arose from the COVID-19 pandemic. With threats mounting daily, it's time for firms to move beyond ZT planning and pilots. Delivering secure organizational agility and cloud migration support requires achieving scale with more mature ZT strategies, capabilities, and systems. Success depends on improving the ongoing ability to make a strong ZT business case to stakeholders and developing expertise around implementation of microsegmentation, which is a crucial technology foundation.

In September 2021, Illumio commissioned Forrester Consulting to explore the current state of Zero Trust strategies and microsegmentation. Forrester conducted an online survey of 362 security strategy decision-makers at firms in North America, EMEA, and APAC. We found that firms are leaning into Zero Trust as a key strategy in this new era and embracing microsegmentation as a cornerstone.

Zero Trust is an information security model moving from perimeter-based defense to minimizing trust by continuously verifying that access is secure, authenticated, and authorized.

Zero Trust Segmentation or Microsegmentation is fine-grained control of application needs, user access, and data repositories. Tools help automate, orchestrate, test, and implement granular policy across network security controls.

Key Findings

Firms are fighting to catch up with accelerated change. Sixty-three percent of respondents said their firm was unprepared for the quickened pace of cloud transformation and migration. An equal number found it difficult to maximize the productivity of remote workers without introducing new security risks. Decision-makers said they are constrained by overlapping and conflicting security frameworks and solutions and inadequate technology for today's new challenges.

Firms are counting on ZT and microsegmentation to better adapt to today's realities. More than three-quarters of surveyed decision-makers cited the importance of ZT to combat mounting security threats. However, ZT efforts at their organizations are in the early stages: Only about one-third said their firm's plans were in deployment, and just 6% said their firm's plan is complete. Encouragingly, two-thirds said their firm's ZT budget will increase next year, and more than one-third of their total spending in the area will go to microsegmentation.

Firms face business and implementation obstacles to fully realize benefits. For Zero Trust and microsegmentation initiatives to mature, organizations must dispel stakeholder notions that both are fads, and they must continue to develop and fine-tune business justifications, metrics, and deeper implementation capabilities and skills. Building on realized benefits (e.g., having better operational security, using more-defined security roadmaps) will help open pocketbooks and doors for next-level benefits.

Security Struggles With The New Normal

The global pandemic greatly accelerated the number of remote employees as well as cloud transformation efforts. Respondents said they recognize that Zero Trust is needed to keep up with security demands of new business realities. To succeed, firms must move beyond their current security solutions and continue to mature their ZT strategies. Forrester's survey found:

Nearly 70% of respondents' firms fight to safely support remote workers.

- **The new normal consists of cloud and device insecurity.** Nearly 70% of respondents said their firm has struggled to maximize the productivity of remote workers without exposing them or their devices to new risk. Seventy-five percent said they agree that to be better prepared, their firms must update their technical reference architectures for cloud security and ensure that ZT design principles are baked into cloud adoption and migration.
- **Zero Trust adoption is uneven.** Respondents said their firms are looking towards ZT to address new security gaps but that they are largely in the early stages of their Zero Trust journeys. Only 36% of respondents' organizations have started to deploy their solutions and just 6% have fully deployed their solutions (see Figure 2).
- **ZT approaches are maturing.** Current ZT approaches focus on networks, data, and devices, and firms use DC switches, firewalls, Zero Trust network access (ZTNA), or identity, credential, and access management (ICAM).

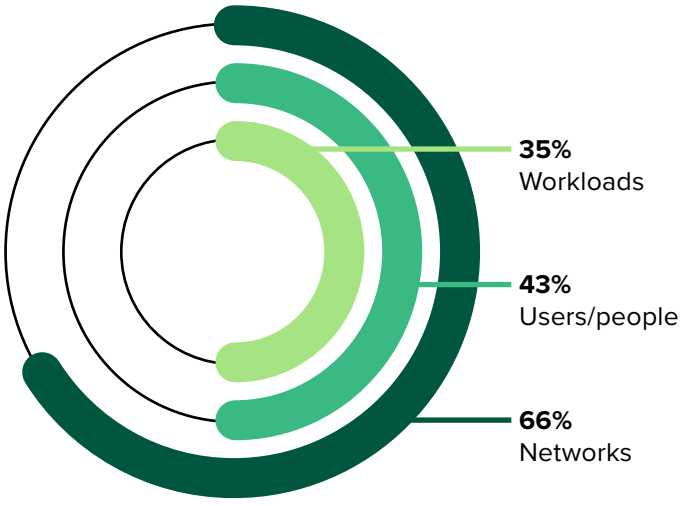
Recognition of the need for Zero Trust is growing, as 78% of respondents said their firm plans to enhance its Zero Trust security operations. Decision-makers indicated that securing workloads across traditional data centers, gaining complete visibility of their firms' cloud data centers, and ensuring Zero Trust segmentation controls are baked into cloud migration are all becoming more important.

- Microsegmentation is a key technology foundation. Respondents said their organizations currently use networking/ software-defined networking (SDN) and firewalls to execute their Zero Trust strategies but that those tools do not meet their firms' new security needs. They also acknowledged the need for their firms to use holistic Zero Trust architectures. Seventy-three percent said they consider microsegmentation and ZTNA to be critical technical foundations of their organization's ZT strategy.

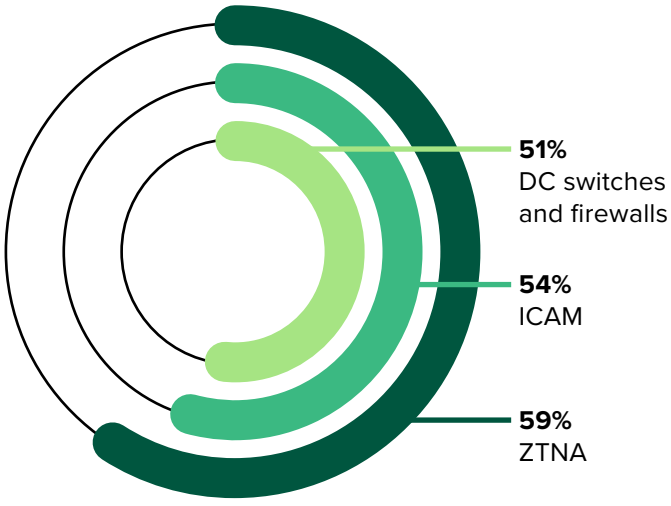
Roughly three-fourths of respondents said they consider microsegmentation to be a key technology foundation and that their firm plans to enhance Zero Trust security.

Figure 1

"Which of the following does your organization manage with a Zero Trust approach?"



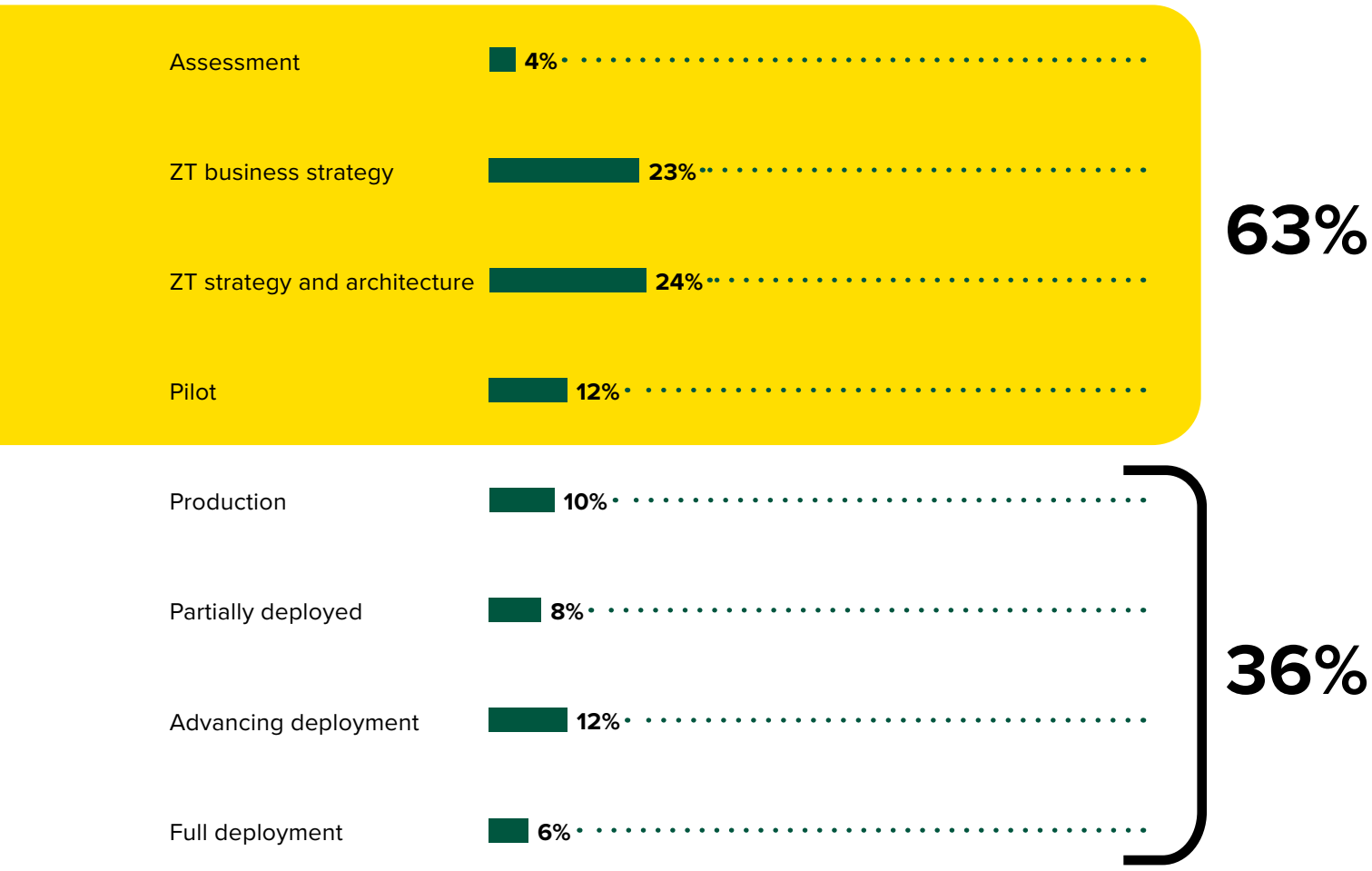
"What solution(s) does your organization use to enable Zero Trust segmentation?"



Base: 362 Zero Trust strategy decision-makers at large companies in NA, EMEA, and APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of Illumio, September 2021

Figure 2

"Where is your organization in its Zero Trust journey?"



Base: 362 Zero Trust strategy decision-makers at large companies in NA, EMEA, and APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of Illumio, September 2021

Lack Of Stakeholder Buy-In Leads To Various Implementation Challenges

Firms must continue advancing their Zero Trust programs from the early stages of development to wide deployment. And to do so, security teams need organizational support and funding. But 64% of respondents said their firm's security organizations struggle to secure the level of funding needed to advance their ZT projects, and 67% said stakeholders struggle to understand the business value of adopting microsegmentation.

The lack of buy-in has led to the following challenges:

- **Implementation expertise is in short supply.** Nearly two-thirds of decision-makers said their firm's internal teams lack the time, subject-matter expertise, and skills to implement best practices for microsegmentation. And the lack of implementation knowledge is painful. Sixty-two percent of respondents said their organization tried using a data center firewall and SDN, but that it took too long to deploy, 53% said it was too expensive, and 50% said their deployment didn't scale. Having expertise in implementation can increase efficiency and maximize ROI.

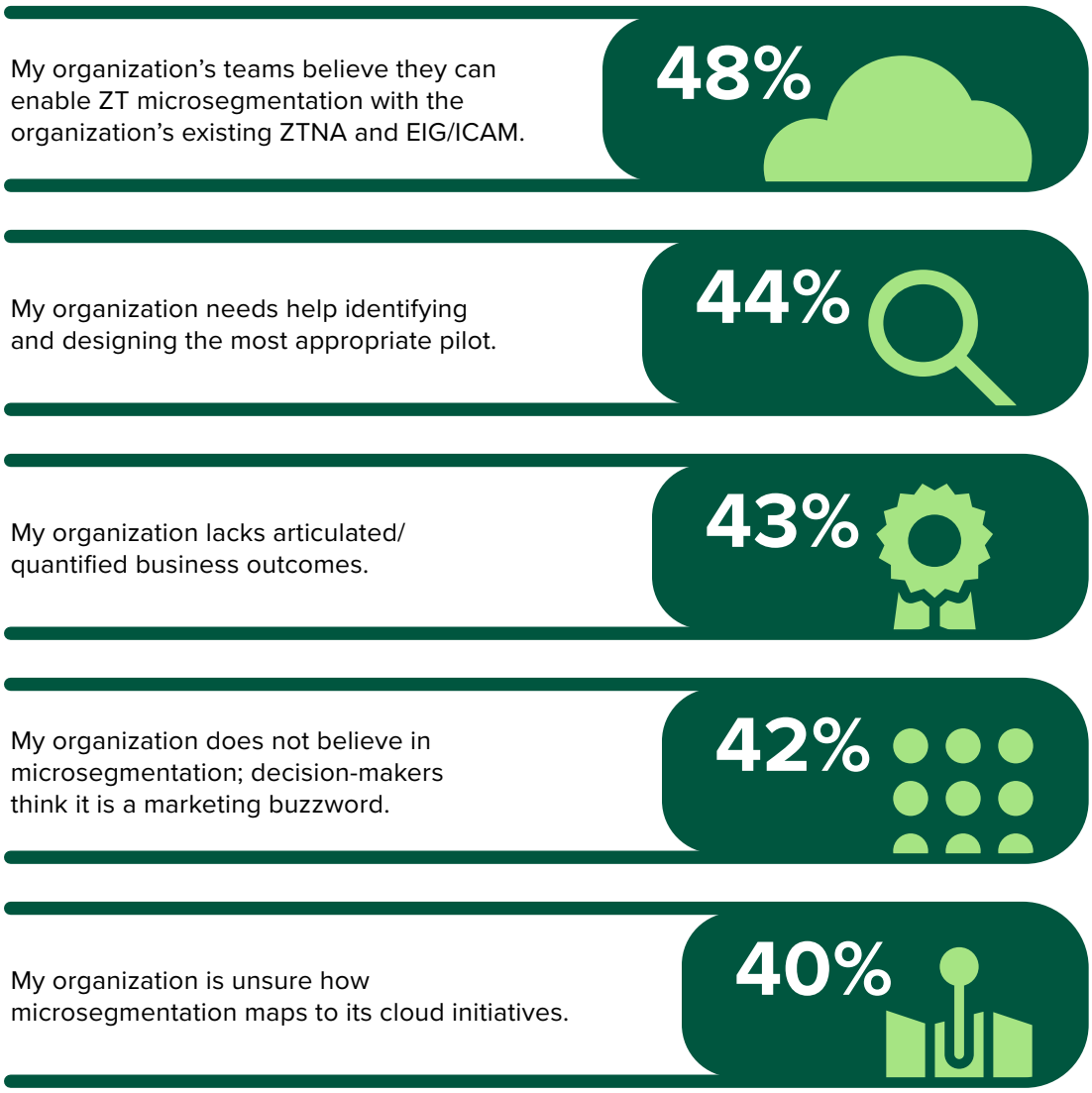
Overcoming obstacles with stakeholders and implementors is crucial for advancing beyond plans and pilots.

- **Firms struggle to identify the right ZT segmentation pilots.** Forty-four percent of respondents said their firm needs help identifying and designing the most appropriate ZT pilot. This is a crucial step in demonstrating business value and making the case for a greater investment to strengthen enterprise protection.
- **Security decision-makers struggle to articulate the value of microsegmentation.** The main challenges of implementing microsegmentation include teams believing they can implement the approach with their current ZTNA and EIG/ICAM networks, lack of

articulated/quantified business outcomes, and stakeholders assuming that microsegmentation is a buzzword. Security decision-makers know microsegmentation is valuable, but they have not successfully articulated that value to their organizational stakeholders.

Figure 3

"What was the most challenging aspect of implementing microsegmentation into your organization's Zero Trust strategy?"



Base: 362 Zero Trust strategy decision-makers at large companies in NA, EMEA, and APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of Illumio, September 2021

In Zero They Trust: Bigger Budgets And Benefits Ahead

To succeed in the new business landscape, every firm must have a strong ZT approach. Security decision-makers said they believe advanced ZT programs can provide increased organizational agility (52%), safer cloud migrations (50%), and support for digital transformation (48%). To accomplish these goals, organizations are investing and increasing their current investments. Forrester's research found:

68%

of respondents' firms plan to increase their Zero Trust investments, and 36% of overall spend in the area will go to microsegmentation.

- **Firms plan to increase their investments in Zero Trust.** Despite reported difficulties in obtaining funding, two-thirds of respondents said their firm will expand its ZT budget in 2022 and that it will allocate an average of 36% of the total spend in the area for microsegmentation.
- **Firms have realized benefits from ZT investments.** Respondents said their firms' Zero Trust strategies have yielded increased efficiency in security operations center (SOC) activity and allowed them to create well-defined cybersecurity roadmaps that align with their business data centers and cloud infrastructure strategies.
- **Decision-makers expect microsegmentation to deliver diverse benefits.** Respondents said they are counting on microsegmentation to help in a variety of areas crucial to the new business landscape, including making cloud and data center transformations (68%) and increasing support for new business and operational models (63%). Notably, respondents expect the technology to enhance their firms' abilities to proactively mitigate cyberattacks like ransomware and improve detection and threat hunting.

Figure 4

"You indicated that your organization is planning to adopt or has adopted microsegmentation. What were the top justifications for adopting microsegmentation at your organization?"

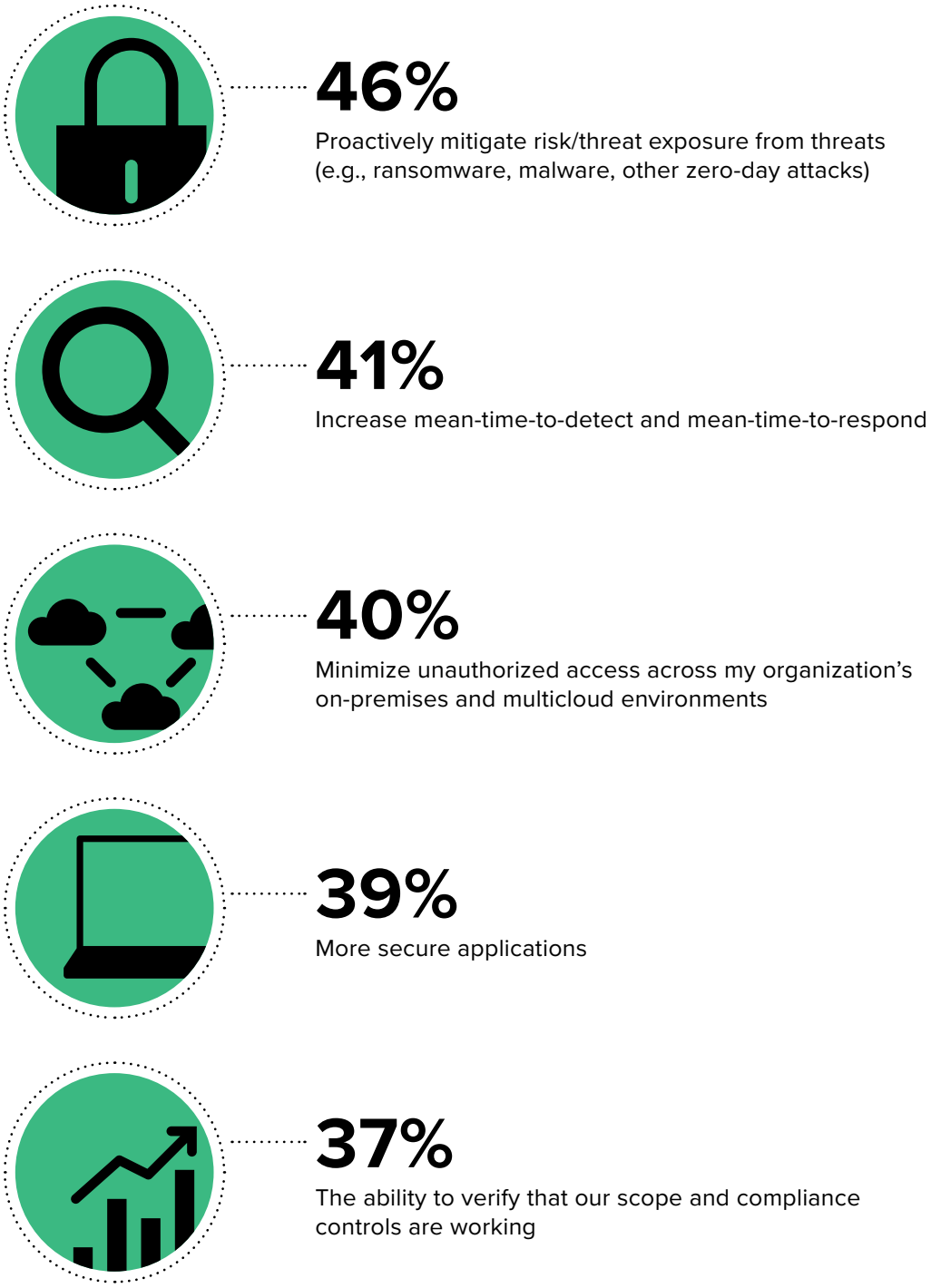
(Total Rank)

Base: 245 Zero Trust strategy decision-makers at large companies in NA, EMEA, and APAC that are implementing microsegmentation or planning to implement microsegmentation

Source: A commissioned study conducted by Forrester Consulting on behalf of Illumio, September 2021

Figure 5

“What benefits do you believe microsegmentation can bring to your organization’s Zero Trust strategy?”



46%

Proactively mitigate risk/threat exposure from threats (e.g., ransomware, malware, other zero-day attacks)

41%

Increase mean-time-to-detect and mean-time-to-respond

40%

Minimize unauthorized access across my organization’s on-premises and multicloud environments

39%

More secure applications

37%

The ability to verify that our scope and compliance controls are working

Base: 362 Zero Trust strategy decision-makers at large companies in NA, EMEA, and APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of Illumio, September 2021

Key Recommendations

Forrester's in-depth survey of 362 security decision-makers about Zero Trust yielded several recommendations:

Prioritize stakeholder buy-in.

To successfully implement ZT and microsegmentation, organizations need stakeholder buy-in. Respondents said they feel like they don't have the resources to advance their firms' ZT approaches, and they said they need the flexibility to hire experts internally and externally. Security decision-makers must show the value of ZT and microsegmentation by demonstrating how each provides a unique addition to their business.

Think holistically.

To ensure ZT implementation success, design a holistic Zero Trust architecture plan and an implementation strategy that account for current and future networking, compute, and cloud environments. This includes revising and updating Zero Trust roadmaps to ensure your firm has an all-encompassing approach.

Prioritize around business risk.

Where resources are constrained, prioritize microsegmentation activity around business-critical applications, but also consider running a proof of concept on noncritical network applications to gain expertise before taking on business-critical applications.

Beware analysis paralysis.

If your organization's current legacy network needs Zero Trust to increase its security posture, focus on solving this gap rather than trying to find a solution that also maps into the cloud. Networks in a public cloud have a different threat surface, different requirements, and different technological solutions. Choose a solution that solves your firm's specific on-premises network problems.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 362 decision-makers at large organizations in North America, EMEA, and APAC to better understand the issues and opportunities around microsegmentation and Zero Trust. Survey participants included decision-makers in C-level, vice president, and director roles. Respondents were offered a small incentive as a thank you for time spent on the survey. The study began in August 2021 and was completed in September 2021.

Appendix B: Demographics

TITLE	
C-level executive	**30%**
Vice president	**29%**
Director	**41%**

COMPANY SIZE	
500 to 999 employees	**3%**
1,000 to 4,999 employees	**49%**
5,000 to 19,999 employees	**30%**
20,000 or more employees	**17%**

REGION	
NA	**42%**
EMEA	**28%**
APAC	**30%**

DEPARTMENT	
IT	**78%**
Security	**22%**

INDUSTRY	
Government	**22%**
Technology/technology services	**14%**
Finance/insurance	**10%**
Retail	**8%**
Manufacturing and materials	**7%**
Electronics	**4%**
Healthcare	**4%**


FORRESTER®