Microsoft Security

hypothesis

Zero Trust Adoption Report

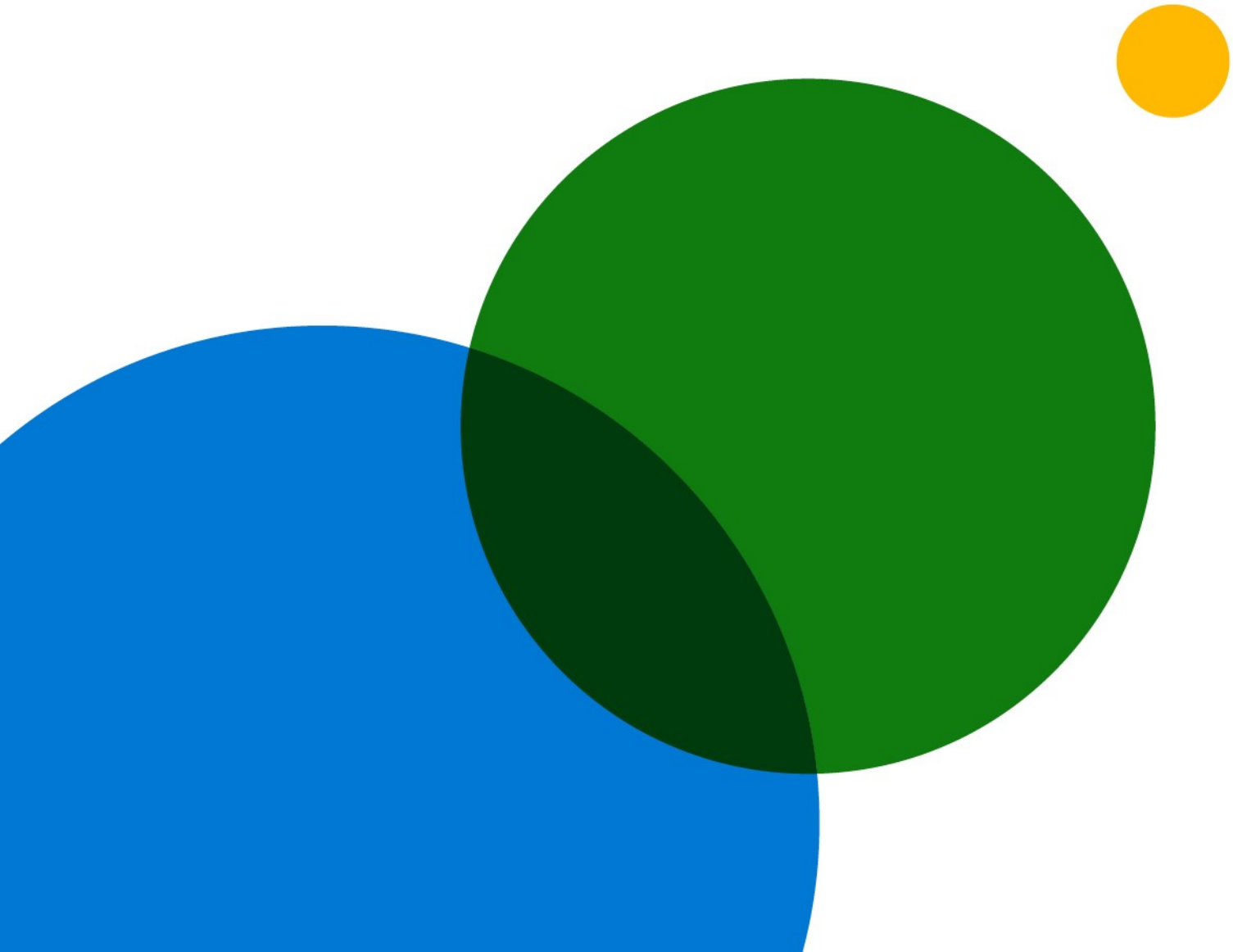


Table of Contents

03
Introduction

04
Methodology

05
Things to know about Zero Trust adoption

06
Who we talked to

07
Overall research learnings

24
Detailed research objectives & audience recruit

Introduction

Vasu Jakkal / Corporate Vice President, Security, Compliance and Identity

This past year has been remarkable in the evolution of cybersecurity and the rise of Zero Trust as a guiding strategy for our industry and organizations around the globe.

At the start of the pandemic, the workplace became almost entirely remote overnight. This shift forced many organizations to rapidly adapt to support employees that were getting work done anyway they could—using personal devices, collaborating through cloud services, and sharing data outside the corporate network perimeter. As organizations were adapting to this transformation, they also faced increasingly sophisticated cybercriminals who continually evolve their targeting, tactics, and resourcing.

Today, hybrid work is the new reality. Against this backdrop, and in the face of rapid change, the organizations we surveyed told us they rely on Zero Trust for increased security and compliance agility, increased speed of threat detection and remediation, and increased simplicity and availability of security analytics.

Based on the principles of verify explicitly, use least privileged access, and assume breach, a comprehensive Zero Trust architecture creates safeguards within and across identity, endpoints, apps, infrastructure, network, and data, partnered with increased visibility, automation and orchestration. We not only recommend this approach with our customers and partners, we embrace it in our approach to global security and software development here at Microsoft.

This report illuminates the path of Zero Trust adoption across diverse markets and industries. We hope that the learning gained by this research can help accelerate your own Zero Trust strategy adoption, shed light on the collective progress of your peers, and provide insights on the future state of this rapidly evolving space.

Methodology

Microsoft commissioned Hypothesis Group, an insights, design, and strategy agency, to execute the Zero Trust Adoption Report and research. The research included two phases in the US to highlight trends and momentum in Zero Trust adoption, with additional markets added in the second phase to uncover global trends.

Initial research occurred in August 2020, when a 15-minute online survey was conducted in the US with 300 security decision-makers (SDMs) involved in Zero Trust strategy decisions at enterprise companies from a range of industries. In addition to the online survey, five in-depth interviews were conducted online in September 2020 among SDMs from the US in a range of industries.

In April 2021, global research was carried out in the US, Germany, Japan, and Australia/New Zealand across a similar group of security decision-makers. Over 900 participants took a 15-minute online survey with questions around their Zero Trust strategy adoption, best practices, benefits, challenges, and how they intend to invest in the future.

Things to know about Zero Trust adoption

01 / Organizations are ready to capitalize on Zero Trust strategy, accelerated by the move to a hybrid workplace and Covid-19

Security decision-makers (SDMs) say developing a Zero Trust strategy is their #1 security priority, with 96% stating that it's critical to their organization's success. The primary motivators for adopting a Zero Trust strategy are to improve their overall security posture and the end user experience. The shift to a hybrid workplace, accelerated by COVID-19, is also driving broader adoption of Zero Trust strategy: 81% of enterprise organizations have begun the move toward a hybrid workplace, with 31% fully there. However, 94% have concerns about transitioning, chiefly, employee misuse, increased IT workloads, and cyberattacks. Given this, key considerations for a strategy include increased training for employees and multi-factor authentication (MFA) to ensure a smooth user experience and transition.

02 / Zero Trust strategy allows for flexibility in where organizations can begin implementing so the approach can be tailored to their needs

Fewer than 15% of organizations started implementing Zero Trust strategy in the same security risk area. This is in large part because implementation is approached as an end-to-end process across pillars and capabilities of security architecture rather than as a series of disparate, individual technologies. Similarly, the order in which individual components of Zero Trust within a security risk area are implemented is highly variable, with security professionals differing substantially in which components they begin implementing first.

03 / While Zero Trust strategy is widely adopted and improves organizations' ability to manage threats, there is still work to be done

76% of organizations have at least started implementing a Zero Trust strategy, with 35% claiming to be fully implemented. However, those claiming to be fully implemented admit they haven't finished implementing Zero Trust strategy across all security risk areas and components. Zero Trust strategy is compelling because it provides increased agility, speed of detecting threats, and improved ability to manage Internet of Things (IoT) and Operational Technology (OT) security. Adoption is growing in the US (70% in Aug 2020 to 79% in Apr 2021); the US is also farther ahead on Zero Trust implementation relative to other countries that started adopting later, and organizations in the US claim to be less constrained by budgets. However, while 57% of organizations claim to be ahead of others when it comes to adoption, around half still have more work to do as they haven't fully implemented Zero Trust across all security risk areas and components.

04 / Looking ahead, Zero Trust strategy will remain a top priority and require careful decision-making when it comes to employees and vendors

Zero Trust strategy is expected to remain the #1 security priority two years from now and organizations anticipate increasing their investment. Overcoming challenges with their employees (including staffing security teams and buy-in from leadership) will be key to doubling down on Zero Trust investment. When it comes to vendor strategy, security decision-makers have a slight preference for working with holistic or consolidated providers given that vendor selection is often contingent on availability of internal expertise. Benefits of the best-in-suite approach include increased expertise, resources, and simplicity, though it can take longer to implement, be harder to integrate into the existing security architecture, and increase potential vulnerability.

Who we talked to

Global

*1000+ employees in US; 500+ employees in Germany, Japan, Australia/New Zealand

Overall research learnings

Organizations are ready to capitalize on Zero Trust strategy

Zero Trust strategy is today's #1 security priority across markets and industries, with a number of organizations adopting a Zero Trust strategy in recent years. While Zero Trust is top-of-mind for all (53%), it is a particularly high priority for organizations in the United States (56%) and Germany (53%).

Almost all security professionals (96%) believe a Zero Trust strategy is critical to their organization's success. (See Exhibit 1) In addition to strengthening their overall security posture and improving end-user experience, security professionals are looking to Zero Trust strategy to simplify security procedures for employees. (See Exhibit 2)

As one US security decision-maker in Hospitality explains, *"The goal is to improve our security posture overall, but it's all about reducing friction in the end user experience and making life easier for them."*

Moreover, 31% of security professionals see Zero Trust strategy as an important tool in the imminent shift to a hybrid workplace post-pandemic; this driver is particularly salient in Australia/New Zealand (44%).

Exhibit 1. Zero Trust is critical

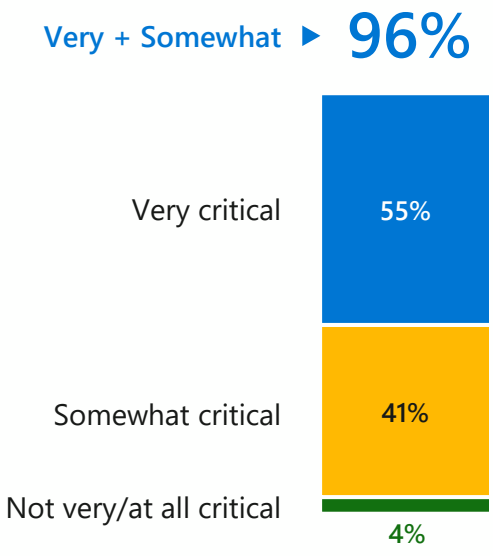


Exhibit 2. Zero Trust motivators

Top Motivators	
Improve overall security posture	47%
Improve end user experience and productivity	44%
Transform the way security teams work together	38%
Simplify security stack	35%
Reduce security costs	35%

The shift to a hybrid workplace is driving broader adoption of Zero Trust strategy

81% of enterprise organizations have begun the move toward a hybrid workplace, with 31% already fully adopted. That said, rates of full adoption are inconsistent across markets: while Australia and New Zealand lead the pack at 37%, Germany is far behind, with just 20% of organizations having already moved to a hybrid model. (See Exhibit 3)

Even as global markets move toward a hybrid workplace at disparate rates, the vast majority (91%) of organizations who haven't completed the transition anticipate doing so in the next five years. Crucially, 94% are worried about the transition, with employee misuse, increased IT workloads, and increased risk of cyberattacks topping the list of concerns. (See Exhibit 4)

Exhibit 3. Hybrid workplace intent

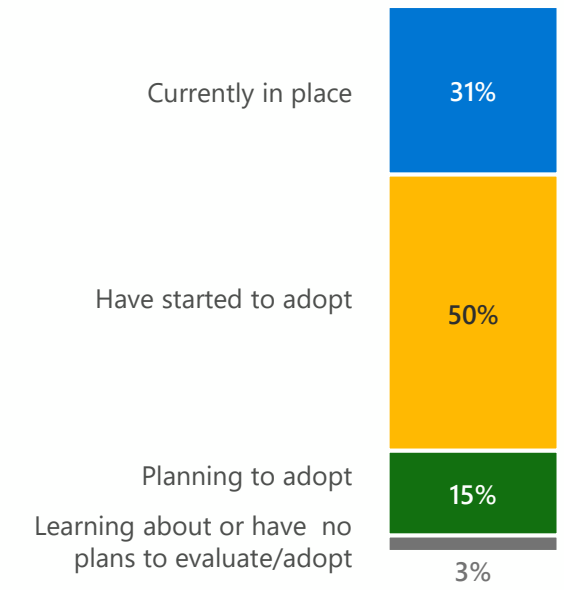
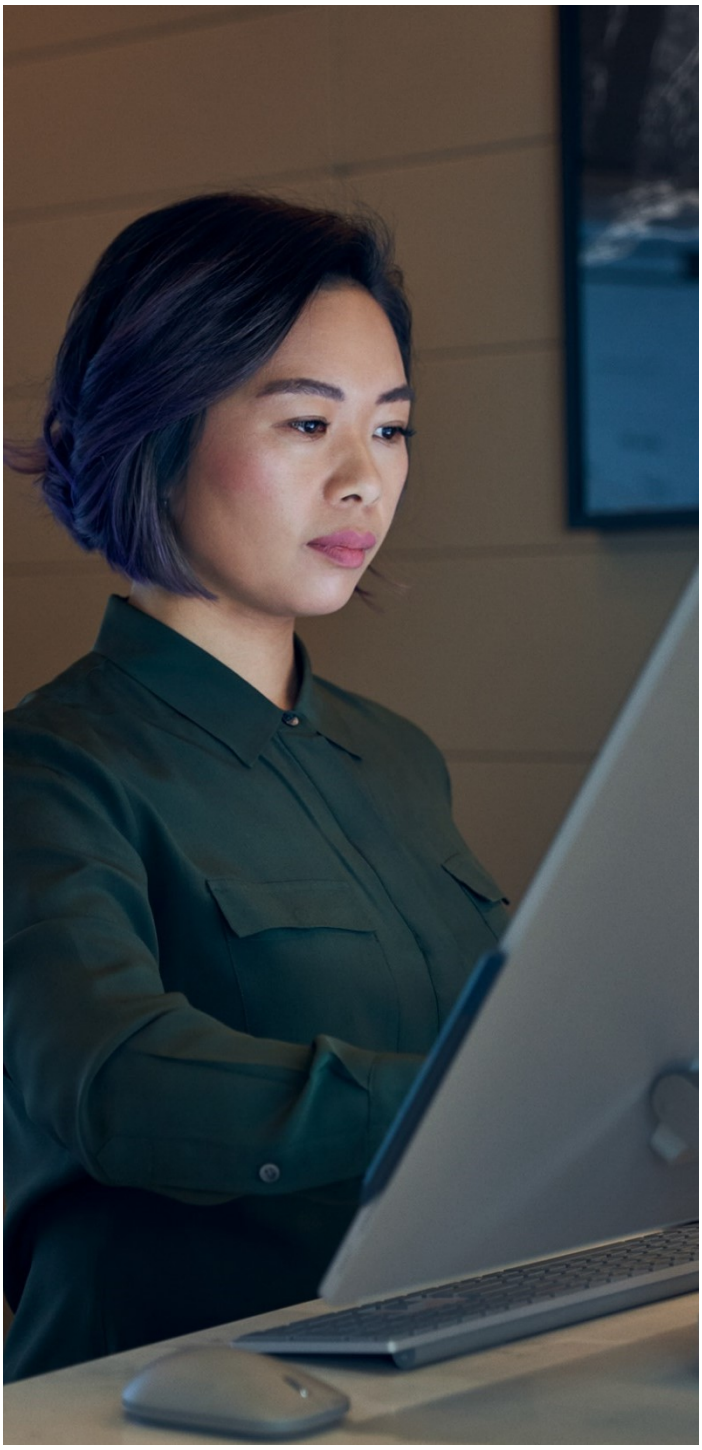


Exhibit 4. Hybrid workplace concerns

Employees downloading unsafe apps	37%
An increase to IT workload	37%
Ransomware attacks	36%
Phishing attacks	35%
Improper use of personal devices	34%
Unauthorized access to data	31%
Inability to manage all devices	30%
Use of personal email accounts	30%
Non-compliance with data regulations	24%

Covid-19 has brought on new considerations that accelerate the move to Zero Trust strategy



In an effort to minimize potential issues, stakeholders emphasize the importance of increased training for employees (54%) (particularly in Japan (61%) and Germany (58%)) and multi-factor authentication (MFA) (50%) (particularly in the United States (52%) and Germany (56%)) to ensure a smooth user experience and transition.

Because secure remote and hybrid work can be aided by Zero Trust strategy, COVID-19 has accelerated adoption of a Zero Trust strategy for 72% of organizations, although asymmetries emerge between markets. While the pandemic catalyzed adoption for around seven in ten organizations in the US (76%), Japan (71%), and Australia/New Zealand (69%), implementation rates have been notably lower in Germany (62%), perhaps due to a slower transition to a hybrid workplace.

Zero Trust is widely implemented around the world and growing in the US

Zero Trust isn't just a buzzword; it's a reality. 76% of organizations have at least started implementing this strategy and 35% believe they are fully implemented. However, this data paints an overly optimistic picture as many organizations who consider themselves fully implemented are, by their own admission, not finished executing across all security risk areas. Today, the US is ahead on Zero Trust strategy adoption relative to other markets and continues to grow rapidly: compared to August 2020, Zero Trust strategy implementation in the US increased from 70% to 79%, a sizable jump in just eight months. (See Exhibit 5)

Although Zero Trust strategy currently predominates the security space, its ubiquity is relatively new. 82% of companies implemented Zero Trust strategies within the past three years, with 21% doing so in the past 12 months. That said, 26% of US organizations began implementation 3+ years ago, versus 19% of Japanese organizations, 6% of organizations in Australia/New Zealand, and 3% of organizations in Germany. This earlier implementation in the US — in tandem with fewer budget constraints — may help explain why organizations in the US are ahead in Zero Trust adoption as compared to organizations in other markets. In a similar vein, the relative nascency of Zero Trust in Germany helps contextualize its lower adoption rates: 97% of German organizations only began implementation in the past three years.

Exhibit 5. Zero Trust implementation

	US (2020)	US	DE	JP	AUS/NZ
Zero Trust implementation	70%	79%	75%	76%	71%
• Fully implemented	27%	44%	19%	32%	28%
• In progress	43%	35%	56%	44%	43%

There is no one-size-fits-all approach to Zero Trust implementation, giving permission to start anywhere

No single security risk area (Identities, Endpoints, Apps, Network, Infrastructure, Data, Automation & Orchestration) stands out as a primary starting point for Zero Trust strategy, as fewer than 15% start with the same security risk area. Organizations are starting in different places likely based on their needs and available internal resources. Eventually, they seek to adopt Zero Trust strategy across all security risk areas to ensure even more protection against threats, so Zero Trust is perceived as an end-to-end strategy to be completed over time. (See Exhibit 6)

Beyond the security risk areas of Zero Trust strategy, organizations must identify the individual components of each security risk area to prioritize. For Endpoints, Apps, Network, Data, and Automation/ Orchestration, there is no clear starting point; security professionals vary substantially in which components they rank as their top priority. However, strong authentication is typically implemented first for Identities, and threat detection tools are a clear priority within Infrastructure. (See Exhibit 7)

Exhibit 6. Current Zero Trust implementation – Security risk areas

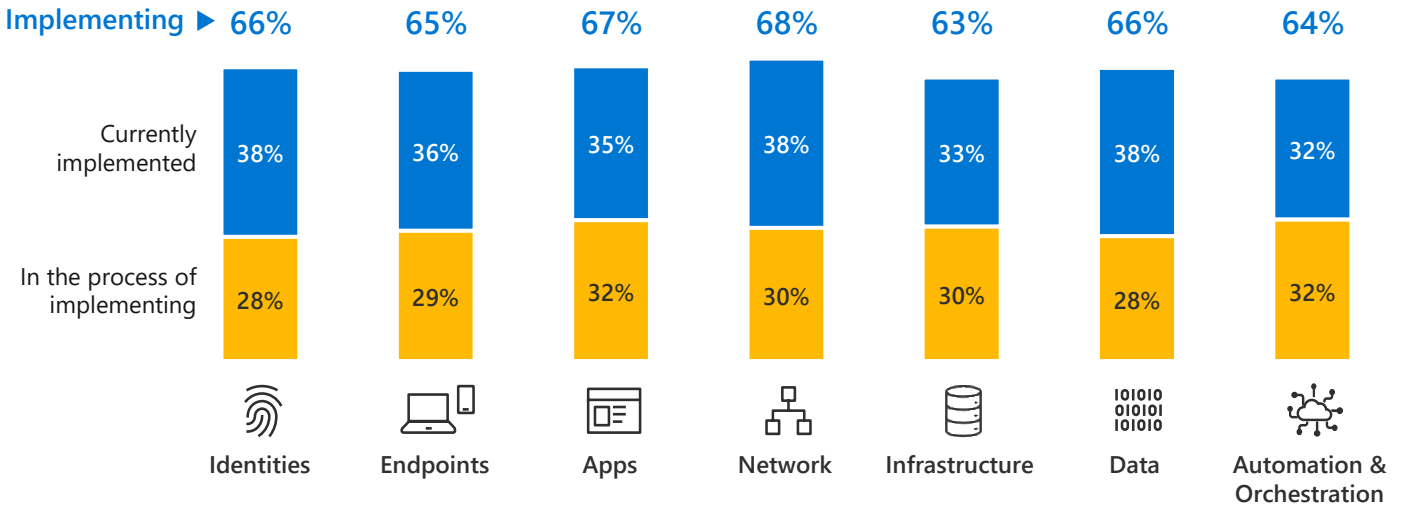


Exhibit 7. Zero Trust component implementation (Top 3) – Ranked #1 (Implemented first)

Identities	
Strong authentication (i.e., multi-factor authentication, passwordless authentication)	32%
Automated risk detection and remediation	27%
Adaptive access policies to gate access to resources	22%

Endpoints	
Data Loss Prevention policies/controls for all unmanaged and managed devices	27%
Real-time device risk evaluation / endpoint threat detection	26%
Devices are registered with identity provider	24%

Apps	
Ongoing Shadow IT Discovery and risk assessment	23%
Granular access control to your apps (such as limited visibility or read only)	22%
Policy-based access control for apps	20%

Network	
Secure access controls to protect networks	25%
Threat protection and filtering with context-based signals	24%
All traffic is encrypted	20%

Infrastructure	
Security operations team access to threat detection tools	25%
Cloud workload protection across hybrid and multi-cloud	19%
Granular visibility and access control across all workloads (virtual machines, servers, etc.)	17%

Data	
Access decisions are governed by security policy engine	21%
Data is classified and labeled	21%
The most sensitive files are persistently protected with encryption	20%

Automation & Orchestration	
End-to-end visibility is established with a centralized platform for investigation and response	29%
Threat data is collected and analyzed across domains (identities, endpoints, apps, network, infrastructure)	28%
Automated investigation and response is enabled	22%

We didn't look at it as just a series of technologies, but as a strategy and approach to treat every user resource, whether inside our network or outside our network, as untrusted until they could be verified."

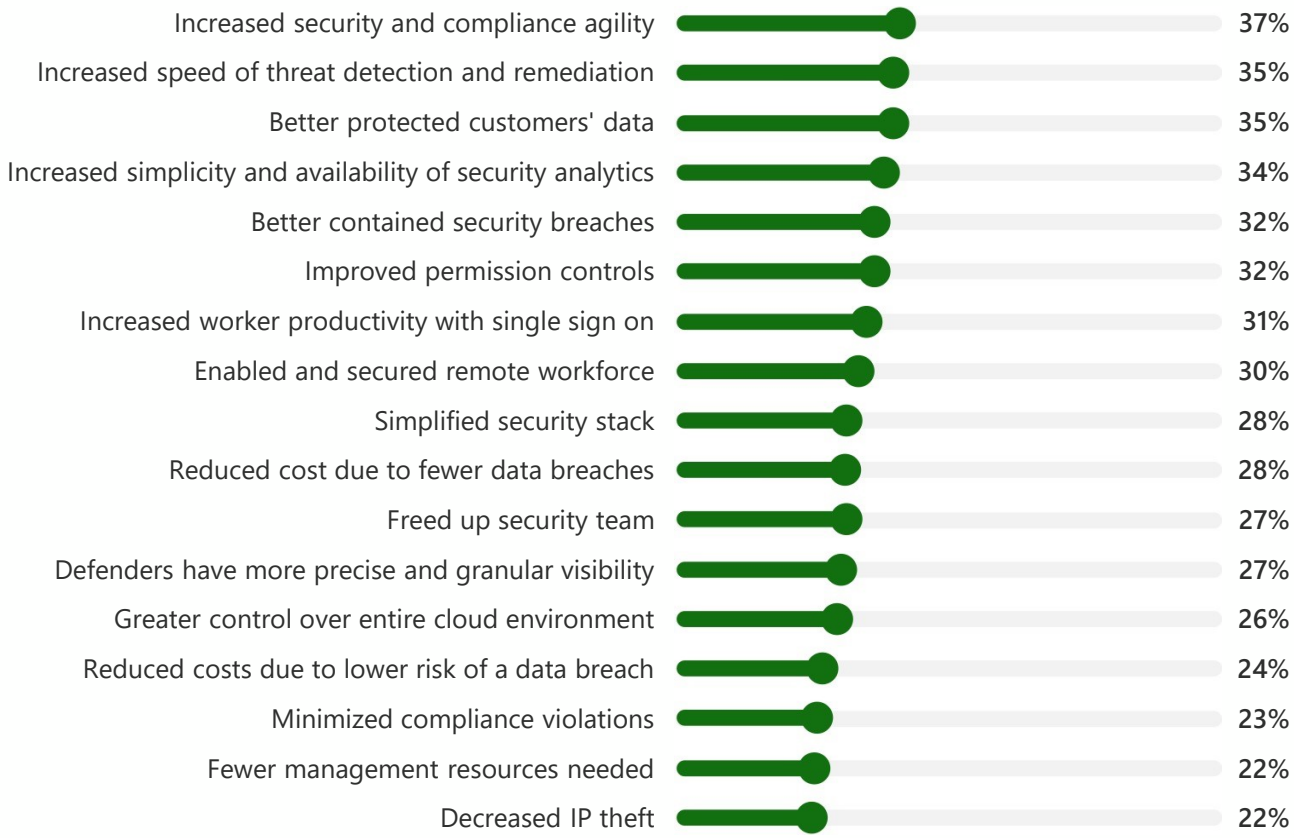
US Security Decision-Maker
Hospitality

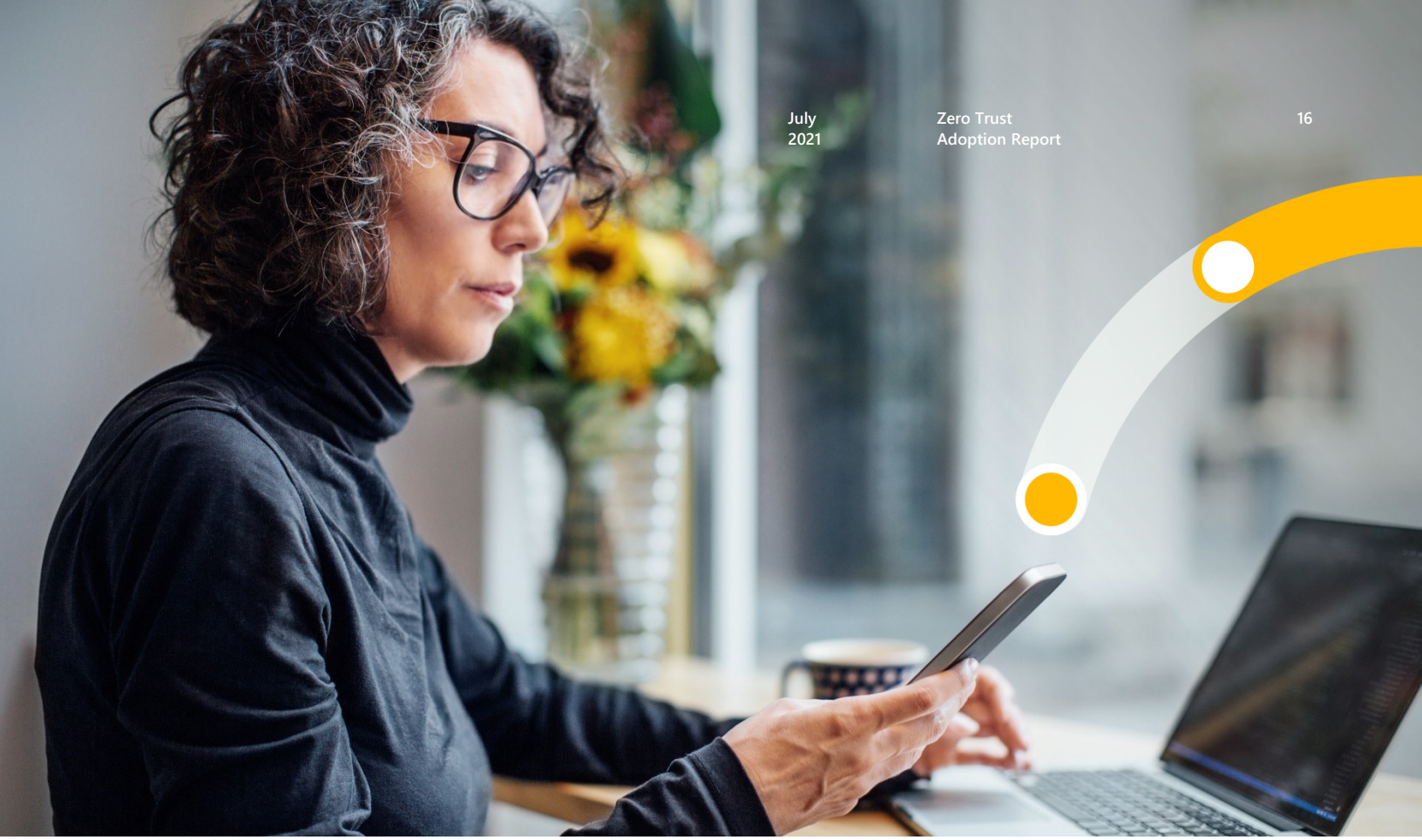
Once organizations start implementing a Zero Trust strategy, top benefits include increased agility, speed, and protection; resource advantages are less common

Once Zero Trust strategy is implemented, organizations benefit from increased agility (37%), speed (35%), and protection of customer data (35%). (See Exhibit 8) However, direct benefits to employees including a freed-up security team (27%) and a need for fewer resources to manage the infrastructure (22%), are less commonly realized.

Importantly, organizations believe their Zero Trust strategy will help them manage most threats and changes to the environment, especially with respect to IoT and OT security (47%).

Exhibit 8. Zero Trust benefits





Organizations feel confident in getting the most out of their Zero Trust strategy

79% feel confident about their ability to handle security threats as a whole, although this confidence wanes when the threat involves a fabrication of truth: SDMs feel least confident about dealing with threats involving synthetic identities (20%) and deepfakes (10%).

In light of the benefits gained, Zero Trust generally garners positive associations. Across the four markets, SDMs see their organizations' approach as simultaneously practical and aspirational, describing it as confident (37%) and efficient (31%) as well as motivating (25%), inspiring (25%), and exciting (25%). In Japan specifically, security professionals describe Zero Trust as both demanding (27%) and transformational (25%), suggesting that — while not easy to implement — its benefits are far-reaching once adopted.

Many believe they are ahead with Zero Trust implementation, but they still have more to do

While only 35% of organizations have fully implemented their Zero Trust strategy, 52% say that they are ahead of where they planned to be and 57% believe they are ahead of other organizations. Organizations consider themselves to be particularly ahead of others in Japan (66%) and Australia/New Zealand (63%). While confidence abounds across markets, there appears to be a gulf between perception and reality: among those who feel ahead of other organizations, only 42% claim to have fully implemented a Zero Trust strategy. (See Exhibit 9)

Although many organizations are confident in their Zero Trust strategy and feel poised to handle future security threats, there is still ample work to be done to fully implement across risk areas. Among organizations that consider their Zero Trust strategy to be fully implemented, for example, almost half have not currently implemented across security risk areas, with Infrastructure and Identities the least likely to be implemented.

Exhibit 9. Zero Trust implementation comparison

	US	DE	JP	AUS/NZ
Ahead	59%	46%	66%	63%
On par	40%	52%	34%	32%
Behind	2%	2%	0%	6%

Looking ahead to the next two years, Zero Trust strategy will remain a top security priority

Organizations are all-in with Zero Trust strategy, and decision-makers say it will continue to be the top security priority over the next two years. The relative importance of Zero Trust strategy as a security initiative is projected to increase (53% to 58%) by 2023, as SDMs anticipate that the strategy will remain critical to overall success (96%). (See Exhibit 10)

Anticipated criticality is particularly high among Japanese organizations, with 70% saying Zero Trust strategy will be very critical in the next two years compared to the overall average of 56%. Zero Trust strategy budgets are also expected to grow with 73% of organizations expecting to increase their budgets. Although, this number is slightly lower in Germany (67%), where 31% anticipate that their budgets will stay the same. (See Exhibit 11)

Exhibit 10. Anticipated criticality of Zero Trust in next two years

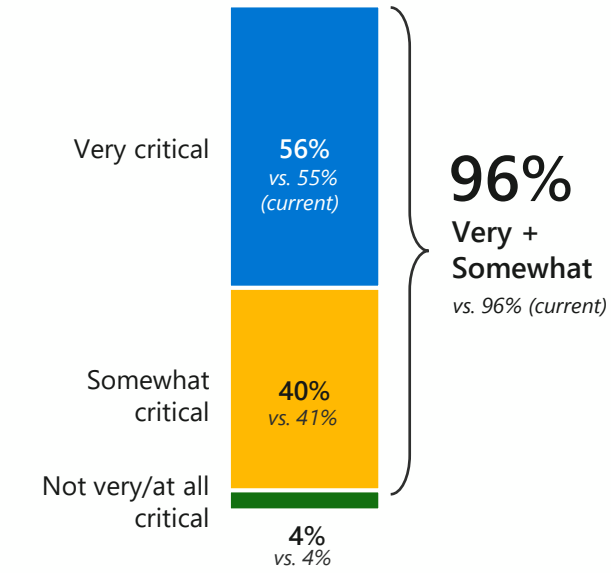
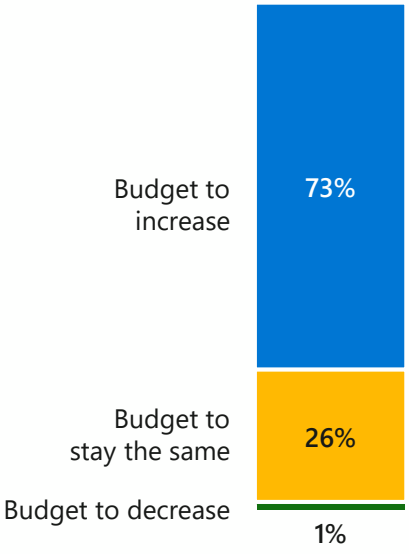
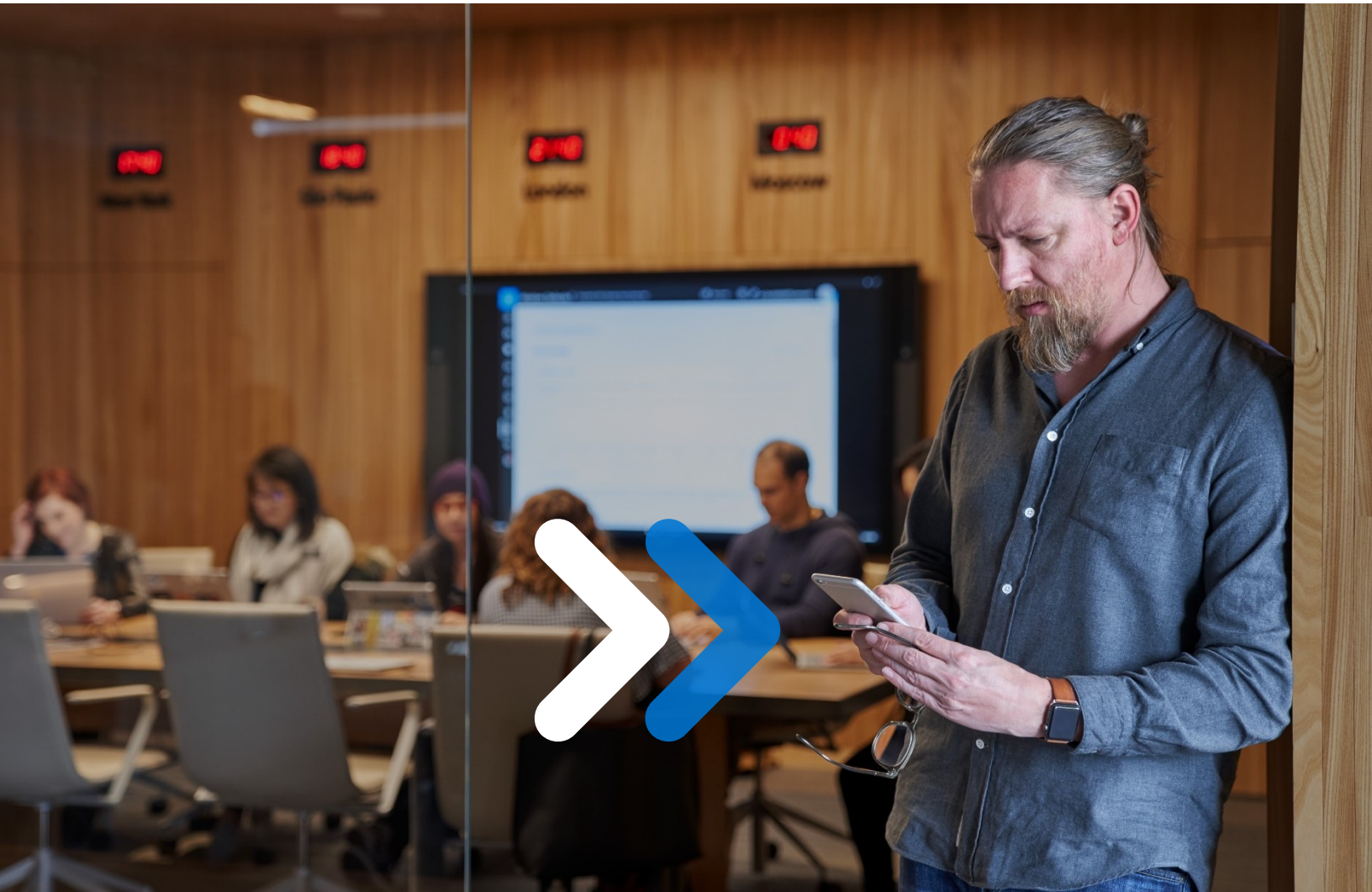


Exhibit 11. Anticipated Zero Trust budget in next two years



Proving successes of Zero Trust strategy could fuel further investment

Organizations that have wholeheartedly embraced Zero Trust expect to double down on their investment in the next two years, and those who have not yet started adopting risk falling further behind. These organizations not only trail their fully implemented counterparts when it comes to prioritizing Zero Trust in their security plans (42% vs. 66%) and anticipating budget increases (66% vs. 72%), but also feel significantly less confident in managing IoT and OT security in the future (40% vs. 53%).



Overcoming challenges with employees will be key to double down on Zero Trust investment

Despite rapid advances in Zero Trust strategy adoption, organizations must overcome a myriad of challenges if they want to advance further with implementation. (See Exhibit 12) Resource and leadership challenges are most prevalent within these categories. The time needed to implement Zero Trust strategies and a lack of support from C-suite leadership top the list of barriers, with the latter being particularly salient in Australia/New Zealand (65%).

Moreover, budgetary constraints — which 45% of organizations identify as a barrier — likely also play a role in resource and leadership challenges.

For example, 21% of SDMs cite difficulties in proving the ROI of an investment in Zero Trust as a barrier to implementation, a challenge that may lead to a lack of C-suite buy-in. Because non-US markets are more likely to have budget constraints (60% of organizations in Japan; 57% of organizations in Germany; 57% of organizations in Australia/New Zealand), it is possible that this has a ripple effect, leading to lower and slower implementation of Zero Trust strategies in Japan, Germany, and Australia/New Zealand as compared to the US.

Exhibit 12. Zero Trust barriers

Resource Challenges 60%	Leadership 53%	Technological 46%	Vendor 46%	Budget Constraints 45%
20% Takes too long to implement	**20%** Lack of support from wider C-suite leadership	**21%** Difficulty integrating security solutions	**21%** Need implementation support from vendors	**21%** Cost of implementing a Zero Trust strategy
19% Lack of internal change management	**19%** Lack of support from stakeholders	**19%** Incompatibility with legacy systems	**21%** Difficulty identifying the right vendors	**21%** Difficulty proving ROI
18% Need more education materials	**19%** Need help to make a compelling business case	**19%** Difficulty scaling throughout the organization	**17%** Inability to find innovative partners	**14%** Don't have a large enough budget
17% Not needed for an organization of our size	**18%** Lack of organizational buy-in			
16% Don't have the right talent to properly implement				

" The initial buy-in was challenging but once we agreed as stakeholders that we were going to invest in this project, everyone was on board."

US Security Decision-Maker
FinTech

Security decision-makers have a slight proclivity for holistic or consolidated providers

When it comes to Zero Trust vendor strategy, organizations are faced with taking a best-in-suite or best-in-breed approach. The former strategy involves purchasing a suite of products for one's entire Zero Trust architecture from a holistic or consolidated provider, a solution that SDMs believe offers more expertise, resources, and simplicity for those who are resource-strapped internally. However, concerns with this approach include increased vulnerability and lack of flexibility. (See Exhibit 13)

The latter strategy, best-in-breed, involves obtaining individual Zero Trust technology components from specialized vendors. Unlike best-in-suite, this strategy relies on providers that specialize in different areas and thus offer greater flexibility and can more closely align with the organization's strategy. That said, security professionals see best-in-breed as more costly, requiring more resources, and inhibiting visibility, drawbacks that ultimately lead to vendor and budgetary challenges. (See Exhibit 14)

While organizations are largely split, a slight majority of SDMs (55%) prefer working with holistic (best-in-suite) providers. (Organizations in Australia/New Zealand, however, lean in the opposite direction, with 52% preferring best-in-breed.)

Exhibit 13. Best-in-Suite benefits & barriers – Ranked in Top 2

⊕ Best-in-Suite benefits	
Vendor has industry-specific expertise across solutions	24%
More resources available to help plan Zero Trust strategy	23%
Simplified security stack	22%

⊖ Best-in-Suite drawbacks	
Reliance on a single vendor increases vulnerability	34%
Requires more complex integration with legacy architecture	33%
Less flexibility for specialized functioning	29%

Exhibit 14. Best-in-Breed benefits & barriers – Ranked in Top 2

⊕ Best-in-Breed benefits	
Flexibility to pursue the best solutions for any component of Zero Trust strategy	33%
Can more closely align the solution with my organization's architecture or strategy	30%
Increased opportunity for innovation with various vendors	26%

⊖ Best-in-Breed drawbacks	
Increased costs	29%
Inability to share data across different solutions	26%
High volume of solutions for internal teams to adopt and manage	26%

Final thoughts

As security risks become not only more frequent but more nefarious, organizations across markets and industries are opting for a Zero Trust strategy which guides us to "never trust, always verify." Zero Trust strategy is the top security priority for organizations who aim to improve their overall security posture, end-user experience, and productivity, simplify security procedures for employees, and reduce costs. However, while the benefits of a Zero Trust strategy are well-established, limited resources and skepticism among leadership stand in the way of universal implementation.

Adoption of Zero Trust strategy has accelerated in the past three years, in part due to the COVID-19 pandemic. Crucially, the shift to remote and hybrid workplaces is driving a broader adoption of Zero Trust approaches, which promise to safeguard systems and data even as employees access them off-site, sometimes on personal devices. Accelerated adoption due to COVID is a good predictor of Zero Trust readiness overall, with organizations that embraced the strategy during the pandemic having implemented in more security risk areas than their counterparts.

That said, even the most advanced Zero Trust strategy adopters have work left to do, and organizations' misperceptions around their own Zero Trust maturity may leave some with vulnerabilities they don't even know they have.

A majority of organizations across markets believe that the criticality of a Zero Trust strategy will only grow with time and are expecting their budgets to increase in turn. This anticipated shift in prioritization is particularly crucial for non-US markets, where budgetary concerns are salient barriers to adoption. Striving for full implementation may be financially and logistically overwhelming; still, the benefits of a Zero Trust approach are undeniable, and Microsoft will be there to guide and support organizations as they embark on this burgeoning frontier.

To learn more about Zero Trust and take an assessment of your organization's Zero Trust maturity, visit

aka.ms/zerotrust

Detailed research objectives & audience recruit

The objectives of the research included:

Understand the current state of Zero Trust approaches

Uncover mindsets, best practices, benefits, and challenges of adopting Zero Trust approaches

Explore the future of Zero Trust approaches

Contextualize innovations and trends in Zero Trust approaches

To meet the screening criteria, Security Decision-Makers needed to be:

Responsible for security in their organization, including Cybersecurity, Security Operations, Threat Protection, Identity Management, Risk Management, Application Security, Digital Forensics, and Incident Response

Employed full-time at an enterprise-level company (1000+ employees in US; 500+ employees in DE/JP/AU/NZ)

Ages 25-75

Familiar with Zero Trust

Involved in decision making for Zero Trust strategy development/implementation

Of the 911 Security Decision-Makers interviewed for the research wave in April 2021:

In the US, 477 SDMs were interviewed

In Germany, 201 SDMs were interviewed

In Australia/New Zealand, 126 SDMs were interviewed

In Japan, 107 SDMs were interviewed

Note: Research was conducted during the global COVID-19 pandemic, which was at varying stages of escalation/containment

© Hypothesis Group 2021. © Microsoft 2021.
All rights reserved. 07/21