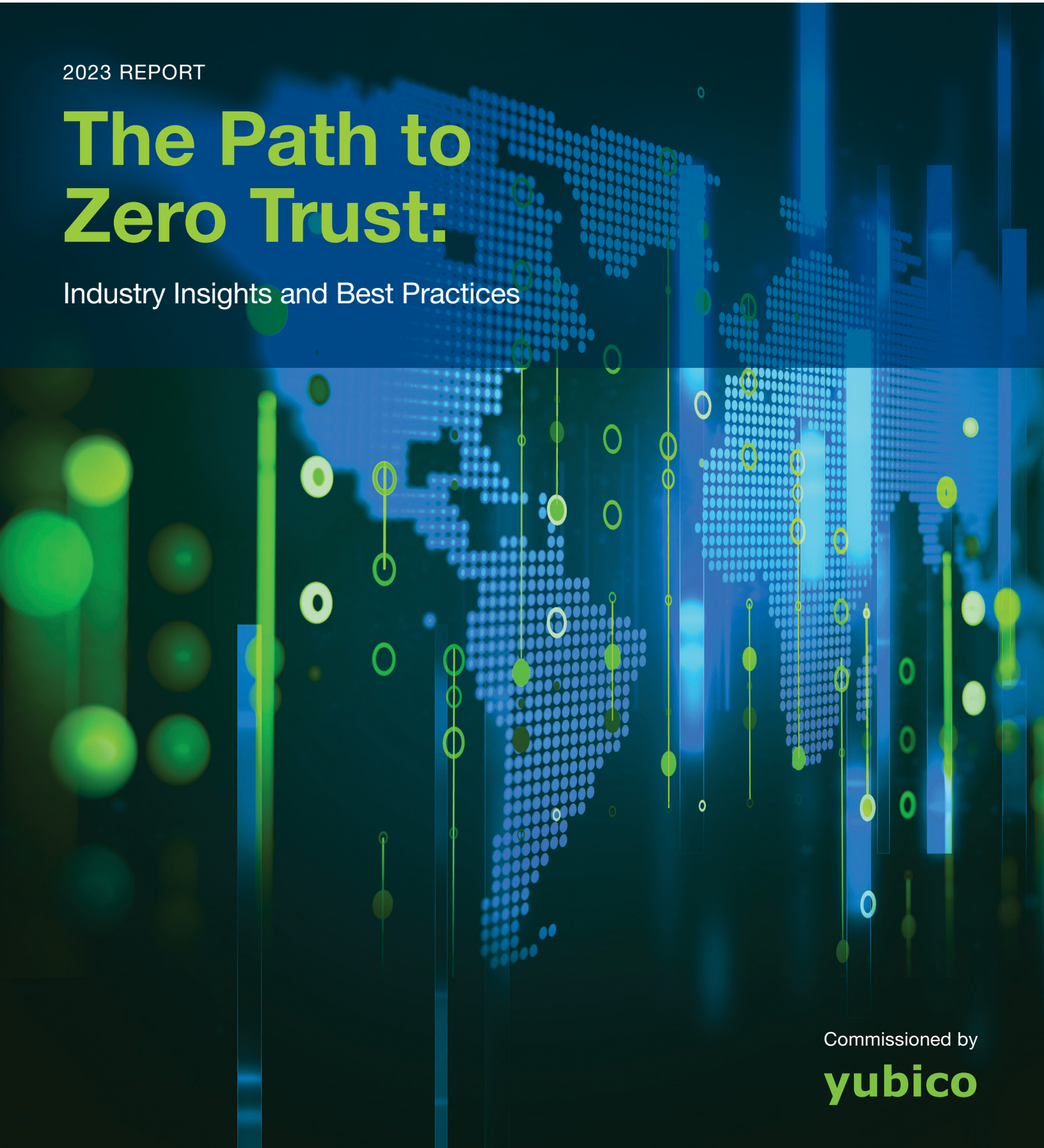
Cybersecurity
INSIDERS

2023 REPORT

The Path to Zero Trust:

Industry Insights and Best Practices



Commissioned by

yubico

Introduction

Rapid digital transformation, increased remote work, and evolving cybersecurity threats have catapulted Zero Trust from an IT buzzword to a foundational cybersecurity model. Zero Trust assumes no inherent trust for any entity (users, devices, applications, etc.) within an organization's network, requiring strict identity verification for every access request, regardless of its origin, to minimize potential security risks.

The 2023 report "The Path to Zero Trust: Industry Insights and Best Practices" made possible through a comprehensive survey of 423 IT and cybersecurity professionals, aims to explore and reveal the adoption trends, challenges, and current state of Zero Trust.

Key findings include:

- A significant percentage of organizations (65%) are prioritizing the modernization of their Zero Trust framework, particularly user authentication with phishing-resistant MFA.
- According to 41% of respondents, the most significant accelerating factor for Zero Trust implementation is enhancing user authentication & access controls.
- The top priority at 62% is moving away from passwords and legacy MFA to modern, phishing-resistant MFA. Organizations are also prioritizing identity and access management (IAM) (52%) and focusing on secure cloud application access (50%).
- Organizations are adopting a multi-product approach to implement Zero Trust, with 50% of respondents using between 2 and 4 products.
- Despite the surge in interest, the actual implementation of Zero Trust is still a work in progress, with only 18% of organizations already having Zero Trust access in operation while 31% have Zero Trust implementation projects underway.

We want to extend our sincere gratitude to Yubico for supporting this important research. As organizations continue to navigate the complexities of the cybersecurity landscape, we hope this report serves as a valuable resource in your journey towards Zero Trust. The insights, best practices, and data-driven perspectives provided in this report will help inform your strategies, investments, and implementations of Zero Trust security.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

Current Security Priorities

We started our survey by asking cybersecurity professionals about their organization's current security priorities. The results indicate a strong alignment with key principles of Zero Trust, with the transition from legacy multi-factor authentication (MFA) to phishing-resistant MFA being a major focus for over half of the respondents (62%). Organizations are also prioritizing identity and access management (IAM) (52%) and focusing on secure cloud application access (50%).

These initiatives echo the core Zero Trust principles of least privilege access and continuous verification. Overall, these priorities indicate that organizations are increasingly adopting Zero Trust security practices to enhance their cybersecurity posture against evolving threats.

What are your organization's current security priorities? (Multiple responses allowed)

62%

Move away from passwords and legacy MFA to modern, phishing-resistant MFA

52%

Improve Identity and Access Management (IAM)

50%

Ensure secure access to applications hosted on cloud service providers

47%
Supplement Endpoint Detection and Response (EDR)

45%
Data Loss Prevention (DLP)

43%
Improve vulnerability remediation

35%
Simplify secure access delivery

35%
Augment or replace existing remote access tools

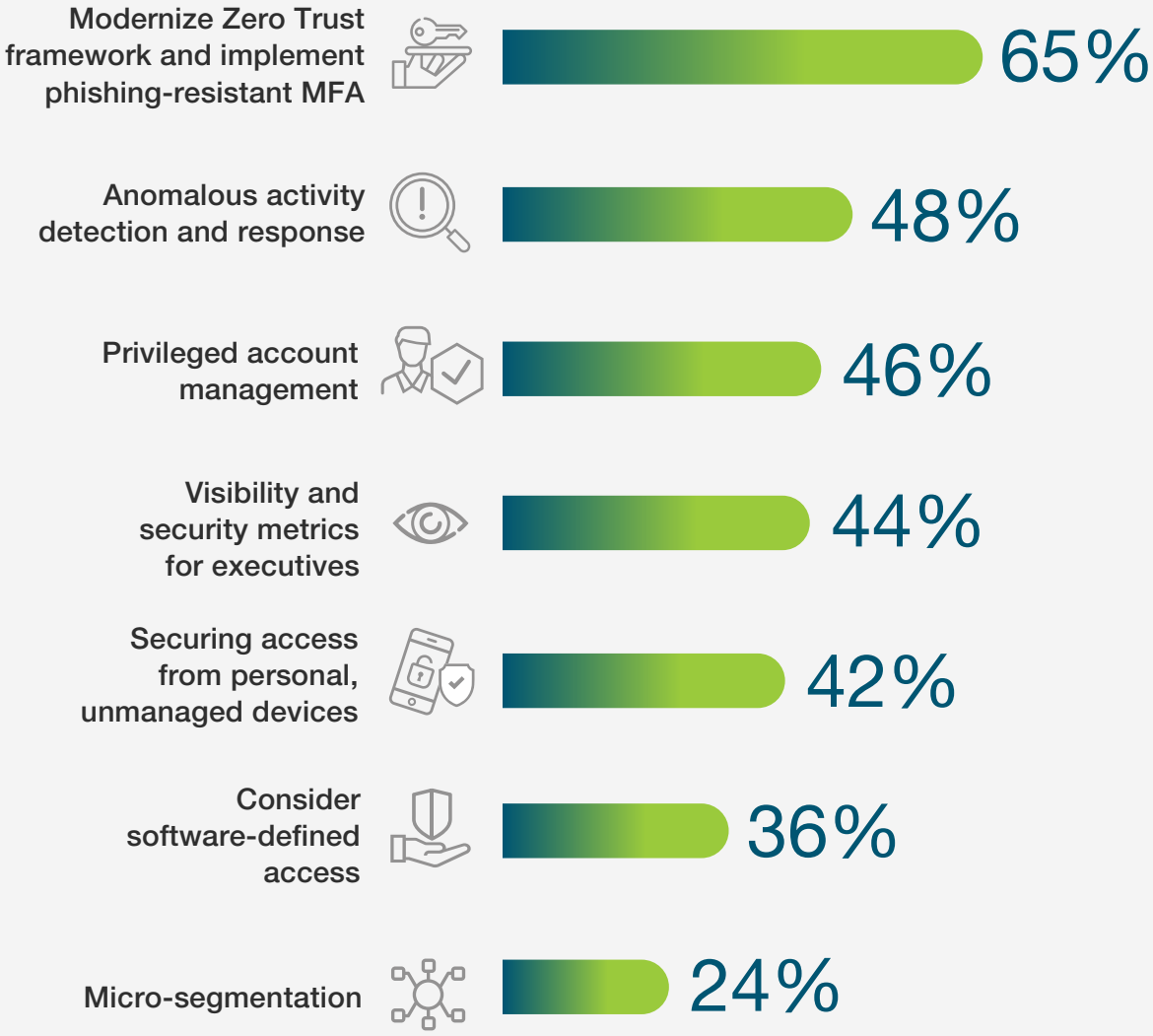
Encrypt sensitive information (e.g. digital rights management) 30% | Enable Endpoint Mobile Management (EMM)/BYOD (e.g. users, devices) 28% Conduct Deep SSL Inspection (e.g. secure session decryption for malware scanning and web/email filtering) 25% | Provide better mobile threat protection (Mobile Threat Defense/Anti-Phishing) 24% | Enhance SD-WAN security functions 21% | Other 3%

Secure Access Priorities

A key element of Zero Trust is the emphasis on advanced user authentication and robust anomaly detection. The survey results underscore the commitment to these facets, with 65% of organizations recognizing the importance of modernizing their Zero Trust frameworks and implementing phishing-resistant MFA. Moreover, 48% of respondents are prioritizing the detection of anomalous activity, which is integral to the Zero Trust mandate of continuous verification.

In a noteworthy shift, 36% of organizations are reassessing their legacy security infrastructures, indicating a transition towards the Zero Trust pillar of software-defined access. All of the highlighted secure access priorities would foster an environment of continuous verification while minimizing the attack surface.

What are your organization's secure access priorities for the next one to two years?
(Multiple responses allowed)

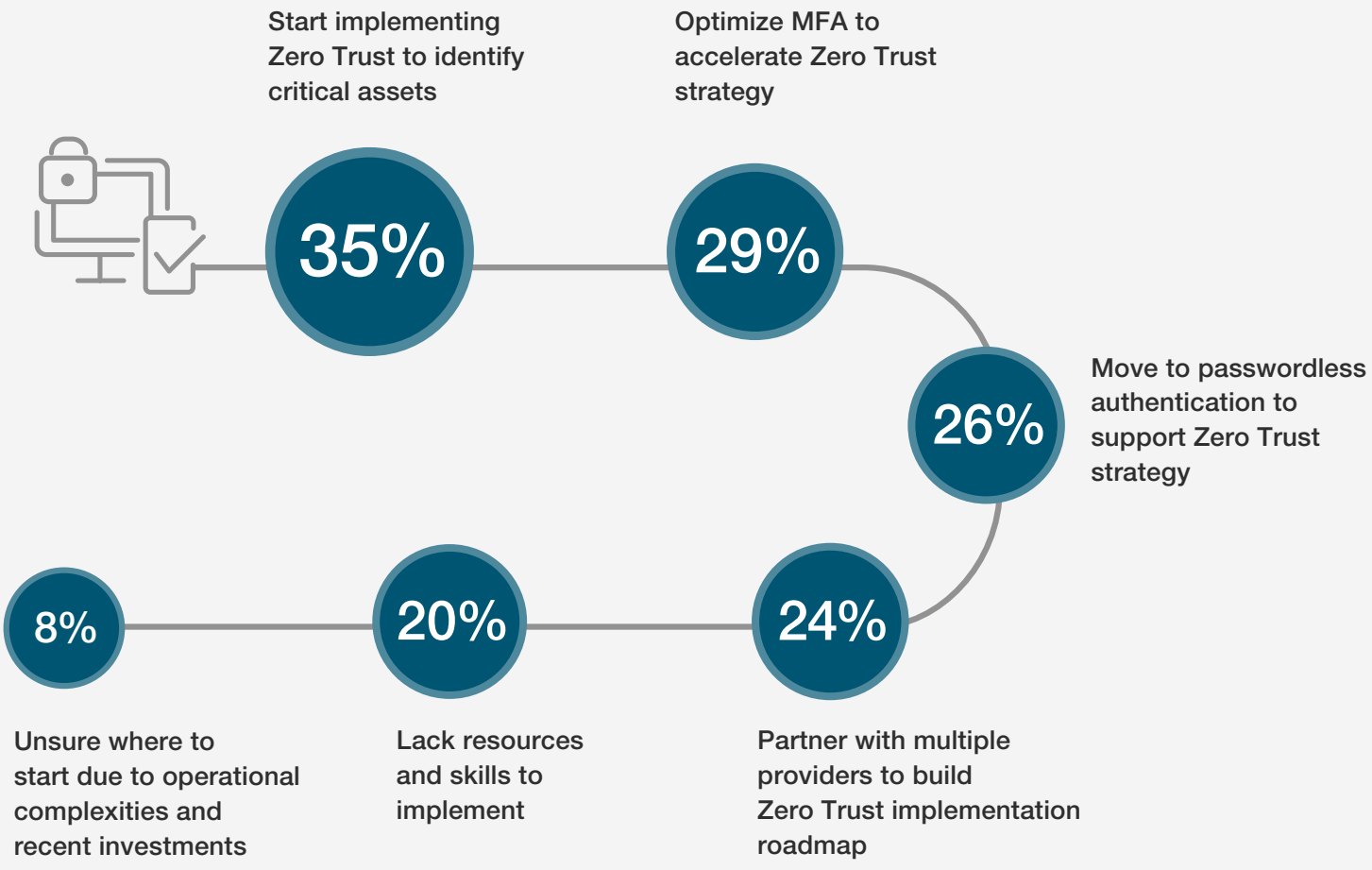


Zero Trust Implementation Paths

Zero Trust implementation is essential in enhancing security posture, requiring a systematic approach and relevant skills. When asked about their plans for Zero Trust implementation, an encouraging 35% of organizations are starting to embark on this journey, with an emphasis on identifying their most critical assets. Meanwhile, 29% are optimizing multi-factor authentication (MFA) as a strategic quick-win in their Zero Trust roadmap. However, it is worth noting that 20% of organizations reported a delay in their readiness due to limitations in resources and skills.

As a best practice, organizations should start their Zero Trust journey with a focus on safeguarding their critical assets and modernizing MFA. This approach can provide an immediate boost in their security posture. Additionally, collaboration with third-party security providers can bridge gaps in resources and skills, accelerating the implementation process.

Zero Trust implementation is a gradual process. How are you planning to implement Zero Trust across your extended environment? (Multiple responses allowed)

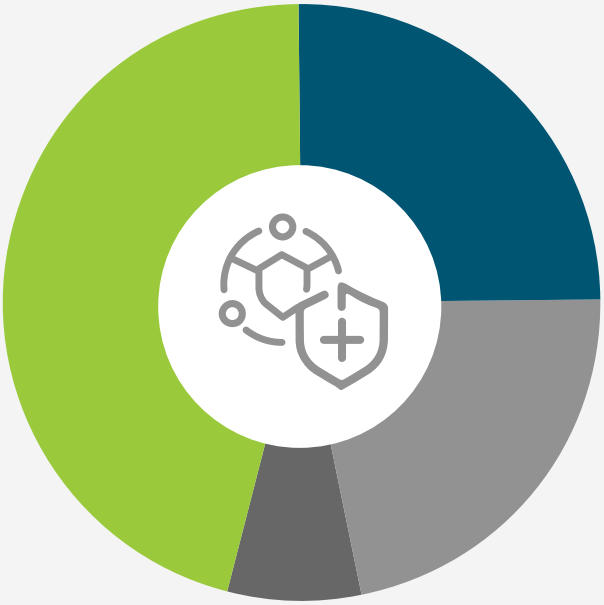


Journey to Zero Trust

When asked about their path to Zero Trust, 46% of organizations are taking a hybrid approach, gradually shifting users to a ZTNA solution while retaining VPN for a core set of users. Meanwhile, 25% plan for ZTNA and VPN to coexist, serving different use cases in the foreseeable future. A smaller cohort of 22% are looking to completely migrate all users to a ZTNA solution.

Based on these responses, organizations could consider a gradual transition towards ZTNA while maintaining certain VPN functionalities. It's essential to remember that the shift to ZTNA is not a one-size-fits-all process, but rather one that should be thoughtfully tailored to meet the unique requirements and security postures of each organization.

Zero Trust Access is going to be a journey - which scenarios best describe your organization's journey?



46%
Shift gradually from VPN to ZTNA solution but keep VPN for core set of users

25%
Operate ZTNA and VPN simultaneously

22%
Migrate all users to a ZTNA solution

7%
Other

Paths to SASE

Incorporating Secure Access Service Edge (SASE) into an organization's security strategy is a forward-thinking decision that integrates security and networking in an increasingly cloud-centric business landscape.

On the journey towards SASE adoption, an impressive 57% of organizations are adopting a 'best of breed' approach, selecting vendors that closely align with their unique requirements. A smaller segment, 22%, are in pursuit of vendors who can deliver a complete SASE solution, whereas 15% opt to remain with their existing vendors and consolidate as necessary.

The data underlines that a custom 'best of breed' strategy is currently the leading choice for SASE adoption. As organizations make their transition towards a SASE model, the primary focus should be to comprehend their distinct needs and select solutions that optimally cater to these requirements, as opposed to exclusively seeking comprehensive packages.

Which of the following approaches is most likely for your organization's evolution towards SASE?

57%

Take a 'best of breed' approach

22%

Look for vendors who can provide complete SASE solution

15%

Stay with existing vendors and consolidate

Other 6%

Secure Access Challenges

Understanding your organization's main security threats is a vital step in forming a robust Zero Trust architecture. The survey results reveal that over-privileged employee access (51%) and at-risk devices accessing network resources (48%) are the primary security concerns among organizations. Additionally, 45% of participants voiced significant worries about cyberattacks. However, issues associated with slower response times due to manual processes and shadow IT also received significant attention, noted by 36% and 39% of respondents, respectively.

In light of these concerns, it's advisable for organizations to emphasize the least privilege principle to curb over-privileged access. This principle, fundamental to the Zero Trust model, restricts access rights for users, accounts, and computing processes to only what's essential for their legitimate purpose, thereby reducing the potential damage from any security breaches. Employing thorough device trust verification measures will further help reduce risks from insecure devices and allow organizations to advance meaningfully on their Zero Trust path.

What top challenges is your organization facing when it comes to securing access to applications and resources? (Multiple responses allowed)

51% Over-privileged employee access

48% At-risk devices accessing network resources

45% Cyberattacks

39% Shadow IT

36% Complex manual processes slow down reaction time

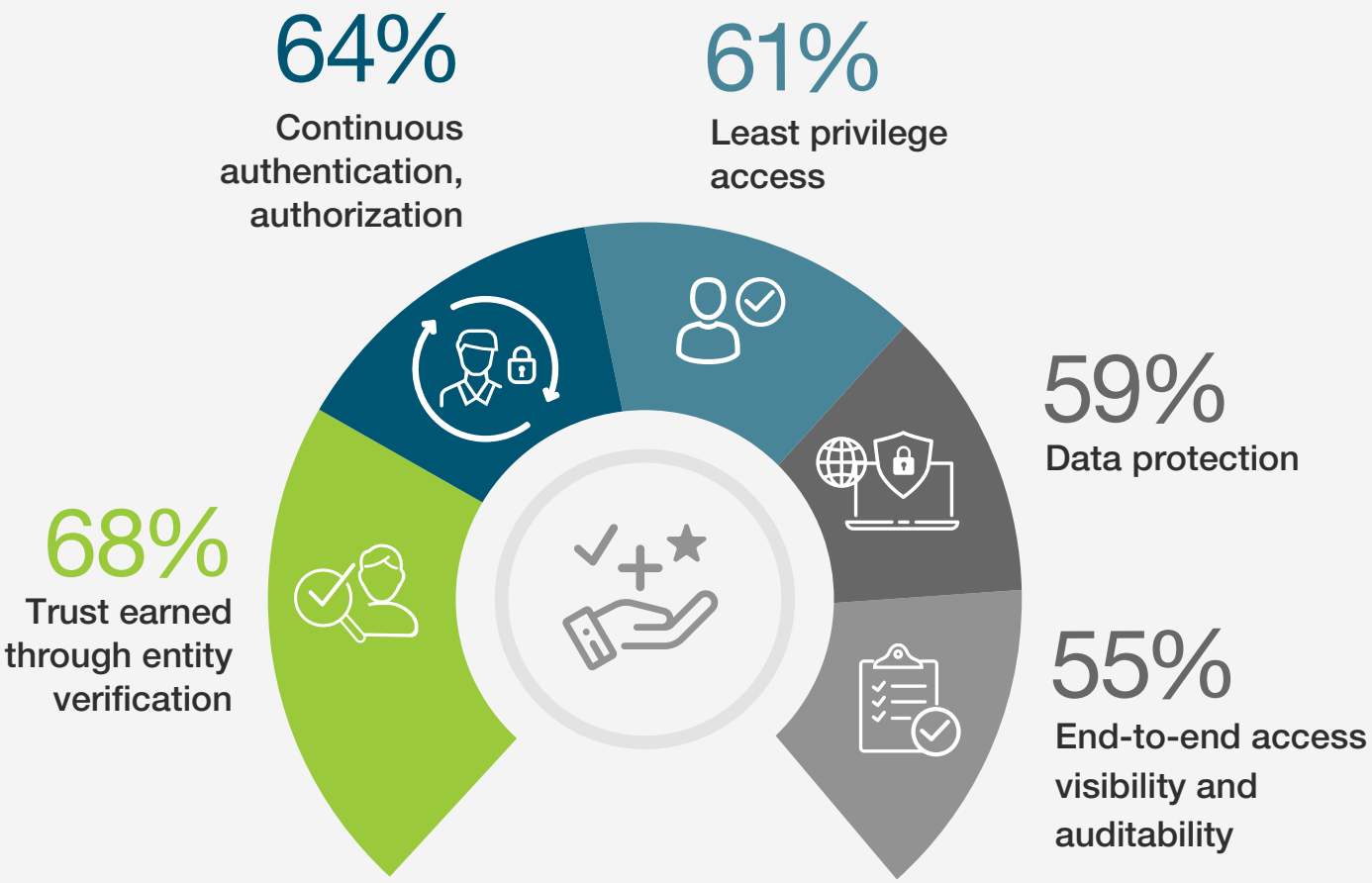
Partners insecurely accessing apps and resources 35% | Vulnerable, jailbroken or lost mobile devices accessing resources 15% | Other 1%

Zero Trust Tenets

What aspects of Zero Trust are most compelling to cybersecurity professionals? Survey participants highlighted trust earned through entity verification (68%) and ongoing authentication and authorization (64%) as the cornerstone aspects of Zero Trust, embodying its "never trust, always verify" philosophy. Additionally, implementing least privilege access (61%) and guaranteeing data protection (59%) emerged as key priorities, reflecting an intent to reduce potential attack surfaces and fortify data security.

In light of these findings, organizations are recommended to establish robust entity verification mechanisms, achievable through phishing-resistant MFA. Embracing constant monitoring and reauthentication as part of the security strategy is also advisable. Further, by adopting the principle of least privilege in access controls, the potential fallout of security breaches can be substantially mitigated.

What Zero Trust tenets are most compelling to you and your organization? (Multiple responses allowed)



No trust distinction between internal or external network 38% | Centralized, granular access policy 36% | Resource segregation 31% | Other 3%

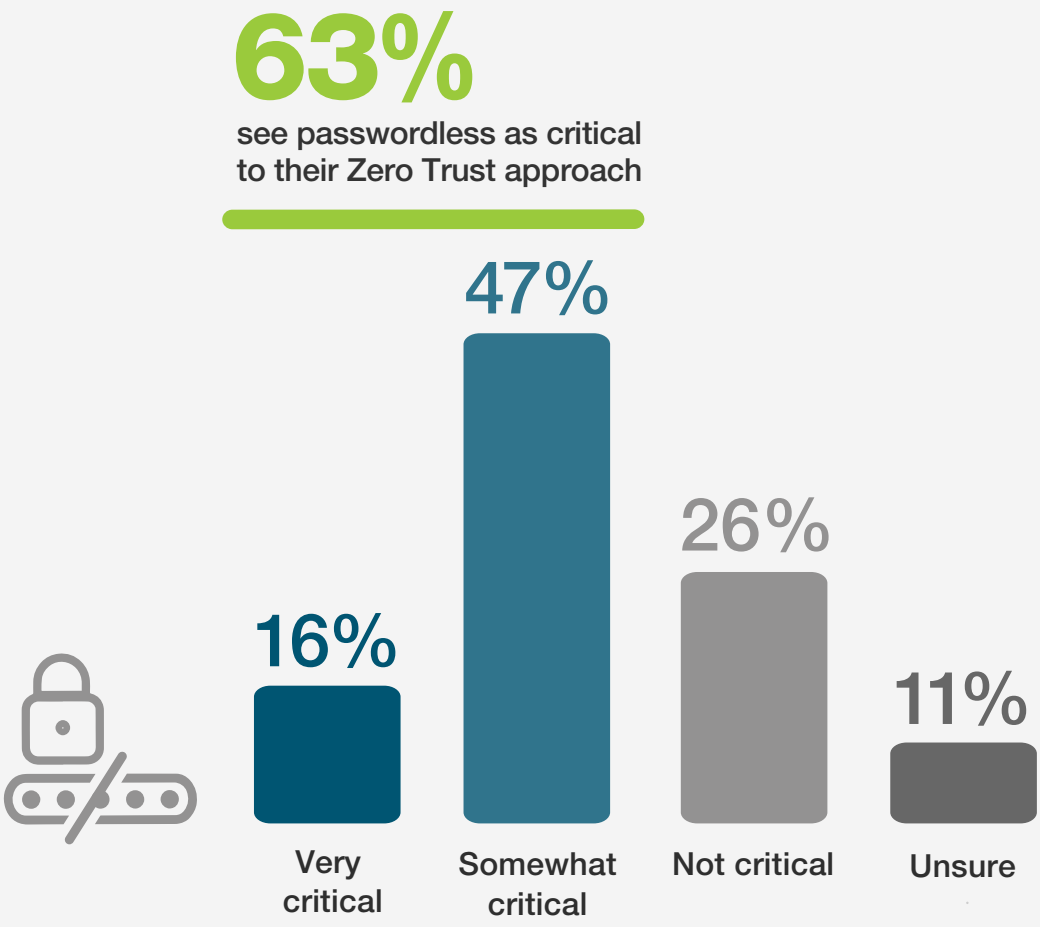
Passwordless Authentication

Passwordless authentication, a feature that combines enhanced security with improved user experience, serves as a fundamental part of the Zero Trust principle “never trust, always verify.”

A majority of survey participants (63%) regard passwordless as either very critical (16%) or somewhat critical (47%) to their Zero Trust approach. This data underlines the weight organizations are putting on the transition away from password-dependent authentication, given its inherent security vulnerabilities. Conversely, a 26% contingent view it as non-essential, possibly reflecting a concentration on other Zero Trust elements or doubts about the practicality of fully passwordless systems.

To harness the advantages of passwordless authentication, it’s recommended that organizations incorporate modern, phishing-resistant MFA methods into their Zero Trust plan, as moving away from legacy MFA to modern MFA is a pre-requisite to being able to go passwordless when ready. Moving to a passwordless state not only delivers reliable entity verification but also enhances the user experience — a crucial step in promoting user acceptance and compliance.

How critical is passwordless in your Zero Trust strategy?



Drivers for Zero Trust

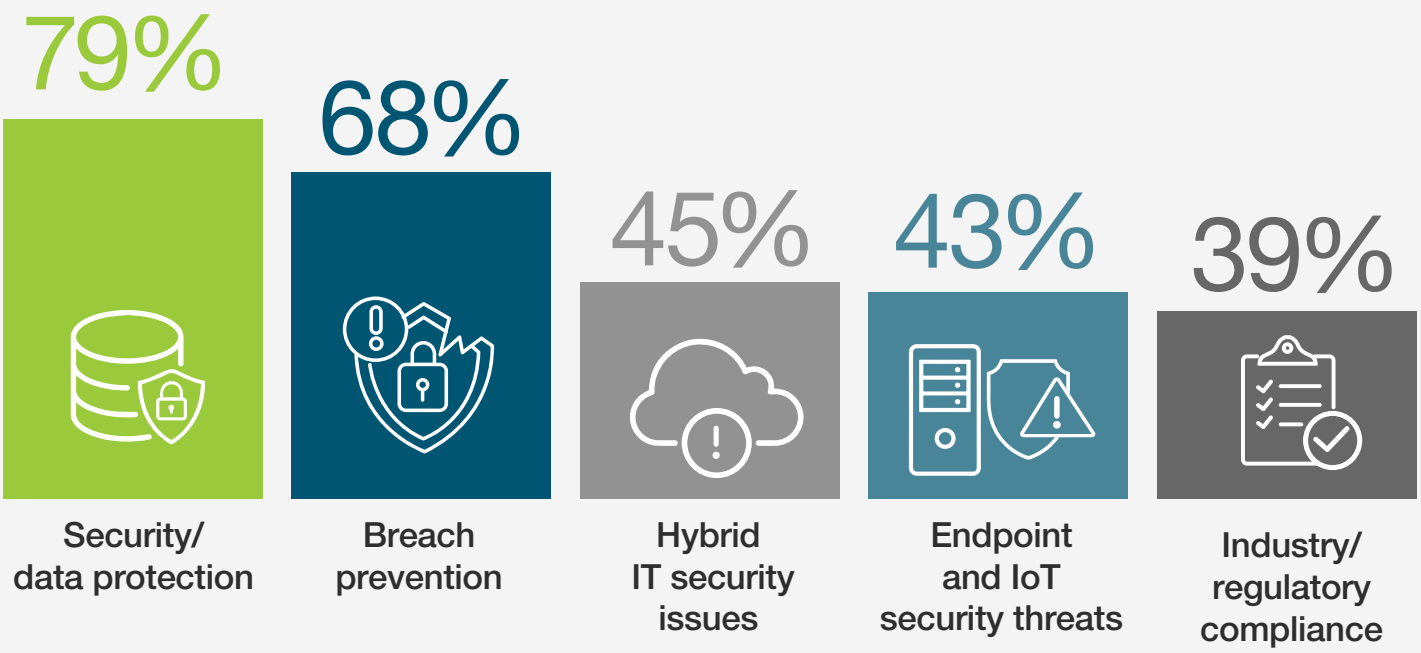
Initiating or augmenting an identity access/Zero Trust management program serves to tighten security controls, mitigate potential threats, and adhere to industry standards and regulations.

The primary drivers for implementing such programs are security/data protection (79%) and breach prevention (68%), demonstrating the central role that Zero Trust plays in fortifying an organization's cybersecurity posture. Surprisingly, despite the prominence of regulatory compliance, only 39% cite it as a driver, perhaps revealing a shift in focus from compliance to proactive security measures.

Interestingly, the need to address hybrid IT security issues and reduce endpoint and IoT security threats were highlighted by 45% and 43% of respondents respectively, reflecting the evolving threat landscape.

To enact a successful Zero Trust initiative, organizations should prioritize their goals, be it security, data protection, breach prevention, or compliance. An effective Zero Trust framework requires a holistic approach, addressing all aspects of an organization's security, from data protection to insider threats and regulatory compliance.

What are key drivers for your organization initiating/augmenting an identity access/Zero Trust management program? (Multiple responses allowed)



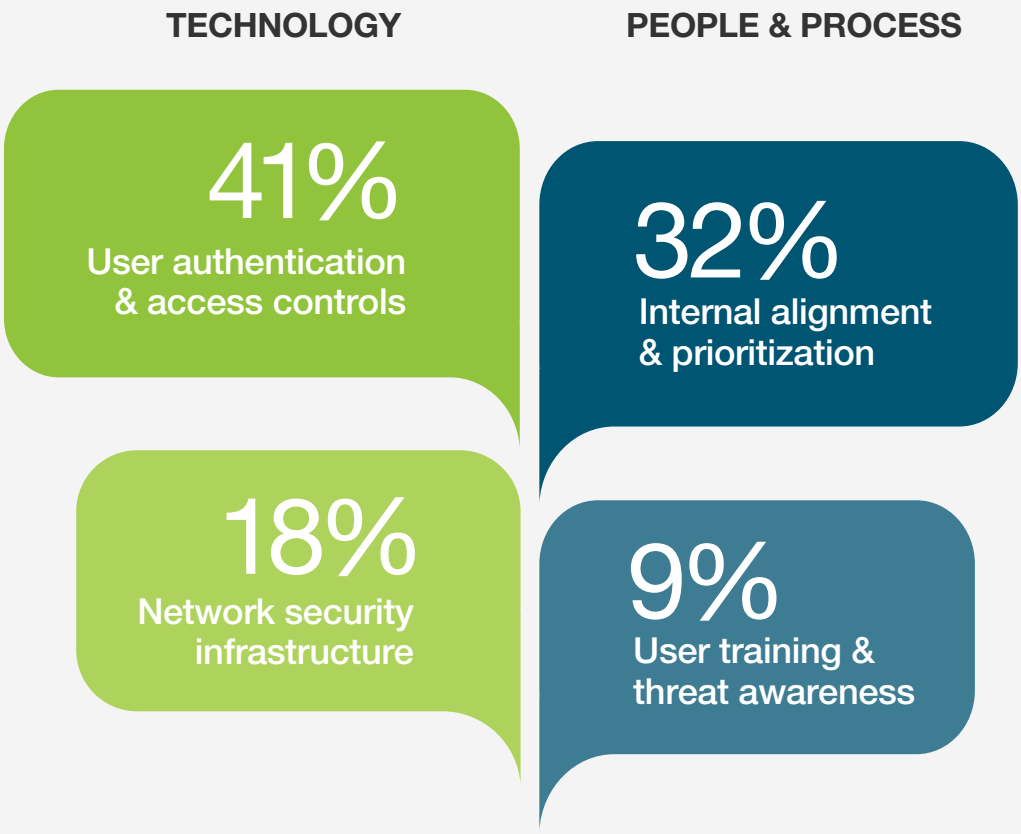
Reduce insider threats 38% | Operational efficiency 35% | Response to audit or security incident 28% | Internal compliance 25% | Other 3%

Accelerating Zero Trust Initiatives

The survey asked respondents about the single most crucial factor that could fast-track their Zero Trust initiative and enhance their security posture. A significant 41% of survey participants identified the improvement of user authentication and access controls as the most impactful way to expedite their Zero Trust initiatives. This highlights the importance of robust identity validation and nuanced access controls in implementing Zero Trust. Furthermore, 32% underscored the significance of internal alignment and prioritization, which is related to people and processes as opposed to technology, recognizing the essential role of organizational culture and collective buy-in required for successful security transformations.

To successfully deploy a Zero Trust model, organizations should balance technology with people-focused processes. On the technology side, it's crucial to invest in solutions that offer robust user authentication and granular access control. On the people and process side, fostering a security-conscious culture through education and ensuring organizational alignment with security objectives will accelerate the shift towards a Zero Trust framework.

What is the single biggest element that could greatly accelerate your Zero Trust initiative and enhance your security posture?



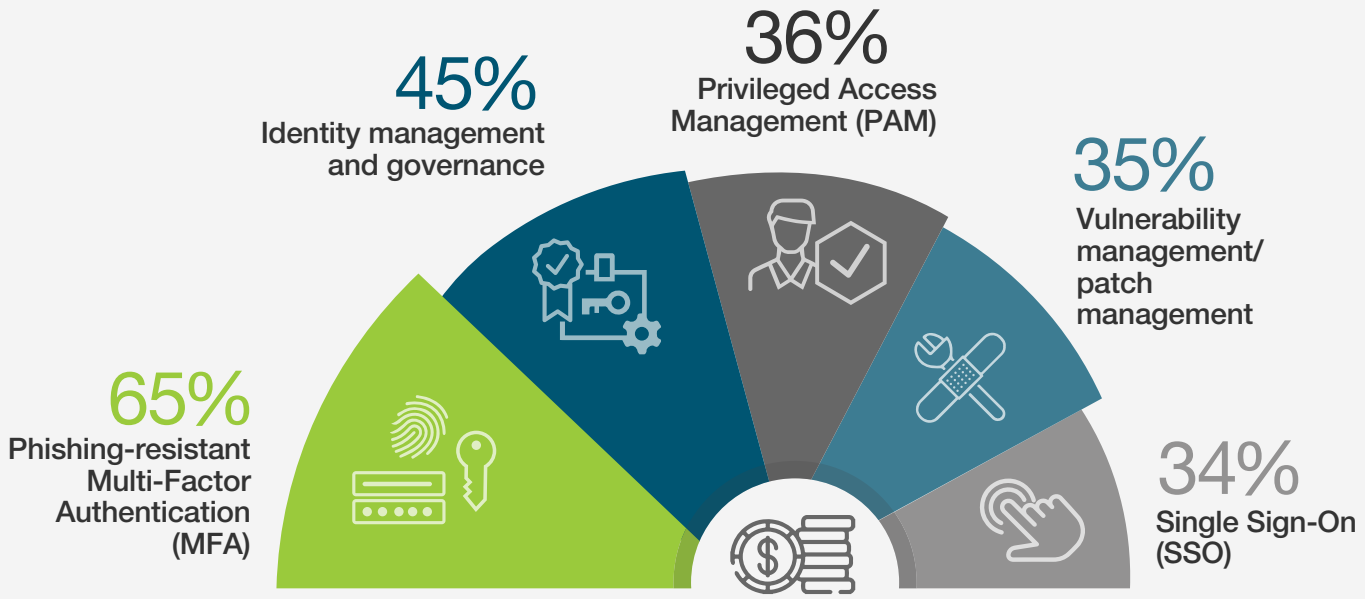
Investment Priorities

Next, we asked survey respondents which identity access and Zero Trust controls their organizations are prioritizing for investment over the next year.

Phishing-resistant multi-factor authentication (MFA) emerged as the highest priority, with 65% of organizations planning to invest in it. This indicates the crucial role of secure authentication in the Zero Trust model and the recognition of phishing as a prevalent threat. Meanwhile, 45% of respondents highlight the importance of identity management and governance, underscoring the importance of managing user identities and their access rights in a Zero Trust framework.

To act on these findings, organizations should focus on strengthening their authentication methods, particularly by implementing phishing-resistant MFA. Furthermore, enhancing identity management and governance systems is key, as it provides the necessary framework for managing user identities and access controls more effectively. Together, these measures will fortify an organization's defense and align with the Zero Trust model's emphasis on least privilege access and continuous verification.

Which of the following identity access/Zero Trust controls do you prioritize for investment in your organization within the next 12 months? (Multiple responses allowed)



Cloud Access Security Broker (CASB) 33% | Virtual Private Networks (VPN) 31% | Micro-segmentation 29% | Data Loss Prevention (DLP) 27% | Enterprise Mobile Management (EMM) 25% | Web Application Firewall (WAF) 25% | Complete control over Zero Trust network access 24% | Anti-phishing 23% | Network Access Control (NAC) 22% | Identity analytics 21% | Software Defined Perimeter (SDP) 19% | Network device invisibility to threats 15% | Mobile threat defense 13% | Enterprise directory services 10% | Digital Rights Management (DRM) 10% | Other 5%

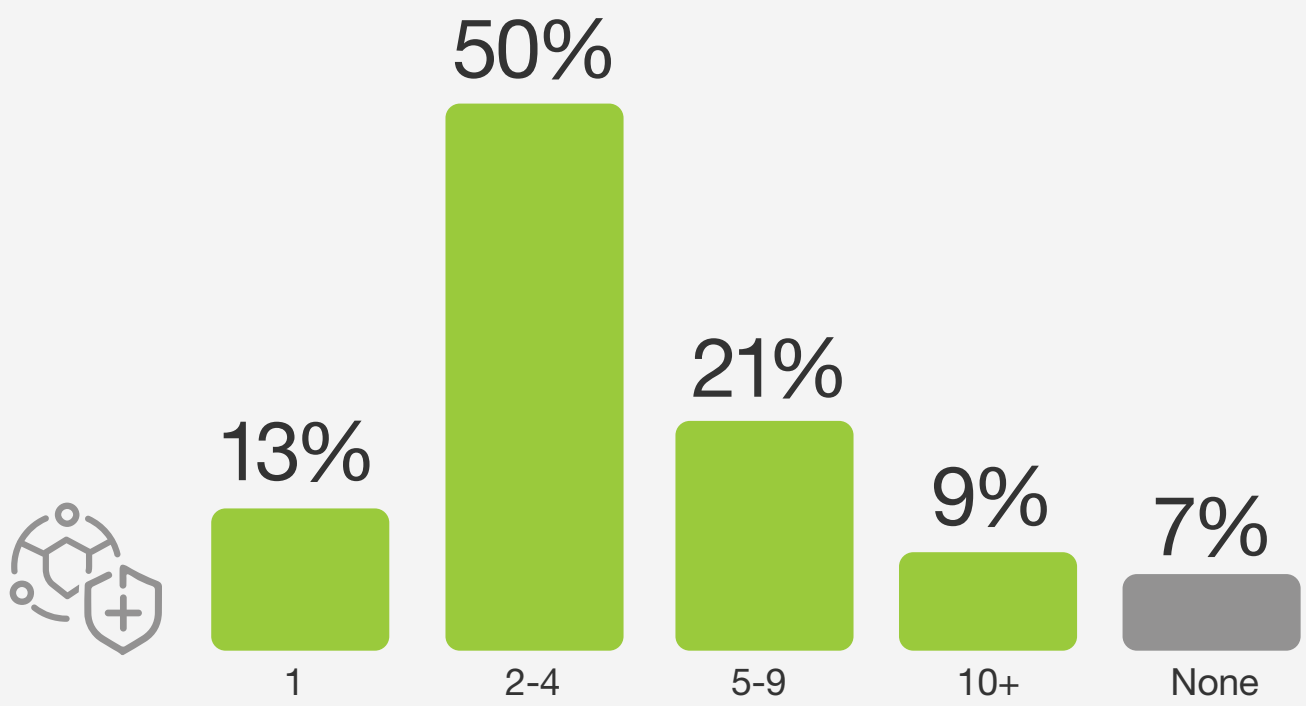
Product Usage for Zero Trust

How many products do organizations typically deploy for Zero Trust secure access programs?

The majority of organizations (63%) are using (or planning to use) between 1 and 4 products, which indicates a preference for streamlined, integrative solutions without overwhelming complexity. However, a substantial 30% are ready to manage 5 or more products, showcasing a willingness to invest in a wider array of technologies for comprehensive, layered security.

Organizations should choose solutions that fit their unique needs, considering the trade-off between complexity and comprehensiveness. Zero Trust entails integrated multi-layered defenses, so a multi-product strategy may be effective. However, it's crucial to ensure seamless interoperability among the chosen products to avoid security gaps and maintain efficiency.

How many products would you use (or currently use) for a Zero Trust secure access program at your organization?



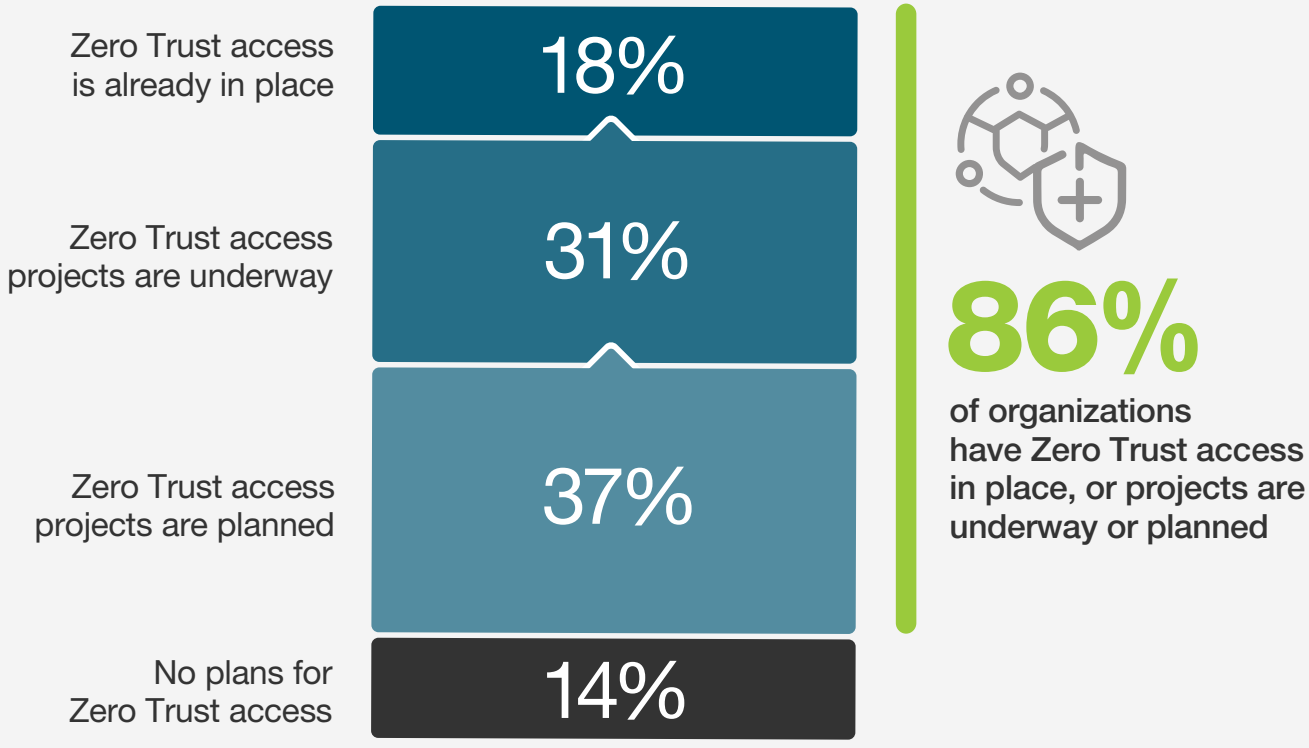
Number of products used for operating a Zero Trust secure access program

Zero Trust Adoption Plans

The survey reveals an encouraging trend — a substantial majority of organizations (86%) have either already implemented a Zero Trust access model (18%), have projects underway (31%), or have project plans in the pipeline (37%). A small but significant 14% of respondents have no plans to implement Zero Trust access, a potentially concerning gap in their security strategy.

Organizations with plans or ongoing projects should continue with their Zero Trust implementations, ensuring the process is methodical and robust, encompassing all aspects from user identities to devices. Those without plans should urgently reassess their strategies in light of the increasingly hostile threat landscape.

What plans do you have to adopt a Zero Trust access model within your company?



Zero Trust Adoption Timeframe

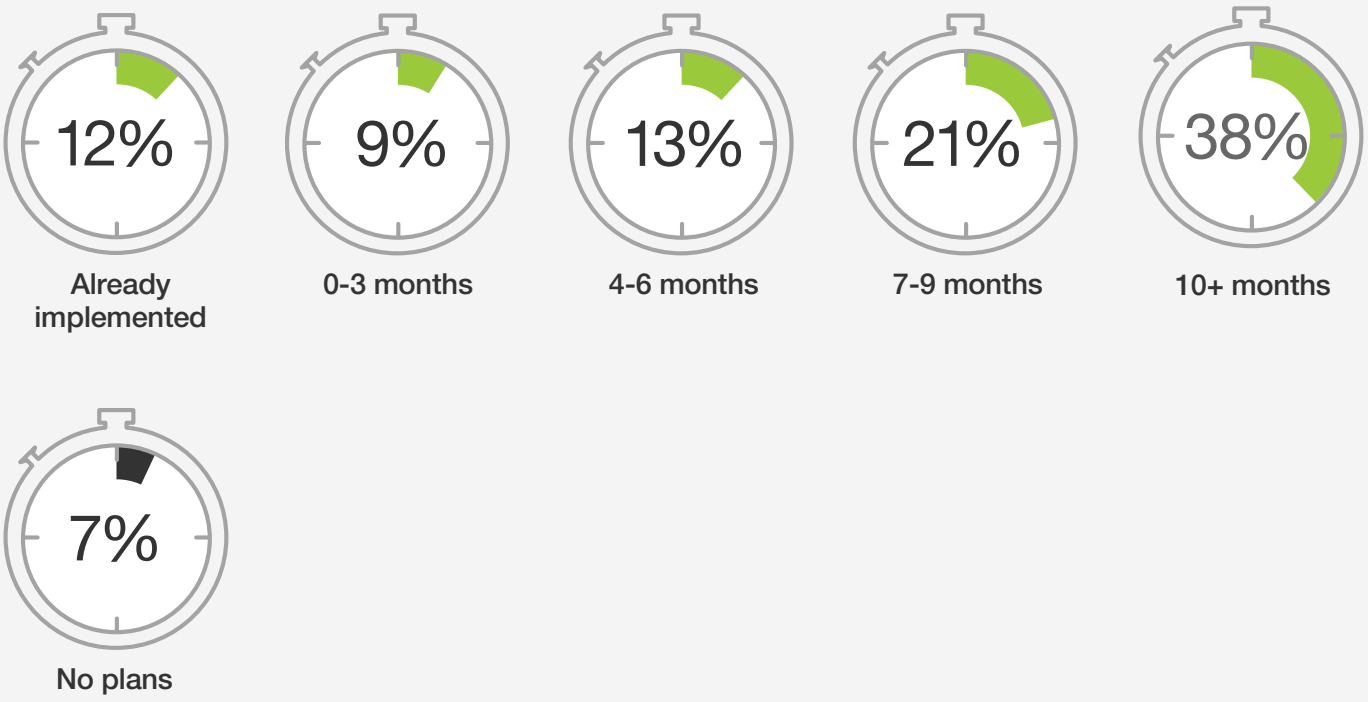
Understanding the planned timeframe for adopting Zero Trust security is important as it indicates organizational readiness and commitment to bolstering cybersecurity posture.

While 12% of organizations have already implemented Zero Trust security, the survey indicates that a combined 43% of organizations plan to adopt a Zero Trust security model within the next 9 months. On the other hand, a large group of respondents (38%) plan to adopt Zero Trust security in a more extended period, in 10 or more months.

For those planning adoption, it's advisable to start with a clear roadmap that aligns with business priorities and risk assessments. Those without plans should urgently consider the benefits of Zero Trust security in today's cyber threat landscape. For organizations that have already implemented Zero Trust architecture, it is crucial to adopt a continuous improvement approach to ensure its ongoing effectiveness.

In what timeframe will you most likely adopt Zero Trust security?

55% of organizations either have Zero Trust security or plan to implement it within nine months

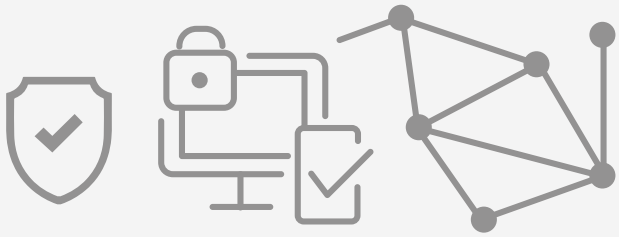


Quality of Zero Trust Implementation

The ability to effectively implement and use identity access and Zero Trust controls is vital, as these measures are the cornerstone of a robust security strategy. The survey reveals that organizations rate their successful implementation and usage of these controls at an average score of 5 on a scale ranging from 0 to 10. This midpoint score suggests that while many organizations have begun the journey towards Zero Trust, they acknowledge room for improvement in applying controls.

Organizations should seek to understand the gaps in their execution that prevent a higher score. Whether it's resource constraints, technological complexity, or a lack of stakeholder buy-in, these issues need to be addressed to advance their Zero Trust journey. Expanding training, aligning stakeholders, and investing in more seamless technological solutions can help organizations enhance their adoption score, improving their overall security posture.

On a scale from 0 to 10, how well has your organization implemented or used identity access/Zero Trust controls within the last 12 months?



Best Practices for the Zero Trust Journey

The journey towards Zero Trust is a process that involves strategic planning, smart investments, and a shift in mindset towards comprehensive security. Here are eight crucial steps that help guide you from the status quo to comprehensive Zero Trust adoption, providing you with key actions and best practices at each phase.

Inventory and Classify Data and Assets:

Understand what resources need to be protected. Start with an inventory of your organization's assets, classifying data according to its sensitivity and criticality.

Emphasize Strong, Phishing-Resistant Authentication:

Adopt strong, phishing-resistant multi-factor authentication. This not only adds an additional security layer, but also counters the most common types of cyberattacks.

Implement Least Privilege Access and Micro-Segmentation:

Adopt a least privilege strategy and segment access to resources. Only allow access to resources that users, applications, or devices absolutely need.

Automate and Regularly Update Security Policies:

Ensure that security policies are consistently applied and regularly updated. Automation can be a great asset in managing this.

Continuously Monitor and Analyze Behavior:

Adopt security solutions that offer continuous monitoring and anomaly detection. This enables swift detection and response to potential threats.

Secure Access to Applications and Data:

Implement controls to secure access to applications and data, irrespective of the location of the user or the hosting of the data.

Consolidate and Simplify Your Security Infrastructure:

Simplify your security stack and look for solutions that provide wide-ranging functionality. A consolidated infrastructure can provide a more robust and manageable security posture.

Educate Users and Foster a Culture of Security:

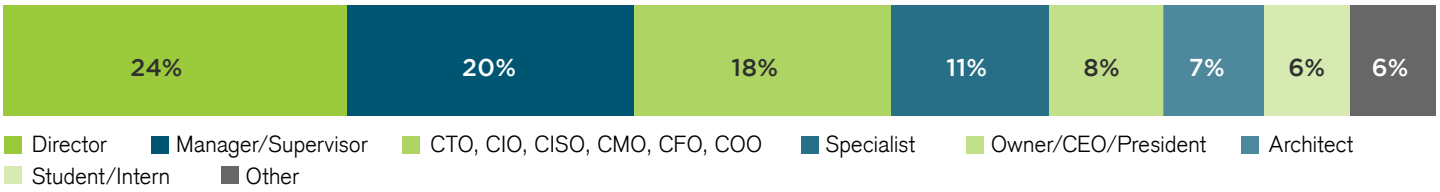
Build a culture of security across the organization. Training programs should be ongoing, including the principles of Zero Trust and the specifics of your implemented security tools.

Methodology & Demographics

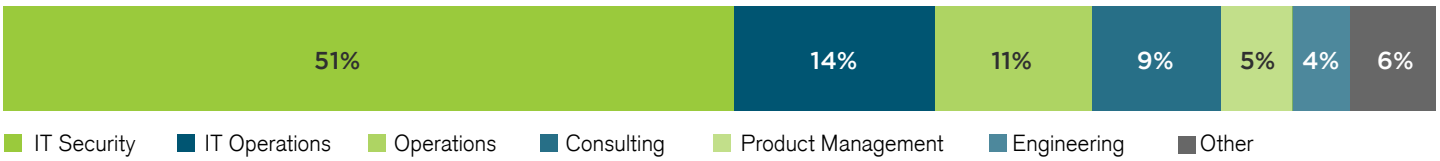
This report is based on the results of a comprehensive online survey of 423 IT and cybersecurity professionals in the US, conducted in June 2023, to identify the latest enterprise adoption trends, challenges, gaps, and solution preferences related to Zero Trust security.

The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

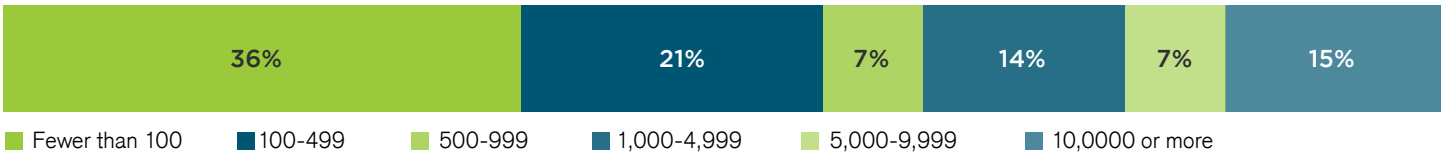
CAREER LEVEL



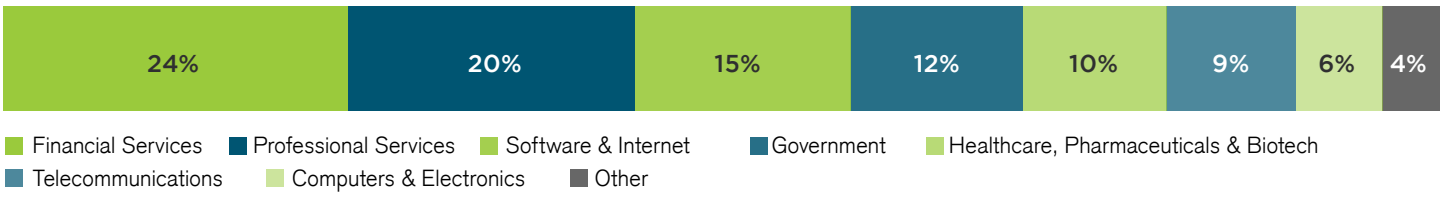
DEPARTMENT



COMPANY SIZE



INDUSTRY



yubico

Yubico, the inventor of the YubiKey, makes secure login easy and available for everyone. Since the company was founded in 2007, it has been a leader in setting global standards for secure access to computers, mobile devices, servers, browsers, and internet accounts. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering modern, hardware-based authentication security at scale.

YubiKeys are the gold standard for phishing-resistant multi-factor authentication (MFA), enabling a single device to work across hundreds of consumer and enterprise applications and services. Yubico's technology enables secure authentication, encryption, and code signing and is used and loved by many of the world's largest organizations and millions of customers in more than 160 countries.

Aligned with its mission of making the internet more secure for everyone, Yubico donates YubiKeys to organizations helping at-risk individuals through the philanthropic initiative, Secure it Forward. Yubico is privately held, with presence around the globe and offices in Palo Alto, San Francisco, Seattle, and Stockholm.

For more information, please visit **www.yubico.com.**

Cybersecurity
INSIDERS

Cybersecurity Insiders is a 600,000+ member online community for information security professionals, bringing together the best minds dedicated to advancing cybersecurity and protecting organizations across all industries, company sizes, and security roles.

We provide cybersecurity marketers with unique marketing opportunities to reach this qualified audience and deliver fact-based, third-party validation thought leadership content, demand-generation programs, and brand visibility in the cybersecurity market.

For more information please visit www.cybersecurity-insiders.com