Cybersecurity
INSIDERS

2023

Zero Trust Security Report

FORTRA

www.fortra.com

Overview

The 2023 Zero Trust Security Report reveals how enterprises are implementing Zero Trust security in their organizations, including key drivers, adoption trends, technologies, investments, and benefits.

To provide this information, we surveyed cybersecurity professionals ranging from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

Many thanks to Fortra for supporting this important research project.

We hope you'll find this report informative and helpful as you continue your efforts in protecting your IT environments.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

Key findings include:

- **Despite Zero Trust's importance, knowledge and readiness gaps persist.**
  Many cybersecurity teams buckle at the overhead that a Zero Trust framework implies. Some companies aren't ready to spend what it takes to do it properly. This may be reflected in the survey, in which only 15% of respondents indicated Zero Trust Network Access (ZTNA) was "already implemented" while another 9% said they had "no plans" to implement. Despite its fad-like identity, Zero Trust is an important security trend and ongoing philosophy that should take a key role in improving an organization's security maturity. And Zero Trust is not something organizations can ever mark "complete." Rather, Zero Trust is a journey, and continuous steps in the right direction will contribute to success and support incremental improvement.

- **Are over-privileged users the problem?**
  Respondents were divided. In one question, it was surprising to see that less than 25% of organizations' security incidents were believed to have been as a result of over-privileged users. This could indicate that respondents either misrepresented the root cause of events, or perhaps there's been a shift in strategy and compromise methods away from the user space and into other domains like SaaS and identity. However, in another question, over-privileged users were listed as a top challenge, indicating this is a moving target for organizations.

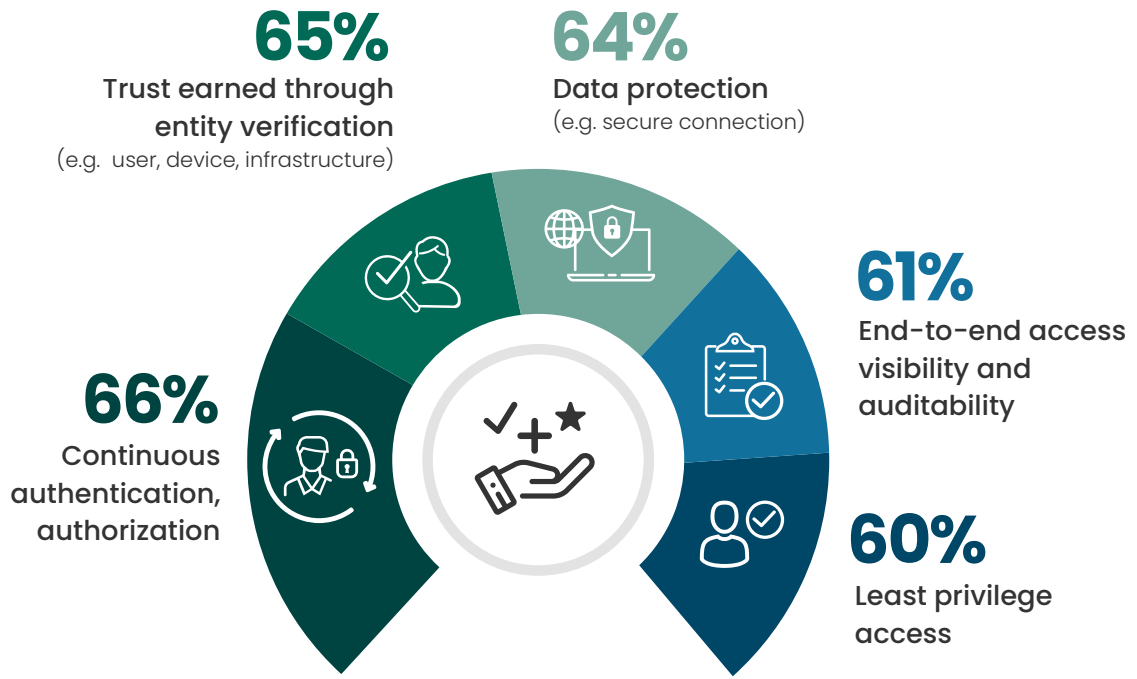
- **Device security needs more attention.**
  Many respondents identified the importance of protecting data but had mobile device management (MDM) and bring your own device (BYOD) low on their priority lists. Addressing BYOD can be complex, as privacy is the key to BYOD but it must be balanced with control. However, securing these devices should be a primary focus area as they are a major pain point today for corporate security teams in their intrusion prevention and data loss prevention (DLP) efforts.

Zero Trust Tenets

What aspects of Zero Trust are most compelling to organizations? Continuous authentication/authorization (66%), trust earned through verification of entities including users, devices, and infrastructure components (65%), and data protection (64%) top the list of core components of Zero Trust. This is followed by end-to-end access visibility and auditability (61%) and least privilege access (60%).

Overwhelmed security teams may have a hard time adding Zero Trust to already-full plates. And yet, the tenants of Zero Trust are clearly critical. This is becoming clear with initiatives such as the White House's National Cybersecurity Strategy which calls out Zero Trust principles as key to implement.

What Zero Trust tenets are most compelling to you and your organization?



Centralized, granular access policy 43% | No trust distinction between internal or external network 43% | Resource segregation 33% | Other 3%

Zero Trust Confidence

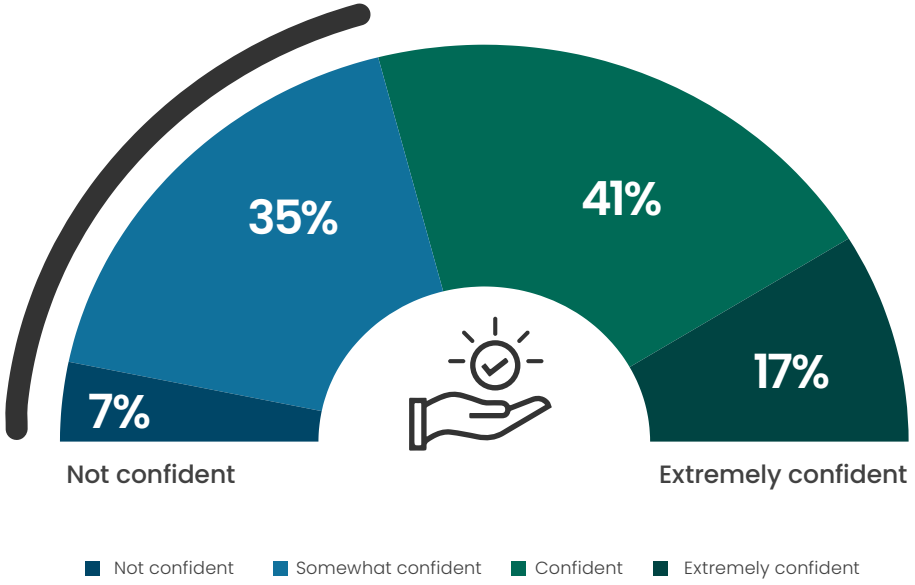
The low rate of respondents who are "extremely confident" in the Zero Trust model seems to indicate pervasive readiness concerns with moving to a Zero Trust architecture.

What are the impediments and challenges these teams are experiencing?
One major gap many organizations face is internal communication and alignment around Zero Trust initiatives. Zero Trust is a journey, not a destination. Internal alignment will help organizations commit to the journey and choose their first steps to take.

EXPERT TIP:
Don't try to boil the ocean. Many businesses make faster headway with Zero Trust when they move step by step, identifying opportunities system by system to reduce risk and privilege.

How confident are you to apply the Zero Trust model in your secure access architecture?

42%
of enterprise IT security teams lack or have low confidence in their ability to provide Zero Trust



Drivers for Zero Trust

Respondents said that security and data protection (79%) was a top driver for Zero Trust, which isn't surprising. Most organizations' value can be found in their data, and most organizations have assets that should not be compromised. For any business with assets in need of protection, start by identifying your core assets and the threats to those assets so you can take steps to protect them.

EXPERT TIP:
Vulnerability management scanning allows organizations to identify their security gaps before attackers can. Vulnerability management focuses on the infrastructure side of vulnerabilities rather than those resulting from overprovisioned access. Fortra's Digital Defense can offer proactive breach prevention to help.

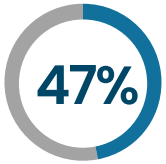
Layered data protection solutions are also key to understanding, governing, and protecting data in a Zero Trust model.

What are key drivers for your organization initiating/augmenting an identity access/Zero Trust management program?

79%
Security/ data protection

68%
Breach prevention

51%
Reduce endpoint and IoT security threats



Address hybrid IT security issues

Industry/regulatory compliance (e.g., HIPAA, GDPR, PCI DSS)

Reduce insider threats

Operational efficiency

Response to audit or security incident 27% | Internal compliance 25% | Other 2%

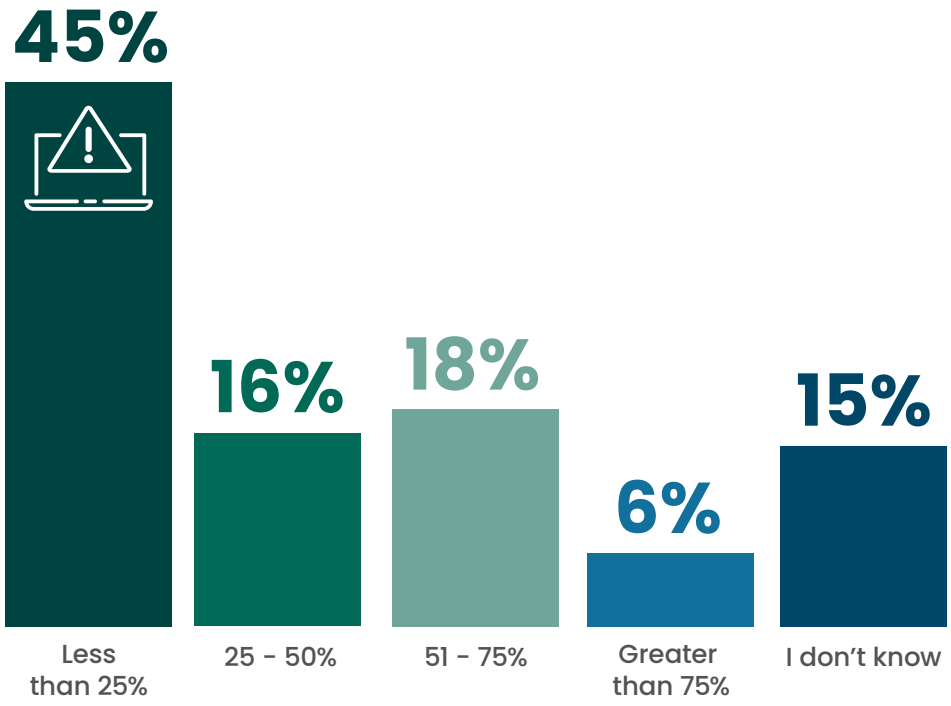
Excessive Privilege Risk

It is surprising to see that almost half of the respondents believe that less than 25% of their incidents could have been resolved by a better least privilege/ZTNA approach. In other words, many respondents were not convinced that excessive privilege risk is a major cause of incidents. We would have expected to see otherwise. Regardless of the cause of incidents, identifying opportunities to reduce privilege is key to a Zero Trust model. Every business will look different and it comes down to identifying what your business needs are in this area.

EXPERT TIP:

There will always be over-privileged users. Pursuing data-centric security allows you to protect files regardless. Secure file transfer solutions offer encryption and automation to enable efficient collaboration and still prioritize file security. And in combination with secure collaboration solutions, security travels with the file to prevent exploitation by over-privileged users.

What percentage of your organization's security incidents in the last 12 months do you believe were caused by end users possessing access privileges beyond what they require for their daily work?



Percentage of user incidents caused by excessive access privileges

Identity Access and Zero Trust Priorities

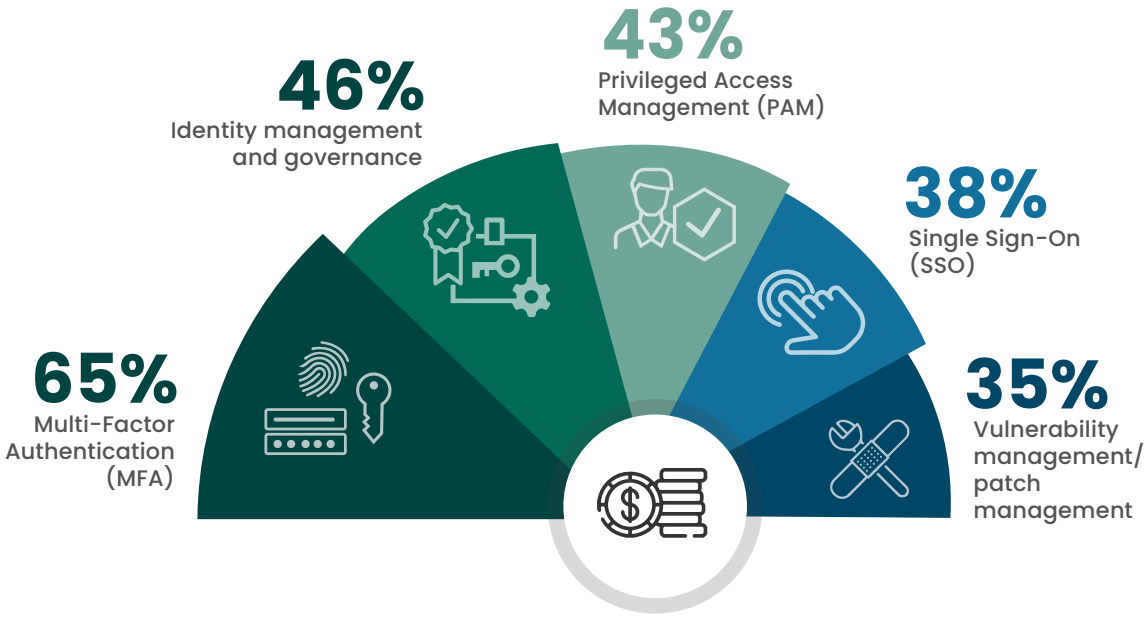
Investments in access controls like PAM (43%) are prioritized higher than SSO (38%). These results are unexpected given that almost half of the respondents believe that less than 25% of their incidents could have been resolved by a better least privilege/ZTNA approach.

Micro-segmentation (34%) is ranked higher than expected on this list, with MDM (29%) and Anti-Phishing (28%) lower than expected due to their importance and prevalence. Enterprise directory (9%) being at the very bottom confirms that the days of the old Active Directory, on-prem style systems are over and they need to be decommissioned across the board.

EXPERT TIP:

Fortra offers leading cybersecurity solutions in many of the areas on this list. Whether your priority is identity governance, PAM, vulnerability management, anti-phishing, or DLP, we can help in your ongoing journey to apply a Zero Trust mindset.

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



Micro-segmentation 34% | Virtual Private Networks (VPN) 33% | Enterprise Mobile Management (MDM) 29% | Anti-Phishing 28% | Cloud Access Security Broker (CASB) 28% | Complete control over Zero Trust network access 27% | Web Application Firewall (WAF) 26% | Network Access Control (NAC) 25% | Identity analytics 24% | Software Defined Perimeter (SDP) 24% | Network device invisibility to threats 20% | Data Loss Prevention (DLP) 17% | Mobile Threat 16% Defense 13% | Enterprise directory services 9% | Digital Rights Management (DRM) 9% | Other 5%

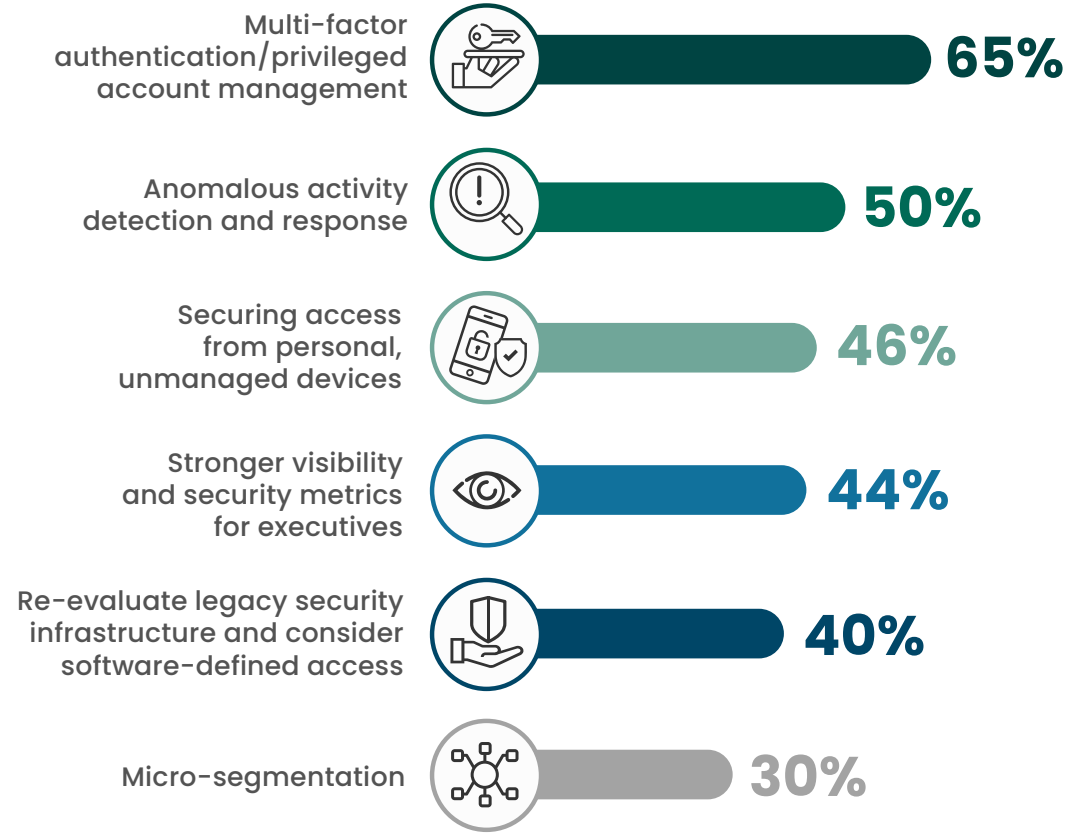
Secure Access Priorities

When we drill down into specific secure access priorities, organizations again prioritize multi-factor authentication/privileged account management (65%). This is followed by anomalous activity detection and response (50%) and securing access from personal, unmanaged devices (46%).

Zero Trust comes down to determining the needs of your business and applying the appropriate controls. No one security control will solve Zero Trust, but all are pieces of the puzzle.

EXPERT TIP:
For those looking for Privileged Account Management solutions, Fortra's Core Security solutions can help.

What are your organization's secure access priorities for the next 1-2 years?



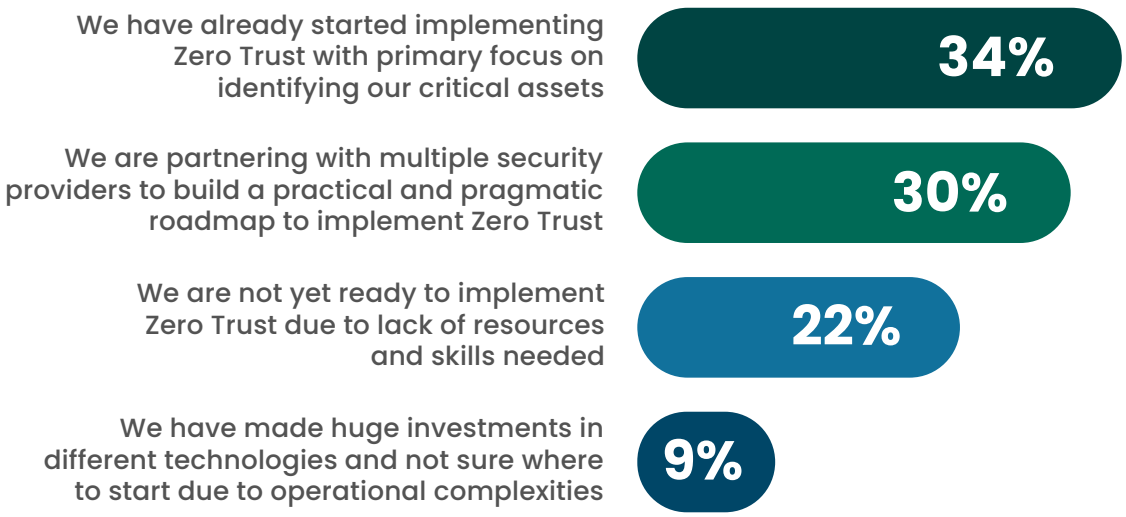
Other 2%

Zero Trust Implementation

It is encouraging to see 34% of respondents getting started and focusing on their critical assets first. Thirty percent of respondents partnering with multiple providers to build their roadmap indicates there is a need for more Zero Trust education. Before bringing on partners, talk internally first. Get a team together, have a conversation, and establish the problem you want to solve.

No one vendor can solve every part of the Zero Trust story, but having an ally along the way can be incredibly helpful.

Zero Trust implementation is a gradual process. How are you planning to implement Zero Trust across your extended environment?

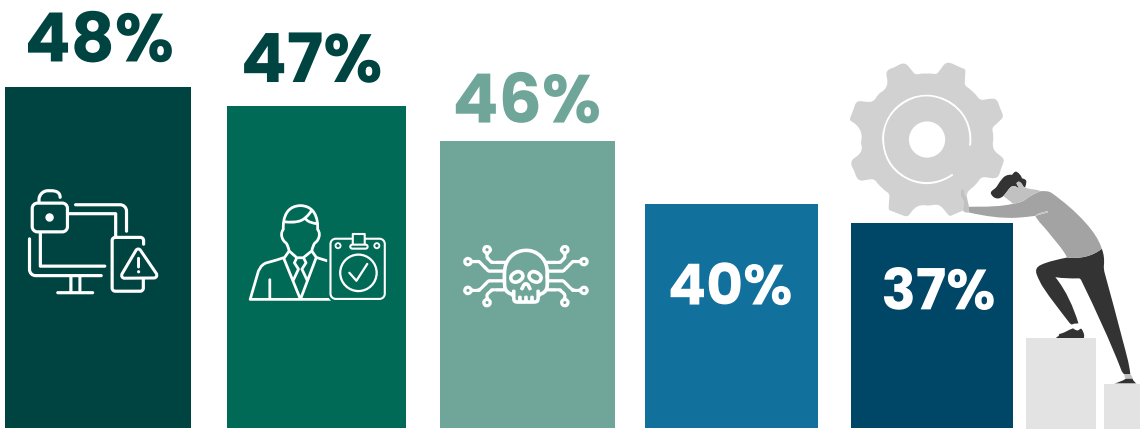


Other 5%

Secure Access Challenges

What are the biggest challenges regarding secure access mentioned by organizations in our survey? At-risk devices tops the list (48%), followed by over-privileged employee access (47%), a moving target on the priority lists.

What top challenges is your organization facing when it comes to securing access to applications and resources?



At-risk devices accessing network resources (unknown, unsanctioned, non-compliance endpoints)

Overprivileged employee access

Cyber attacks (e.g., denial of service, cross-site scripting, man-in-the-middle, phishing)

Shadow IT

Manual processes are complex and slow down ability to react quickly

Other 5%

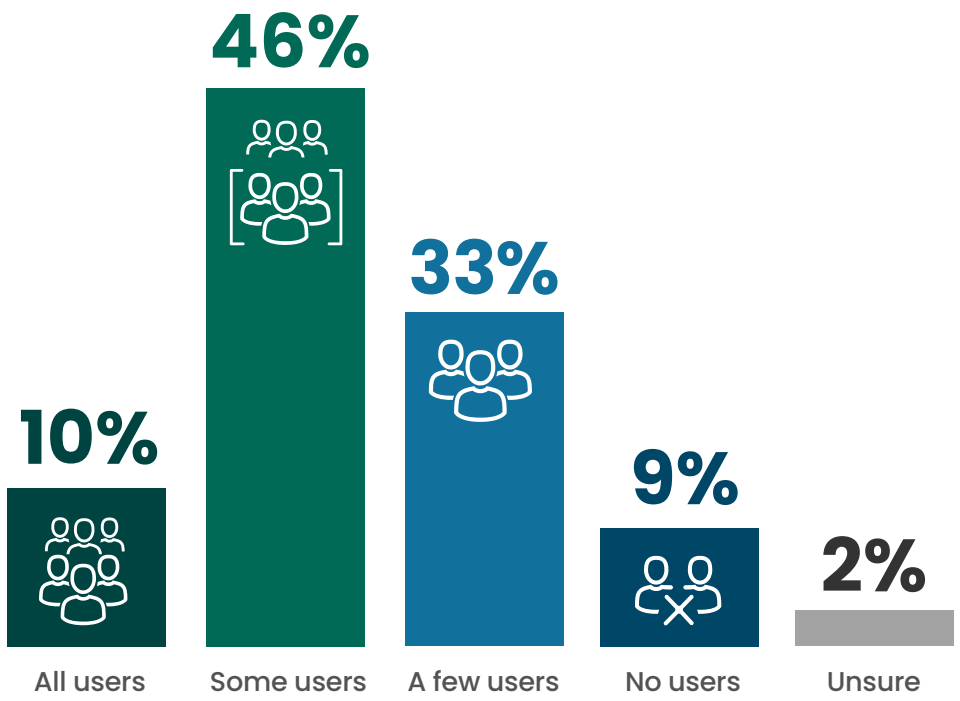
EXPERT TIP:

We recommend taking an integrity-focused approach to Zero Trust. After setting up systems in a known and secure state, integrity controls are required to ensure ongoing trustworthiness and identify when something changes that shouldn't have. Fortra's Tripwire has solutions to help monitor and control access to assets.

Excess Access Privileges

Given the recent news of security breaches, it is surprising that 46% of respondents selected "some users" as having excessive access privileges beyond what they require.

To what extent do you believe users in your organization have access privileges beyond what they require?



EXPERT TIP:
Regardless of access privileges, combining secure file transfer and collaboration technology can ensure access control no matter where files travel. For organizations handling intellectual property, M&A files, sensitive video footage, and other files, a solution like SFT Rights Management can protect files from over-privileged users.

Zero Trust Adoption

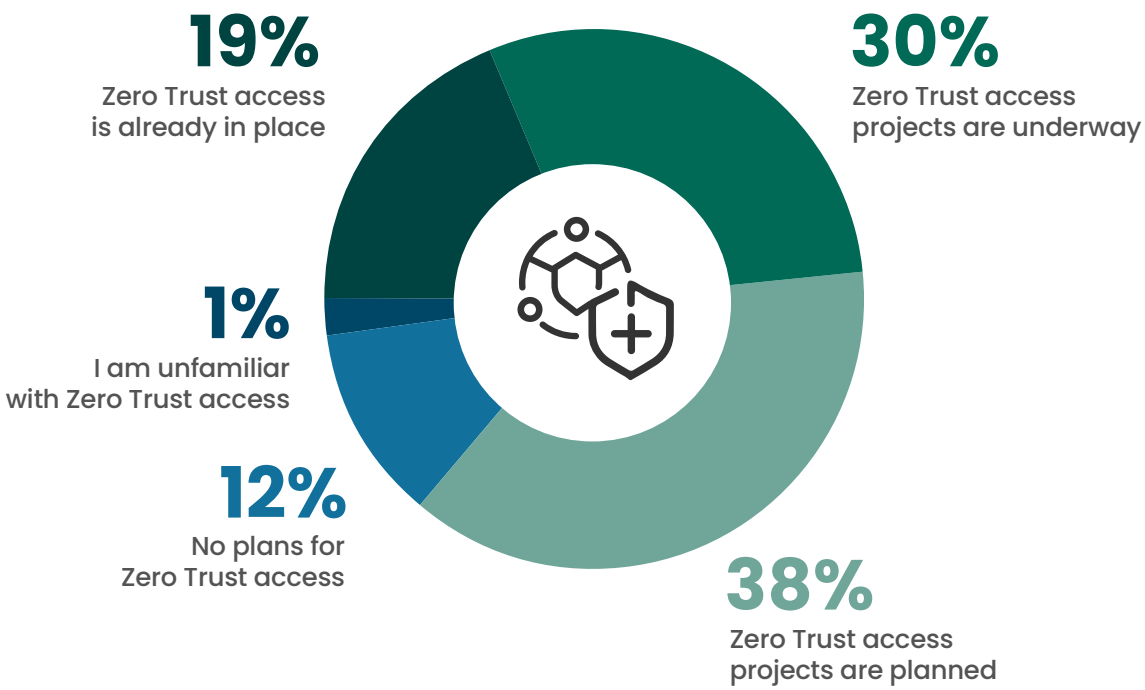
The concept of Zero Trust is quickly gaining momentum. Eighty-seven percent said their organizations have Zero Trust access in place or have projects underway or planned.

Only 12% of organizations have no plans for Zero Trust access.

EXPERT TIP:

There's no shortage of resources available for organizations to learn about Zero Trust. For organizations who have no plans to adopt a Zero Trust access model, it is important to take time to understand the concept. As with many buzzwords, confusion and lack of clarity has impeded understanding of this approach to protecting data for many. Fortra put together this guide around what Zero Trust is and why it matters as a helpful starting point.

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



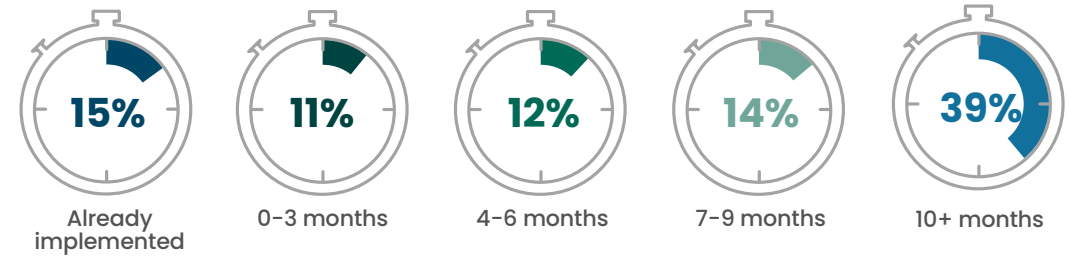
Zero Trust Adoption Timeframe

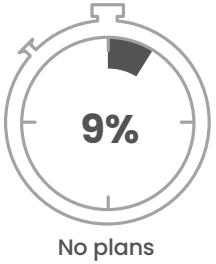
When asked about the timeframe in which organizations will adopt Zero Trust security, a majority (52%) either have Zero Trust security in place or are planning on implementing it within 9 months.

Only a small portion (9%) have no current plans for adoption of Zero Trust. Again, education is key here. Zero Trust should be a key part of an organization's security posture and an ongoing initiative.

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

52% of organizations either have Zero Trust security or plan to implement it within nine months





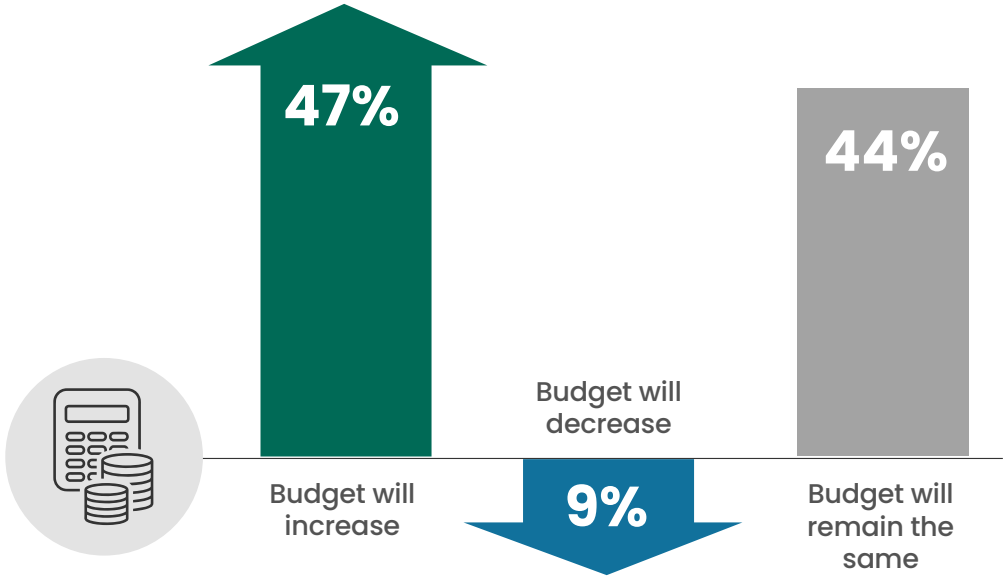
On a scale from 0 to 10, how well has your organization implemented or used identity access/Zero Trust controls within the last 12 months?

Zero Trust Budget

Almost half of the organizations (47%) expect their access management related budgets will increase in the next 18 months.

This is a significant gain for cybersecurity and all industries that have any sort of connected technologies.

How do you expect your organization's Zero Trust related budget to change over the next 18 months?



Security Priorities

When asked about their current security priorities, cybersecurity professionals mentioned improved IAM (57%) most frequently, followed by secure application access (52%) and supplementing Endpoint Detection and Response (EDR) (46%).

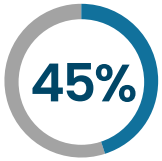
EXPERT TIP:
Talk to Fortra if you are looking for leading Identity and Access Management, vulnerability management, Data Loss Prevention, or Rights Management solutions.

What are your organization's current security priorities?

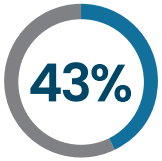
57%
Improve Identity and Access Management (IAM)

52%
Ensure secure access to applications hosted on cloud service providers
(e.g., Microsoft, Amazon, Google)

46%
Supplement Endpoint Detection and Response (EDR)

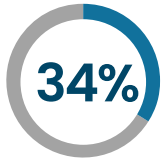


Improve vulnerability remediation
(e.g. Vulnerability Management, Patch Management)



Data Loss Prevention (DLP)

Augment or replace existing remote access tools
(e.g., VDI, VPN, RDP)



Simplify secure access delivery
(e.g., user experience, administration)

Conduct Deep SSL Inspection (e.g. secure session decryption for malware scanning and web/email filtering) 30% | Enable Endpoint Mobile Management (EMM)/BYOD (e.g. users, devices) 29% | Provide better mobile threat protection (Mobile Threat Defense/Anti-Phishing) 27% | Enhance SD-WAN security functions 22% | Encrypt sensitive information (e.g. digital rights management) 17% | Other 3% | None 1%

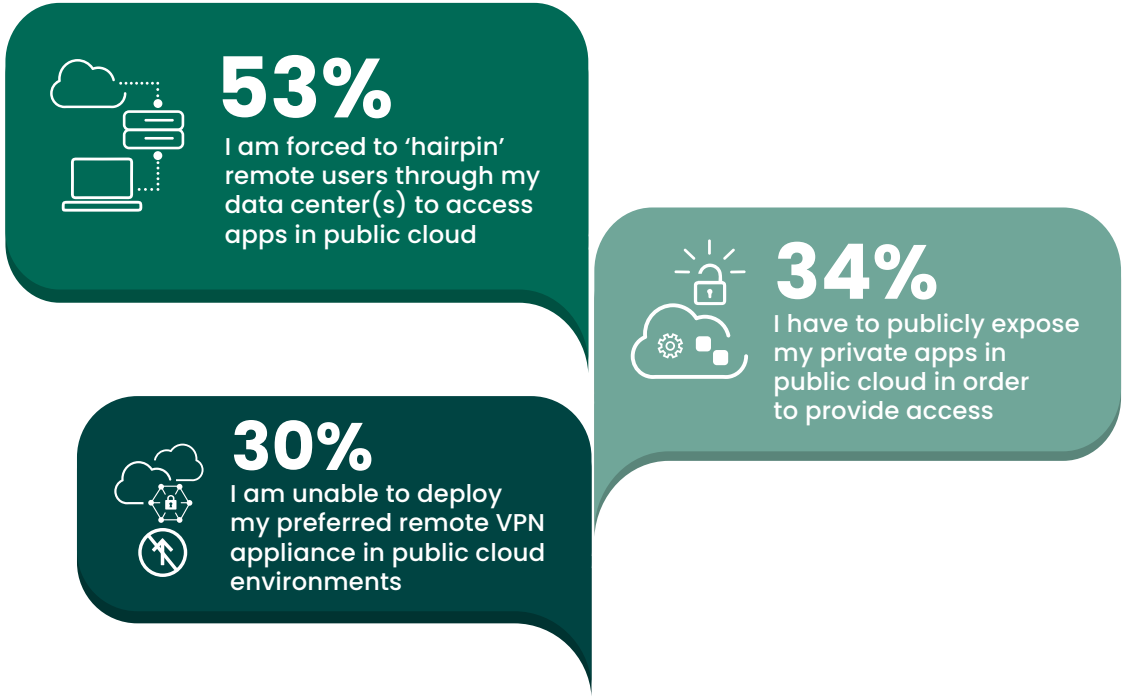
Access to Apps in Public Clouds

Traditional remote access solutions are failing the requirements of today's dynamic and distributed cloud environments.

When asked about the scenarios cybersecurity professionals encounter when providing secure access to cloud apps, the most mentioned workaround is "hairpinning" remote and mobile users through data centers to access public app clouds (53%).

An alarming 34% have to publicly expose cloud apps to enable remote and mobile users, thereby introducing significant risk.

Which of the following scenarios have you encountered when providing secure access to public cloud apps for remote or mobile users?



FORTRA

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers.

Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world.

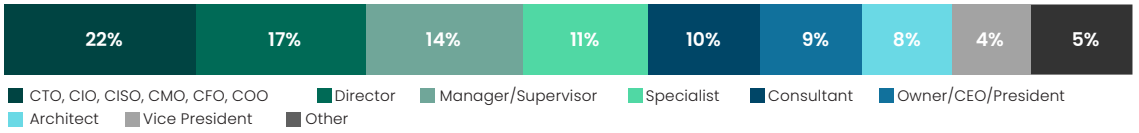
We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey.

Learn more at fortra.com.

Methodology and Demographics

This report is based on the results of a comprehensive online survey of 398 IT and cybersecurity professionals in the US, 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.

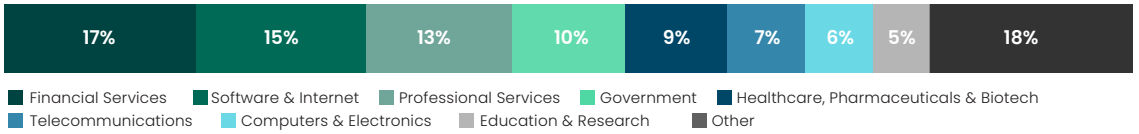
CAREER LEVEL



DEPARTMENT

COMPANY SIZE

INDUSTRY



Cybersecurity
INSIDERS

Cybersecurity Insiders is a 500,000+ 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