ivanti

Cybersecurity
INSIDERS

2023 Zero Trust Progress Report



ivanti.com

Overview

Zero Trust, built upon the fundamental premise of “never trust, always verify,” is becoming a cornerstone in today’s cybersecurity practices.

The 2023 Zero Trust Progress Report, based on a survey of 431 IT and cybersecurity professionals, provides a comprehensive analysis of the rising adoption, key challenges, and effective strategies surrounding Zero Trust access models in today’s organizations.

The survey reveals that 68% of respondents are planning or actively working towards adopting a Zero Trust access model. On their path to Zero Trust, organizations focus on a holistic approach to security, with 57% prioritizing Identity and Access Management (IAM) and 52% aiming to secure cloud application access. Along with supplementing Endpoint Detection and Response (EDR) and improving vulnerability remediation, these priorities confirm an increasing adoption of Zero Trust security practices.

At-risk devices accessing network resources were identified as the top challenge by 48% of respondents, emphasizing the importance of strict device verification and continuous monitoring. Overprivileged employee access, a concern for 47% of respondents, underlines the need to implement the least privilege principle in a Zero Trust framework.

Investment in Multi-Factor Authentication (MFA) stands out as the top priority for 65% of respondents, emphasizing its importance in the Zero Trust framework. Most organizations (54%) use 2-4 products for Zero Trust, suggesting a layered approach to implementation.

As the cybersecurity landscape evolves, adopting Zero Trust principles and aligning security priorities with them will be crucial for organizations to mitigate risks and protect their assets effectively.

We extend our appreciation to Ivanti for supporting this critical research and hope it serves as a useful resource for your ongoing journey to protect your IT environments.

Thank you,

Holger Schulze



Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity INSIDERS

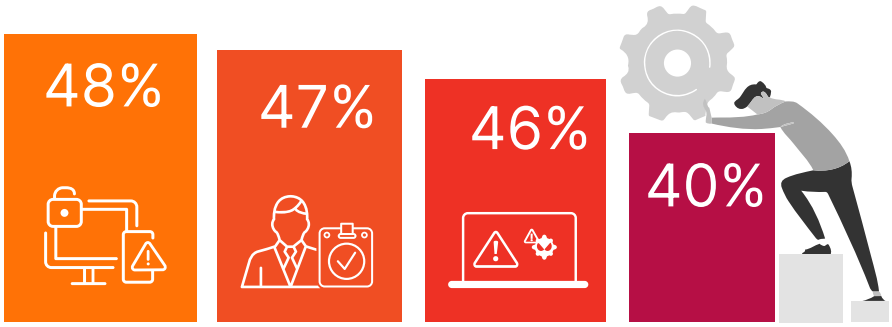
©2023 Cybersecurity Insiders All Rights Reserved.

Secure Access Challenges

The top challenges organizations face in securing access to applications and resources are closely related to the core principles of Zero Trust. The highest concern, at 48%, is at-risk devices accessing network resources – moving to the number one spot since last year. This challenge underscores the need for Zero Trust's strict device verification and continuous monitoring, ensuring that only trusted devices gain access to sensitive resources.

Overprivileged employee access is another significant challenge, with 47% of respondents identifying it as a concern. In the context of Zero Trust, this highlights the importance of implementing the principle of least privilege, ensuring that users only have the minimum necessary access rights to perform their job functions.

What top challenges is your organization facing when it comes to securing access to applications and resources?[1] [n = 424]



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

Security Priorities Reflect Zero Trust Focus

The chosen security priorities suggest that organizations are adopting a holistic approach to security, addressing multiple layers of protection. The strong focus on IAM (57%) and secure access to cloud applications (52%) is highly relevant to Zero Trust security, as these priorities align with the principles of verifying user and device identities and controlling access to resources. Additionally, the emphasis on supplementing EDR (46%) and improving vulnerability remediation (45%) reflects the Zero Trust principle of continuous monitoring and rapid response to security threats. Overall, these priorities indicate that organizations are increasingly adopting Zero Trust security practices to enhance their overall cybersecurity posture.

What are your organization's current security priorities? [n = 421]



57%

Improve Identity and Access Management (IAM)



52%

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



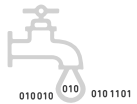
46%

Supplement Endpoint Detection and Response (EDR)



45%

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



43%

Data Loss Prevention (DLP)



40%

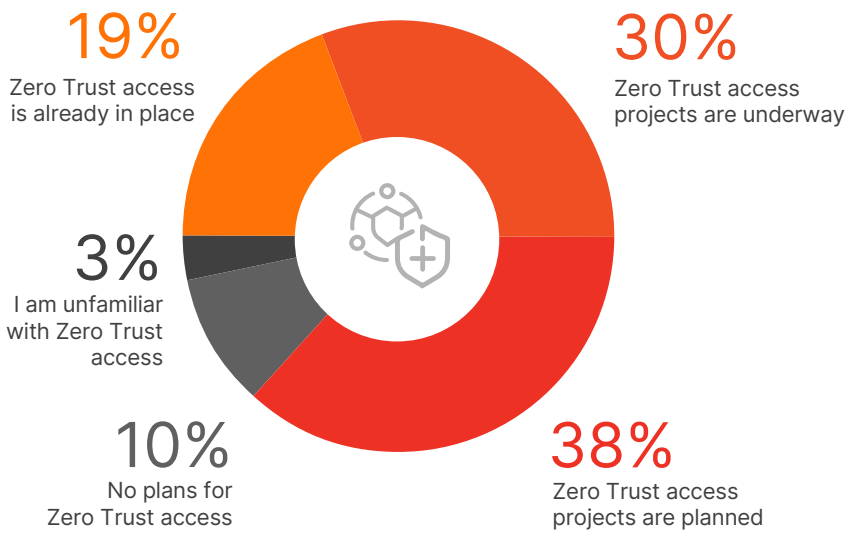
Augment or replace existing remote access tools (e.g., VDI, VPN, RDP)

©2023 Cybersecurity Insiders All Rights Reserved.

Zero Trust Adoption Plans

With Zero Trust already in place for one in five organizations (19%), a significant portion of respondents (38%) have plans to implement Zero Trust access projects, and 30% already have projects underway. This suggests that most organizations surveyed (68%) are either planning or actively working towards adopting a Zero Trust access model.

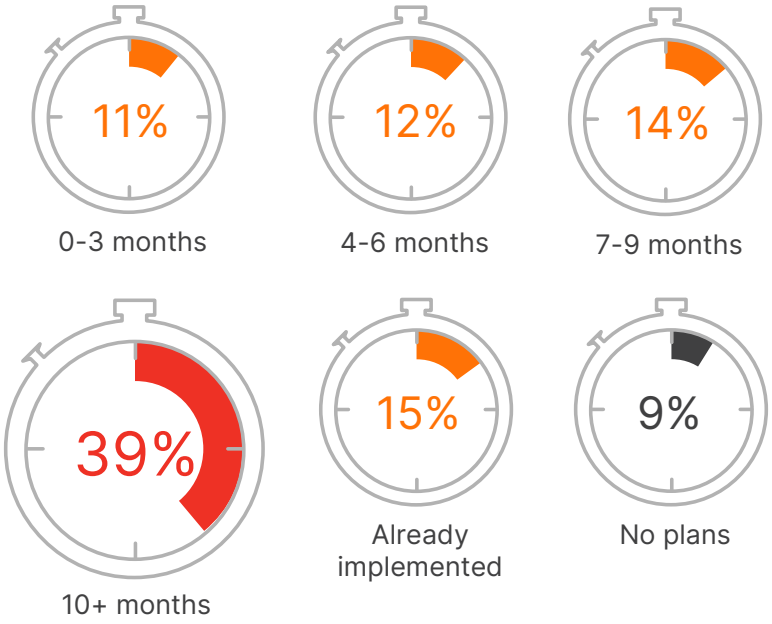
What plans do you have to adopt a Zero Trust access model within your company? [n = 424]



Zero Trust Adoption Timeframes

Adoption of Zero Trust security is occurring at various rates among organizations. While a considerable portion has already implemented the framework (15%), others plan to adopt Zero Trust relatively soon (37% within 9 months), and a sizable group recognizes that it may take 10 or more months to fully embrace Zero Trust security (39%).

In what timeframe will you most likely adopt Zero Trust security? [n = 423]

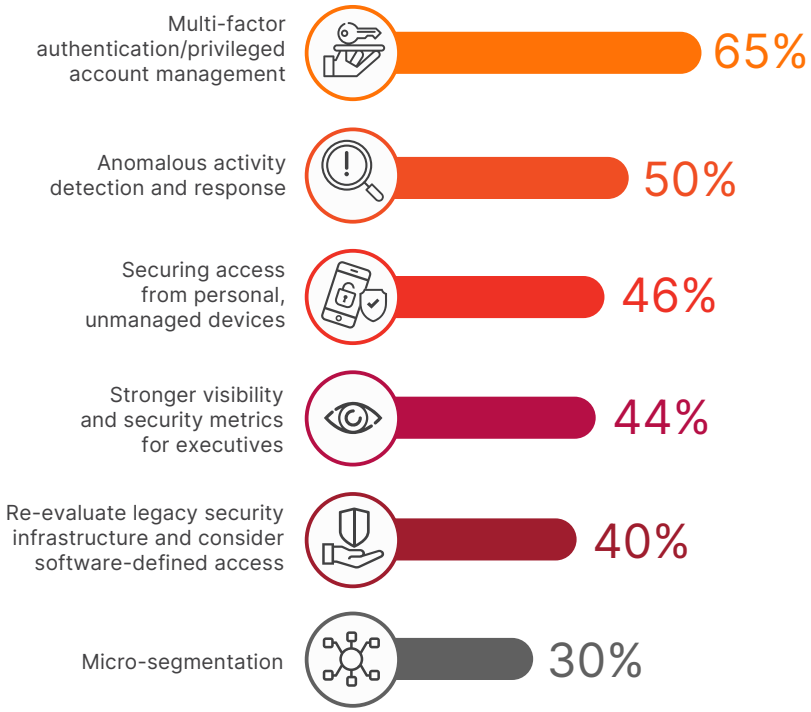


©2023 Cybersecurity Insiders All Rights Reserved.

Secure Access Priorities

Organizations are focusing on multiple secure access priorities that are closely aligned with Zero Trust principles, such as Multi-Factor Authentication (MFA) (65%), real-time threat detection (50%), and securing access from personal devices (46%). This aligns well with the Zero Trust principle of "never trust, always verify," ensuring that users are properly authenticated and authorized before granting access to sensitive resources.

What are your organization's secure access priorities for the next 1-2 years? [n = 430]

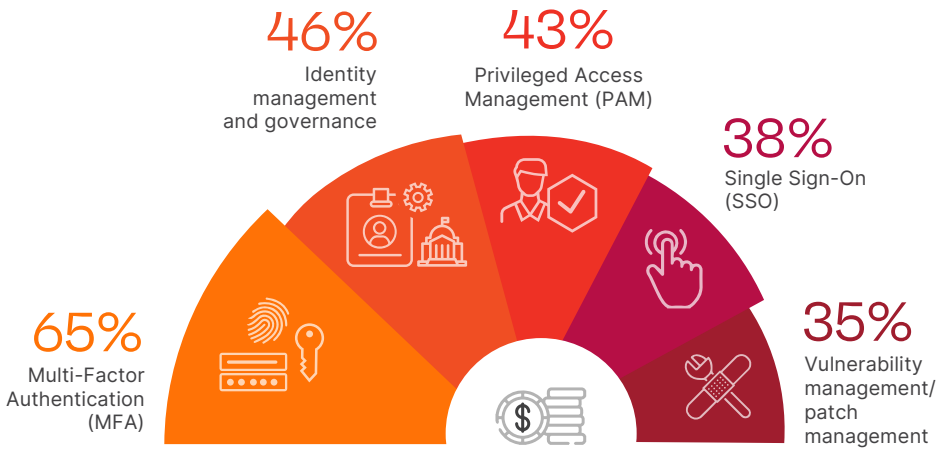


Investment Plans

Organizations' investment priorities for identity access and Zero Trust controls are focused on enhancing user authentication, managing access rights, and maintaining overall system security. MFA, a key component of Zero Trust, stands out as the top priority, with 65% of respondents planning to invest in it.

These priorities reflect the core principles of Zero Trust, indicating a growing emphasis on adopting this security framework across organizations.

Which of the following identity access/Zero Trust controls do you prioritize for investment in your organization within the next 12 months?[2] [n = 431]

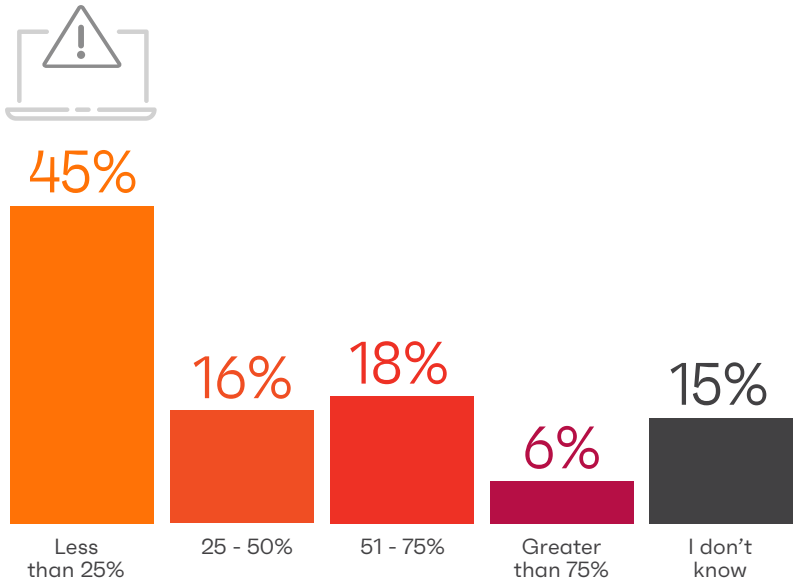


©2023 Cybersecurity Insiders All Rights Reserved.

Risk From Excessive Access Privileges

For nearly half of the respondents (45%), overprivileged access accounted for less than 25% of security incidents. This suggests that, while overprivileged access is a concern, it is not the primary driver of security incidents for many organizations. A third of organizations (34%) experienced 25%-75% of incidents due to excessive access privileges. These findings emphasize the importance of implementing the Zero Trust principle of least privilege to minimize security risks related to excessive access privileges.

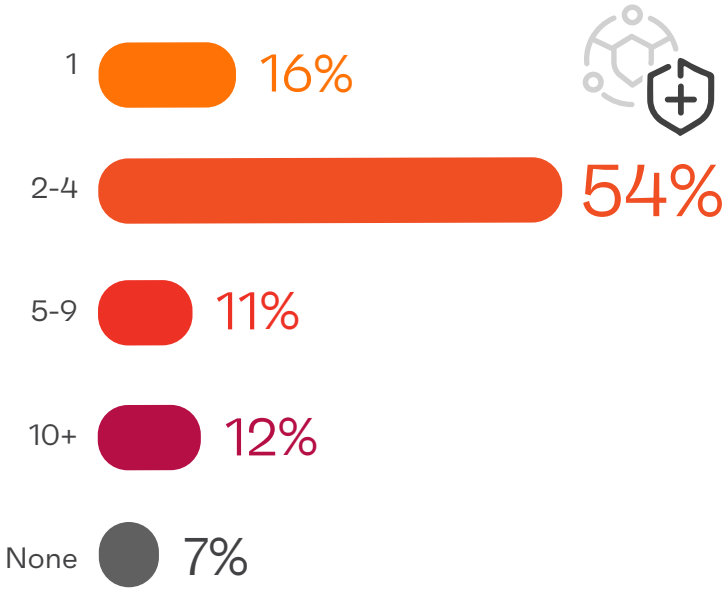
About what percentage of your organization's security incidents in the last 12 months do you believe were caused by end users possessing access privileges beyond what they require for their daily work? [n = 431]



Layered Approach to Zero Trust

The majority of respondents (54%) use 2-4 products for Zero Trust/secure access, suggesting that most organizations take a layered approach to Zero Trust implementation, utilizing multiple products to address various aspects of the framework, such as access management, device verification, and network segmentation. In the context of Zero Trust, these findings suggest that organizations adopt different approaches and levels of complexity when implementing a secure access program.

How many products would you use (or currently use) for a Zero Trust secure access program at your organization? [n = 429]



©2023 Cybersecurity Insiders All Rights Reserved.

Zero Trust Best Practices

Zero Trust is a security model that assumes no inherent trust within an organization's network and enforces strict verification of every user, device, and request. To effectively implement Zero Trust, organizations should consider these essential best practices:



Implement Multi-Factor Authentication (MFA):
Strengthen authentication by using multiple methods, such as biometrics or tokens, in addition to traditional usernames and passwords.



Adopt the Principle of Least Privilege (POLP):
Grant users only the minimum necessary access rights to perform their job functions, minimizing insider threats and data breaches.



Continuously Verify and Monitor Devices:
Ensure that only trusted devices access sensitive resources by enforcing strict device verification and continuous monitoring.



Secure Access to Cloud Applications:
Adopt Zero Trust principles when granting access to cloud resources and employ security measures like encryption, access controls, and logging.



Regularly Review and Update Access Controls:
Continuously evaluate and adjust access controls to keep them relevant and secure, aligned with your organization's changing roles and responsibilities.



Implement Anomaly Detection and Response:
Incorporate advanced detection and response technologies, such as Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR), to identify and mitigate threats quickly.



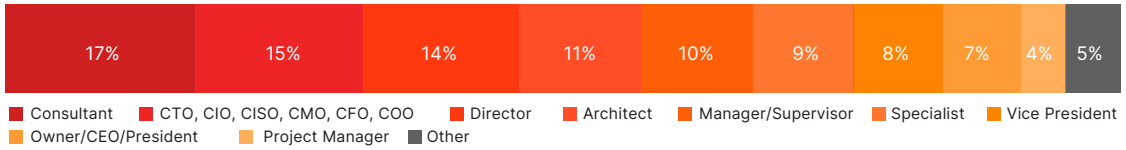
Provide Security Awareness Training:
Educate employees about Zero Trust principles, safe online practices, and how to recognize and report potential security threats to reduce the likelihood of security incidents resulting from human error.

©2023 Cybersecurity Insiders All Rights Reserved.

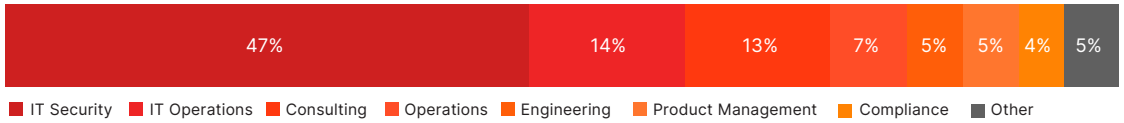
Methodology and Demographics

This report is based on the results of a comprehensive online survey of 431 IT and cybersecurity professionals in the US, conducted in March 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.

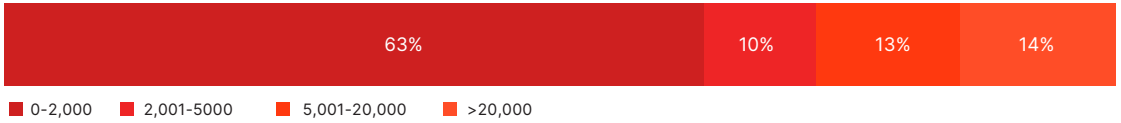
Career Level



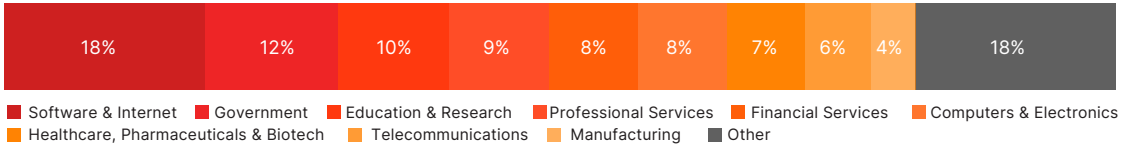
Department



Company Size



Industry



ivanti.com
1 800 982 2130
sales@ivanti.com

ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT applications and data over various networks to stay productive as they work from anywhere.

The Ivanti Neurons automation platform connects the company's industry-leading unified endpoint management, Zero Trust security, and enterprise service management solutions, providing a unified IT platform that enables devices to self-heal and self-secure and empowers users to self-service.

Over 40,000 customers, including 78 of the Fortune 100, have chosen Ivanti to discover, manage, secure, and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work.

For more information, visit www.ivanti.com and follow @GoIvanti.

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti") and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document, nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.ivanti.com.

1 Manual processes are complex and slow down ability to react quickly 37% | Partners insecurely accessing apps and resources 33% | Vulnerable, jailbroken, or lost mobile devices accessing resources 17%

2 Micro-segmentation 34% | Virtual Private Networks (VPN) 33% | Enterprise Mobile Management (EMM) 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 defense 16% | Enterprise directory services 13% | Digital Rights Management (DRM) 9% | Other 5%

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

©2023 Cybersecurity Insiders. All Rights Reserved. Data can be reproduced or referenced as long as it is sourced and linked to www.cybersecurity-insiders.com.