ivanti

Cybersecurity
INSIDERS

2021 Zero Trust Progress Report

ivanti.com

Overview

Enterprise adoption of the zero trust security model is gaining momentum as a majority of organizations plan to implement zero trust capabilities to mitigate growing cyber risk, especially in the wake of the massive shift to remote work. With its principle of user and device verification before granting conditional access based on least privilege, zero trust holds the promise of significantly enhanced usability, data protection, and governance.

The 2021 zero trust 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.

Key findings include:

- Trust earned through verification of entities including users, devices and infrastructure components (64%) tops the list of core components of zero trust. This is followed by data protection (63%) and continuous authentication/authorization (61%);
- Determining current access privileges for all users can be a daunting task to make sure users are limited to the appropriate access levels. More than 3/4 of organizations (88%) acknowledge that users may have access privileges beyond what they require;
- When asked about their current security priorities, cybersecurity professionals mentioned improved IAM (68%) most frequently, followed by data loss prevention (56%), and secure application access (46%).

Many thanks to Ivanti 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

Zero Trust Tenets

We asked organizations what aspects of zero trust they find most compelling. Trust earned through verification of entities including users, devices, and infrastructure components (64%) tops the list of core components of zero trust. This is followed by data protection (63%) and continuous authentication/authorization (61%).

What zero trust tenets are most compelling to you and your organization?[1]

64%

Trust earned through entity verification (e.g., user, device, infrastructure)

63%

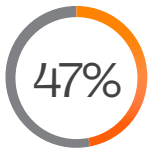
Data protection (e.g., secure connection)

61%

Continuous authentication/ authorization

End-to-end access visibility and audit

Facilitate least privilege access



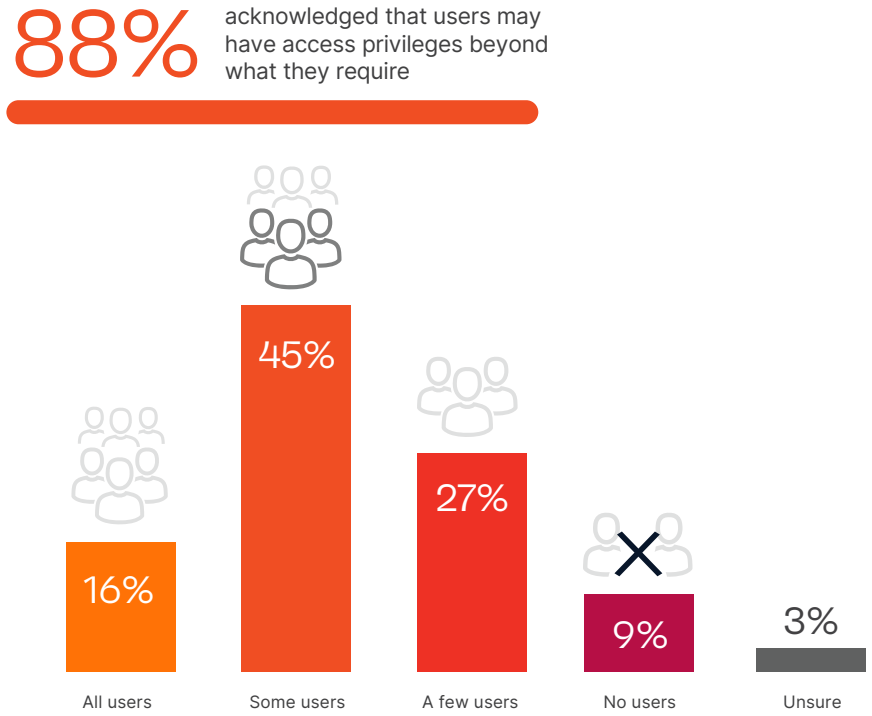
Centralized, granular access policy

No trust distinction between internal or external network

Excess Access Privileges

Determining current access privileges for all users can be a daunting task to make sure users are limited to the appropriate access levels. More than 3/4 of organizations (88%) acknowledge that users may have access privileges beyond what they require.

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



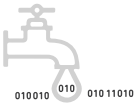
Security Priorities

When asked about their current security priorities, cybersecurity professionals mentioned improved IAM (68%) most frequently, followed by data loss prevention (56%), and secure application access (46%).

What are your organization's current security priorities?[2]

68%

Improve Identity and Access Management (IAM)

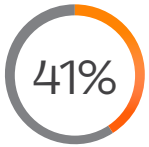


56%

Data Loss Prevention (DLP)

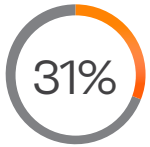
46%

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



Enable Endpoint Mobile Management (EMM)/BYOD
(e.g., users, devices)

Conduct deep SSL inspection
(e.g., secure session decryption for malware scanning and web/email filtering)



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

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

Identity Access and Zero Trust Priorities

We asked organizations what identity access and zero trust security controls they are investing in. The priority, from an investment perspective, is on multi-factor authentication (58%), followed by identity management and governance (48%), and single-sign on (45%).

Which of the following identity access/zero trust controls do you prioritize for investment in your organization within the next 12 months?[3]

58%

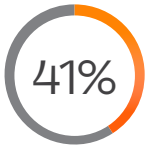
Multi-Factor Authentication (MFA)

48%

Identity management and governance

45%

Single Sign-On (SSO)



Privileged Access Management (PAM), micro-segmentation

Virtual Private Networks (VPN)

Micro-segmentation

Network Access Control (NAC), Web Application Firewall (WAF)

Secure Access Priorities

When we drill down into specific secure access priorities, organizations again prioritize multi-factor authentication/privileged account management (69%). This is followed by anomalous activity detection and response (58%), and securing access from personal, unmanaged devices (55%).

What are your organization's secure access priorities for the next one to two years?

69%

Multi-factor authentication/ privileged account management

58%

Anomalous activity detection and response

55%

Securing access from personal, unmanaged devices

Re-evaluate legacy security infrastructure and consider software-defined access

Stronger visibility and security metrics for executives

Micro-segmentation

Secure Access Challenges

The top concern regarding securing access to apps and resources is over-privileged access (60%), followed by providing secure access to partners (50%) - both challenges are directly addressed by zero trust.

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

60%

Overprivileged employee access

50%

Partners insecurely accessing apps and resources

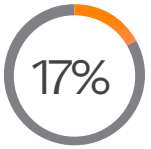
47%

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

Vulnerable, jailbroken or lost mobile devices accessing resources

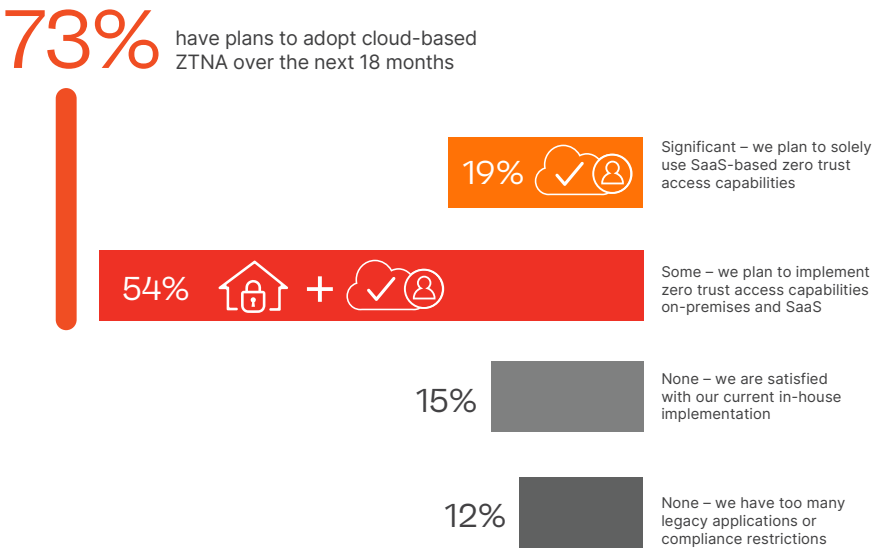


At-risk devices accessing network resources
(unknown, unsanctioned, non-compliance endpoints)

Zero Trust SAAS

Security is moving to the cloud, and ZTNA is no exception. Almost three-quarters of respondents are planning to adopt a cloud-based ZTNA solution over the next 18 months.

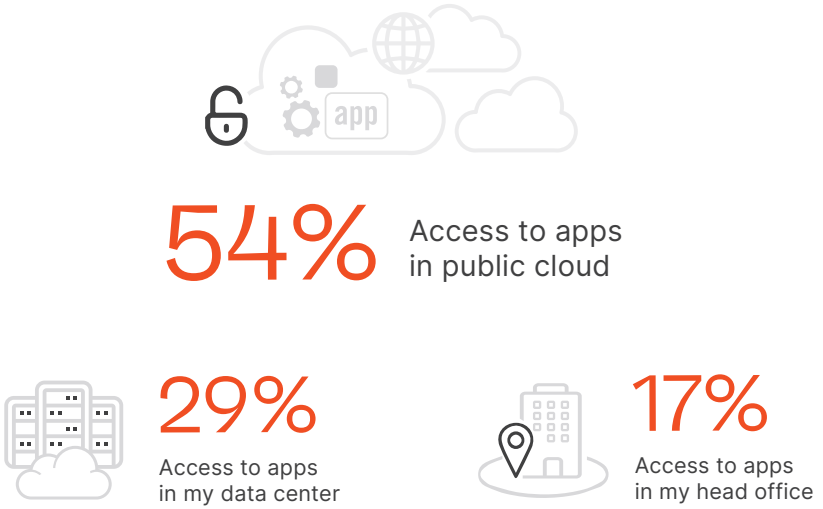
Over the next 18 months, to what extent do you and your organization plan to move zero trust access capabilities to SaaS?



Access to Private Apps

We asked organizations about their biggest challenges when it comes to securing private apps. For more than half of respondents, securely accessing applications deployed in public cloud environments is the single biggest headache today (54%).

When it comes to securing access to private apps, please rank the below in terms of your biggest challenge today?

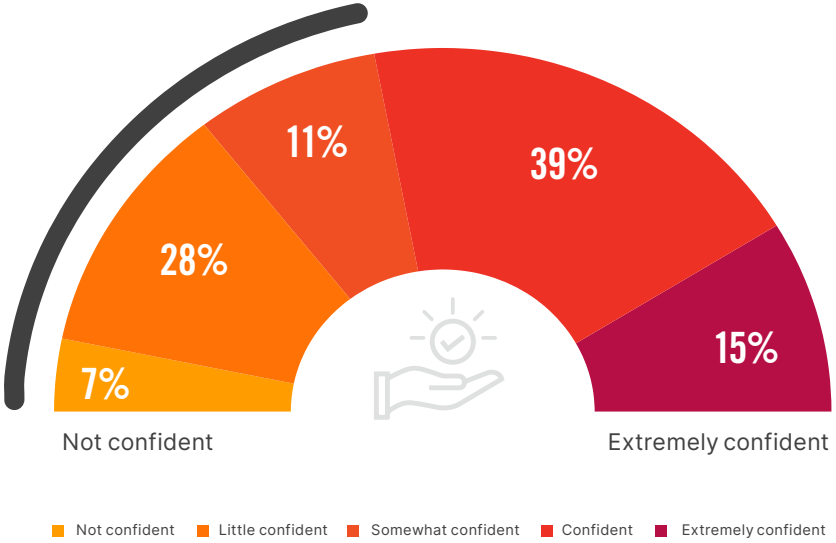


Zero Trust Confidence

When asked about their confidence in the ability to apply zero trust, almost half of enterprise IT security teams lack confidence (46%).

How confident are you to apply a full zero trust model/tenets in your secure access architecture?

46% of enterprise IT security teams lack confidence in their ability to provide zero trust



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, the most mentioned workaround is "hairpinning" remote and mobile users through data centers to access public app clouds (47%). An alarming 37% 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?

47%

I am forced to 'hairpin' remote users through my data center(s) to access apps in public cloud

37%

I have to publicly expose my private apps in public cloud in order to provide access

35%

I am unable to deploy my preferred remote VPN appliance in public cloud environments

Drivers for Zero Trust

What motivates organizations to initiate or build out a zero trust posture? Data security tops the list with 82%, followed by breach prevention (68%), and reduction of threats to endpoints (53%).

What are key drivers for your organization's initiating/ augmenting an identity access/zero trust posture?[4]

82%

Security/ data protection

68%

Breach prevention

53%

Reduce endpoint and IoT security threats

Reduce insider threats

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

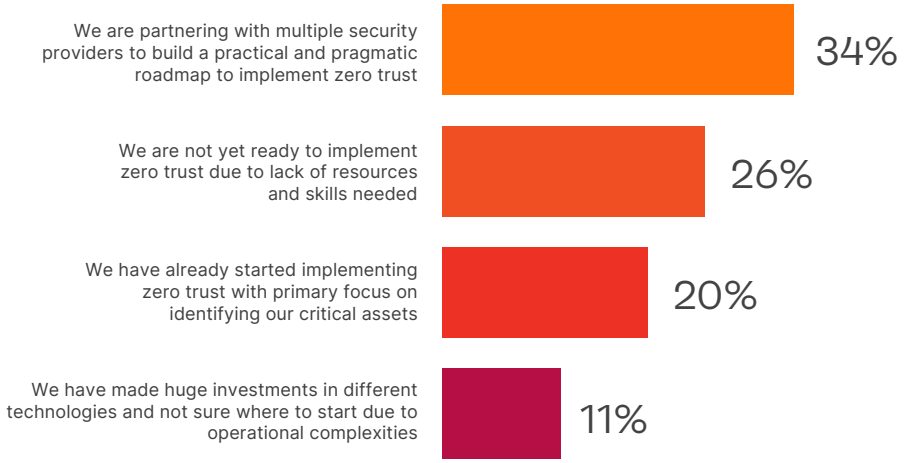
Address hybrid IT security issues

Operational efficiency

Zero Trust Implementation

Zero trust is quickly gaining momentum and organizations are taking different paths in implementing the technology. The most common approach organizations take is to partner with multiple security providers to build a practical and pragmatic roadmap to implement zero trust (34%). However, lack of resources and required skills (26%) remains a significant roadblock to zero trust.

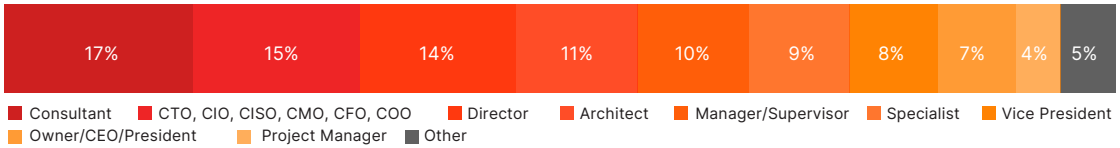
If zero trust implementation is a gradual process, how are you planning to implement zero trust across your extended environment?[5]



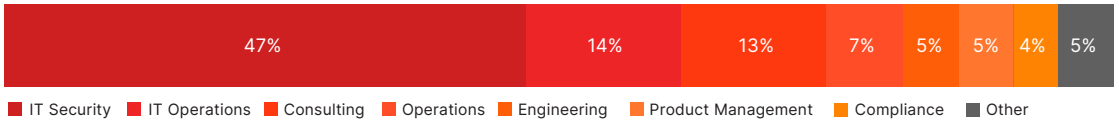
Methodology and Demographics

This report is based on the results of a comprehensive online survey of 443 IT and cybersecurity professionals in the US, conducted in July 2021, 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

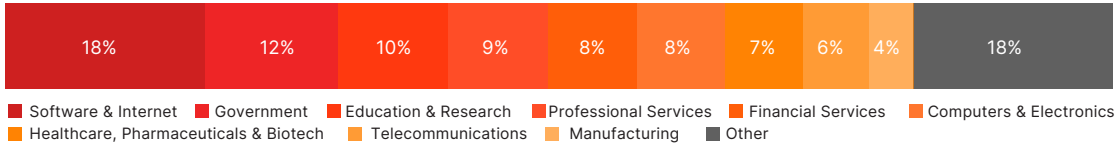


Department



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.

1 Resource segregation 40% | Other 2%

2 Supplement Endpoint Detection and Response (EDR) 28% | Enhance SD-WAN security functions 27% | Improve vulnerability remediation (e.g., vulnerability management, patch management) 5% | Provide better mobile threat protection (mobile threat defense/ anti-phishing) 2% | None 2% | Other 4%

3 Web Application Firewall (WAF) 35% | Enterprise Mobile Management (MDM) 31% | Cloud Access Security Broker (CASB) 30% | Identity analytics 27% | Software Defined Perimeter (SDP) 26% | Enterprise directory services 17% | Complete control over zero trust network access 12% | Vulnerability management/ patch management 9% | Network device invisibility to threats 7% | Anti-phishing 7% | Mobile threat defense 5% | Other 2%

4 Internal compliance 28% | Response to audit or security incident 28% | Other 5%

5 Other 9%