2020

Cybersecurity
INSIDERS

ZERO TRUST REPORT

netskope

INTRODUCTION

Enterprise adoption of the Zero Trust security model is gaining momentum as 72% of organizations plan to assess or implement Zero Trust capabilities in 2020 to mitigate growing cyber risk.

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 2020 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.

For almost half (45%) of respondents to the survey, ensuring remote access to private applications hosted in public cloud was a security priority. Zero Trust Network Access (ZTNA) was an area of focus for this report, the key findings supporting the view that ZTNA is a way to simplify, scale and secure remote access for a cloud-first organization.

Key findings include:

- Securely accessing applications deployed in public cloud environments is the single biggest headache for organizations today (65%).
- Traditional remote access solutions are failing the requirements of today's cloud environments. The most mentioned workaround is "hairpinning" remote users through data centers to access public app clouds (47%). An alarming 31% have to publicly expose cloud apps to enable remote workers, thereby introducing significant risk.
- Over 75% of respondents see value in consolidating ZTNA security services with other cloud-based security services such as CASB and SWG.

Many thanks to Netskope 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

ACCESS TO PRIVATE APPS

Securely accessing applications deployed in public cloud environments is organizations' single biggest headache today (65%).

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

65% Access to apps in public cloud

20% Access to apps in my head office

17% Access to apps in my data center

ACCESS TO APPS IN PUBLIC CLOUDS

Traditional remote access solutions are failing the requirements of today's cloud environments. The most mentioned workaround is "hairpinning" remote and mobile users through data centers to access public app clouds (47%). An alarming 31% 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

39%

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

31%

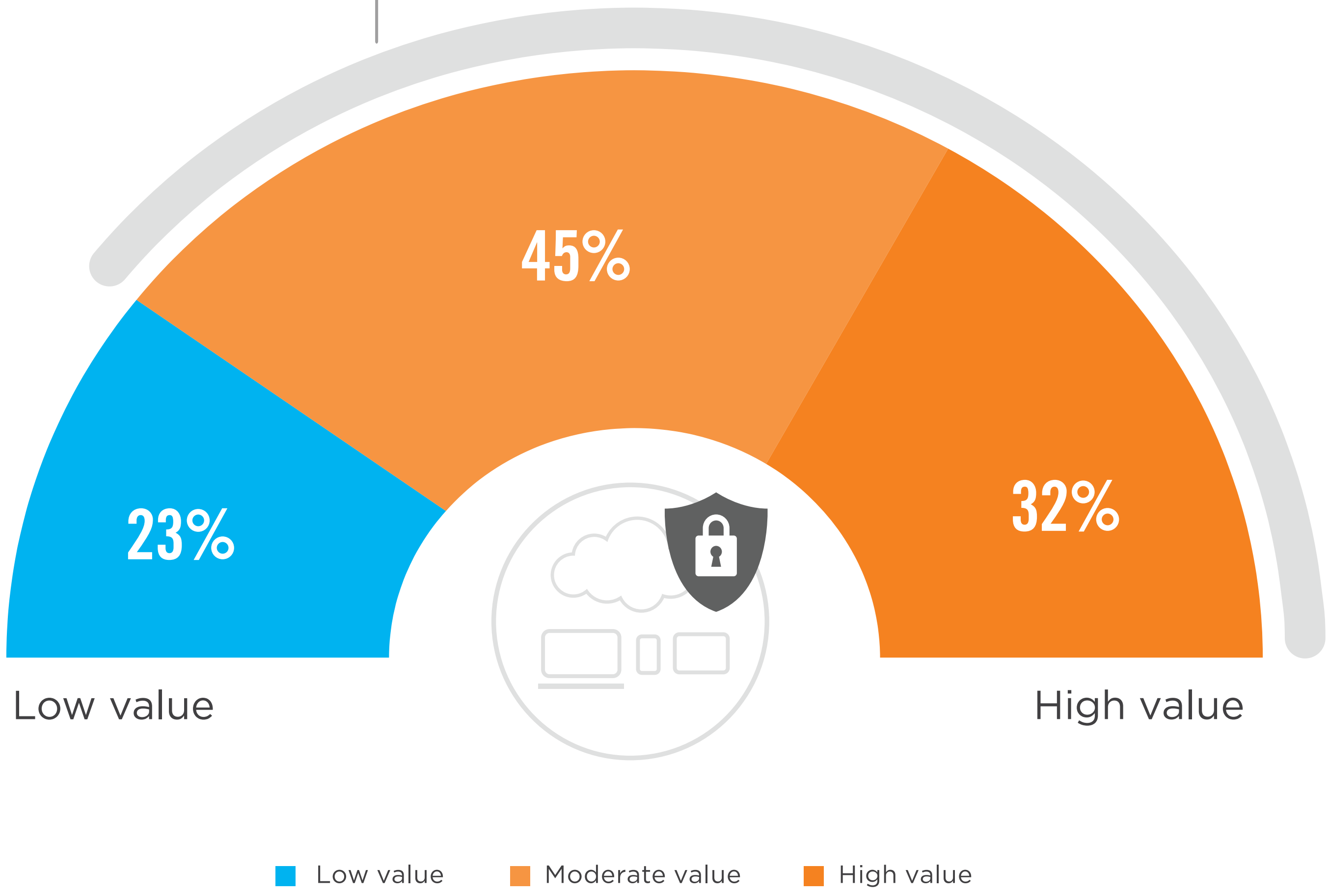
I have to publicly expose my private apps in public cloud in order to provide access

ZTNA CONSOLIDATION

Over 75% of respondents see value in consolidating ZTNA security services with other cloud-based security services such as CASB and SWG.

What value do you place on the consolidation of ZTNA with other cloud-based security capabilities (such as CASB and SWG) to create a solution aligned with the Secure Access Service Edge (SASE) recently defined by Gartner?

77% See value in consolidating ZTNA security services with other cloud-based security services



SECURE ACCESS CHALLENGES

Over-privileged access is the top concern regarding securing access to apps and resources for 62% of organizations, followed by providing secure access to partners (55%). Both challenges are directly addressed by ZTNA.

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

62%

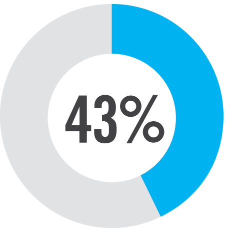
Overprivileged employee access

55%

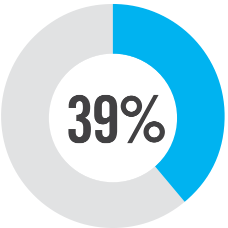
Partners insecurely accessing apps and resources

47%

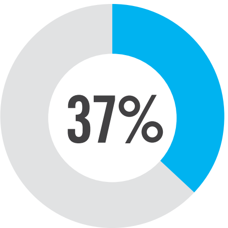
Cyber attacks
(e.g. denial of service, cross-site scripting, man-in-the-middle, phishing)



Shadow IT



Vulnerable, jailbroken or lost mobile devices accessing resources



Manual processes are complex and slow down ability to react quickly

At risk devices accessing network resources (unknown, unsanctioned, non-compliance endpoints) 10% | Other 2%

SECURITY PRIORITIES

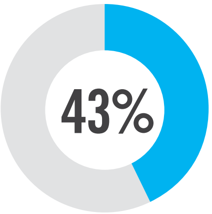
When asked about their current security priorities, improved IAM (71%) leads the list, followed by data loss prevention (55%), and secure application access (45%).

▶ What are your organization's current security priorities?

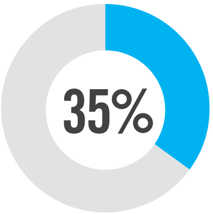
71%
Improve Identity and Access Management (IAM)

59%
Data Loss Prevention (DLP)

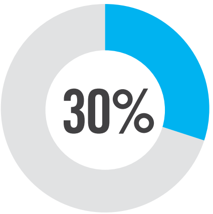
45%
Ensure secure access to applications hosted on Cloud Service Providers
(e.g. Microsoft, Amazon, Google)



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)



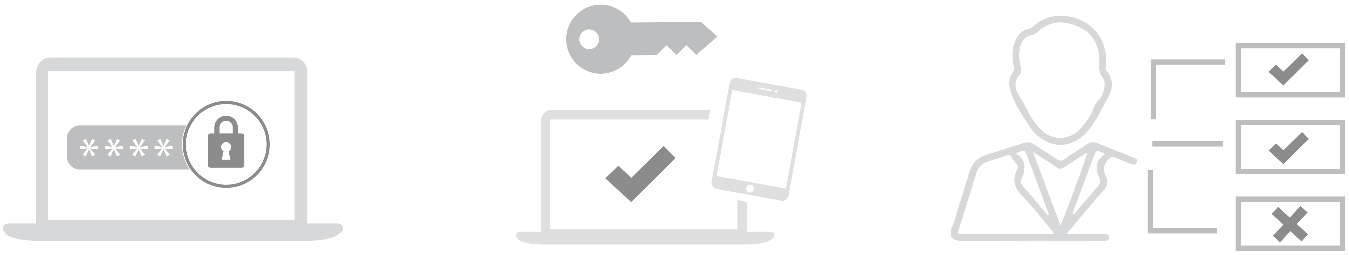
Simplify secure access delivery
(e.g. user experience, administration)

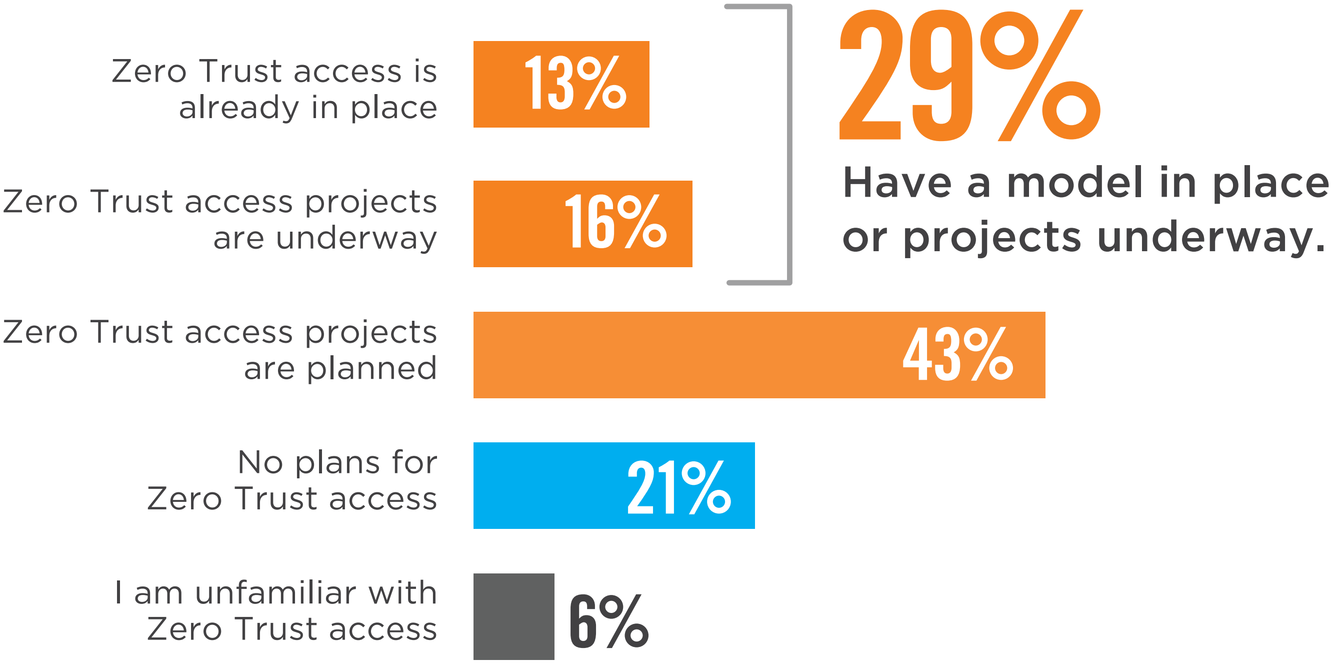
Enhance SD-WAN security functions 28% | Supplement Endpoint Detection and Response (EDR) 27% | Augment or replace existing remote access tools (e.g. VDI, VPN, RDP) 24% | Other 5% | None 2%

ADOPTION OF ZERO TRUST

The concept of Zero Trust is quickly gaining momentum. It has been established as a desirable end state with 29% of organizations already using or currently implementing zero trust, and 43% currently in the planning stage.

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

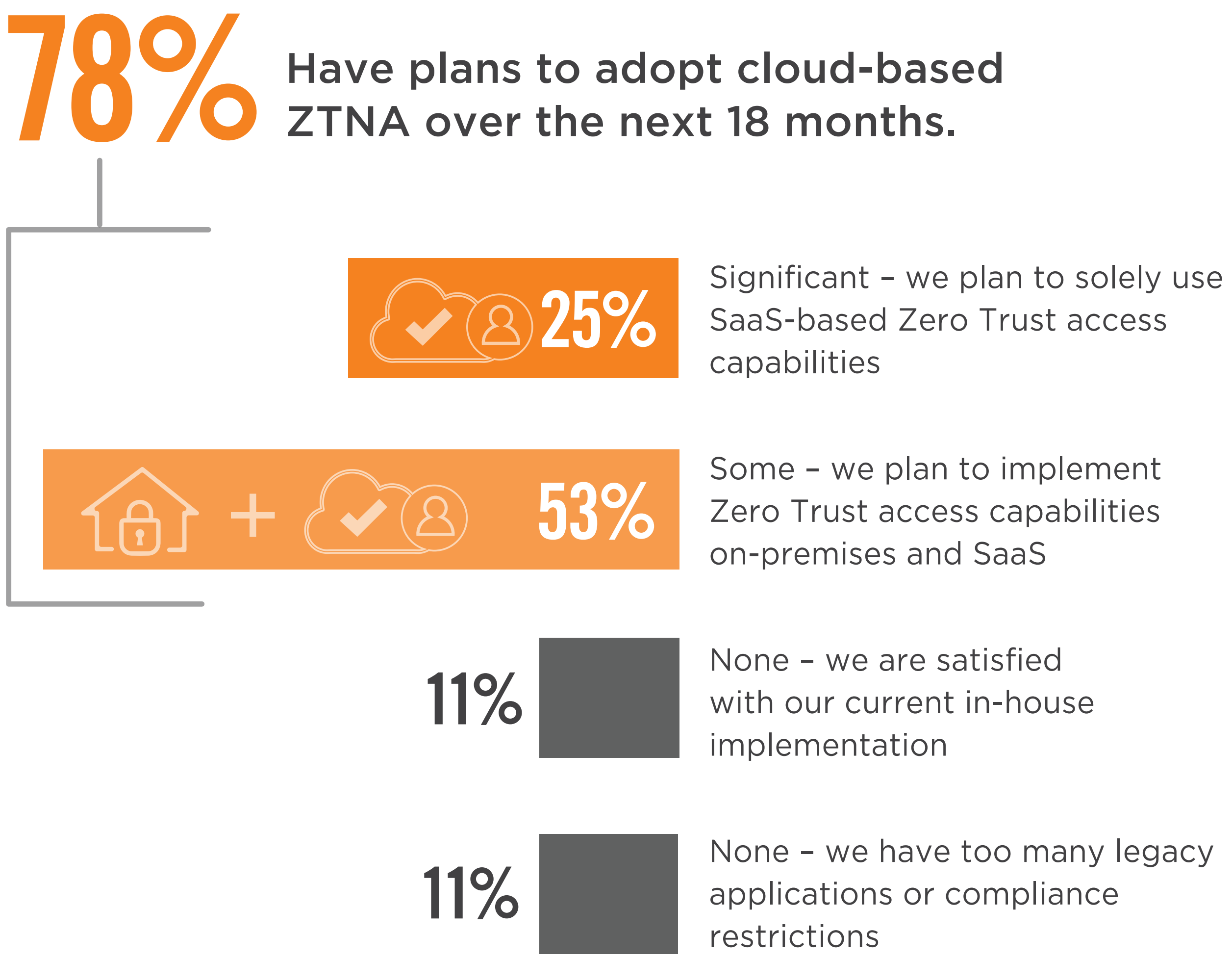




ZERO TRUST SAAS

Security is moving to the cloud, and ZTNA is no exception. More than 3/4 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?



78% Have plans to adopt cloud-based ZTNA over the next 18 months.

25% Significant – we plan to solely use SaaS-based Zero Trust access capabilities

53% Some – we plan to implement Zero Trust access capabilities on-premises and SaaS

11% None – we are satisfied with our current in-house implementation

11% None – we have too many legacy applications or compliance restrictions

IDENTITY ACCESS AND ZERO TRUST PRIORITIES

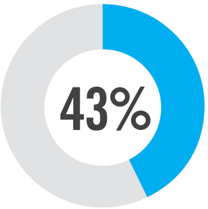
Organizations prioritize multi-factor authentication (59%), identity management and governance (48%), and single-sign on (44%) as the top three priorities for investment in zero trust controls over the next 12 months.

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

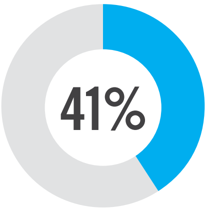
59%
Multi-Factor Authentication (MFA)

48%
Identity management and governance

44%
Single Sign-On (SSO)



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



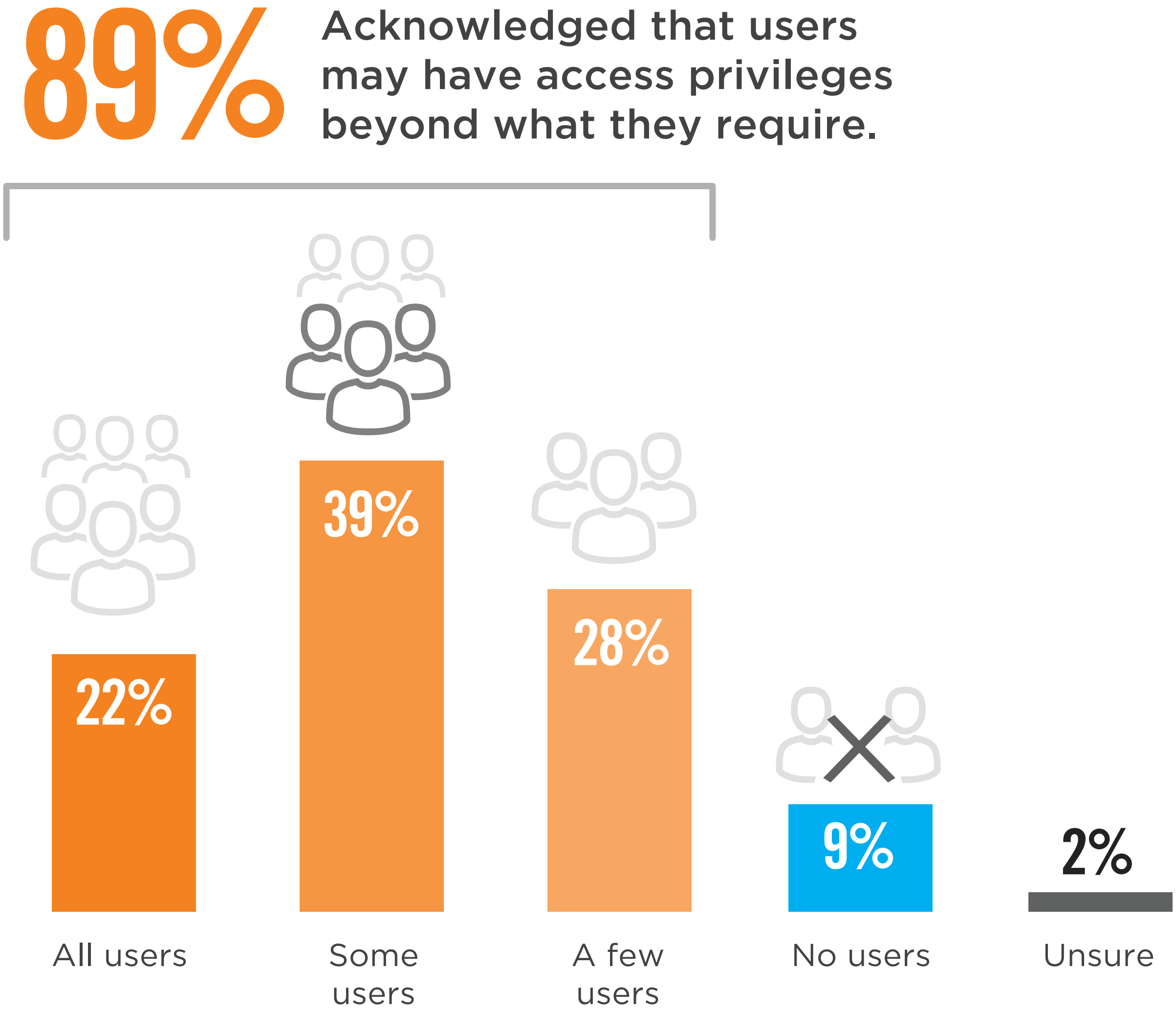
Privileged Access Management (PAM), Micro-segmentation

Virtual Private Networks (VPN) 35% | Cloud Access Security Broker (CASB) 33% | Enterprise Mobile Management (MDM) 31% | Software Defined Perimeter (SDP) 28% | Identity analytics 24% | Enterprise directory services 17% | Other 2%

EXCESS ACCESS PRIVILEGES

Almost 90% of organizations acknowledge that users have access privileges beyond what they require.

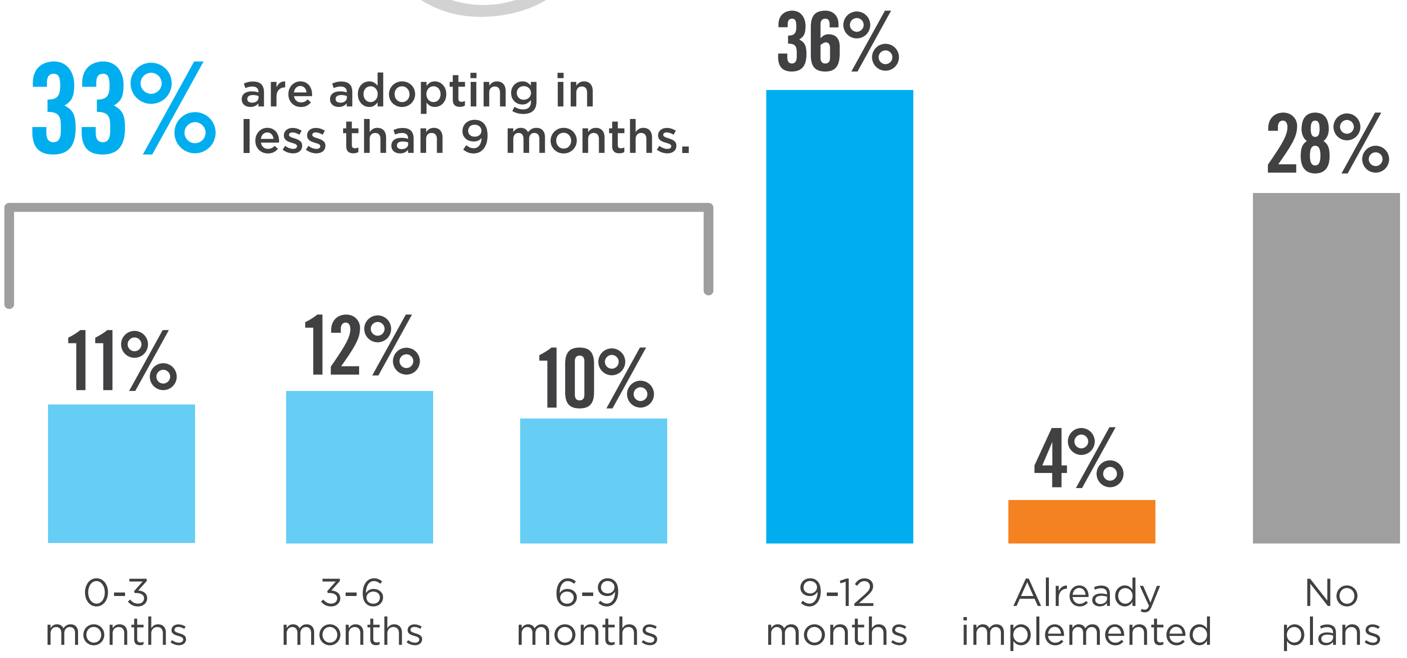
To what extent do you believe users in your organization have access privileges beyond what they require?



SPEED OF ADOPTION

Zero Trust interest is moving from planning to initial deployments. In fact, 33% of enterprises will adopt Zero Trust within 9 months.

▶ **In what timeframe will you most likely adopt zero trust security?**



ZERO TRUST TENETS

What tenets of the Zero Trust paradigm are most compelling to organizations? Continuous authentication/authorization tops the list as a core component of the Zero Trust value proposition (67%) together with data protection (e.g. secure connection) (67%). This is followed by trust earned through verification of entities including users, devices and infrastructure components (63%).

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

67%

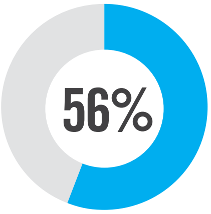
Continuous authentication, authorization

67%

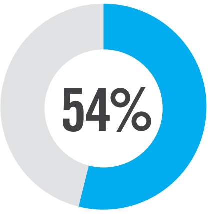
Data protection
(e.g. secure connection)

63%

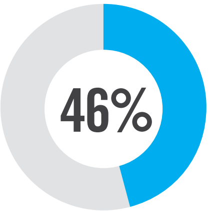
Trust earned through entity verification
(e.g. user, device, infrastructure)



End-to-end access visibility and audit



Facilitate least privilege access



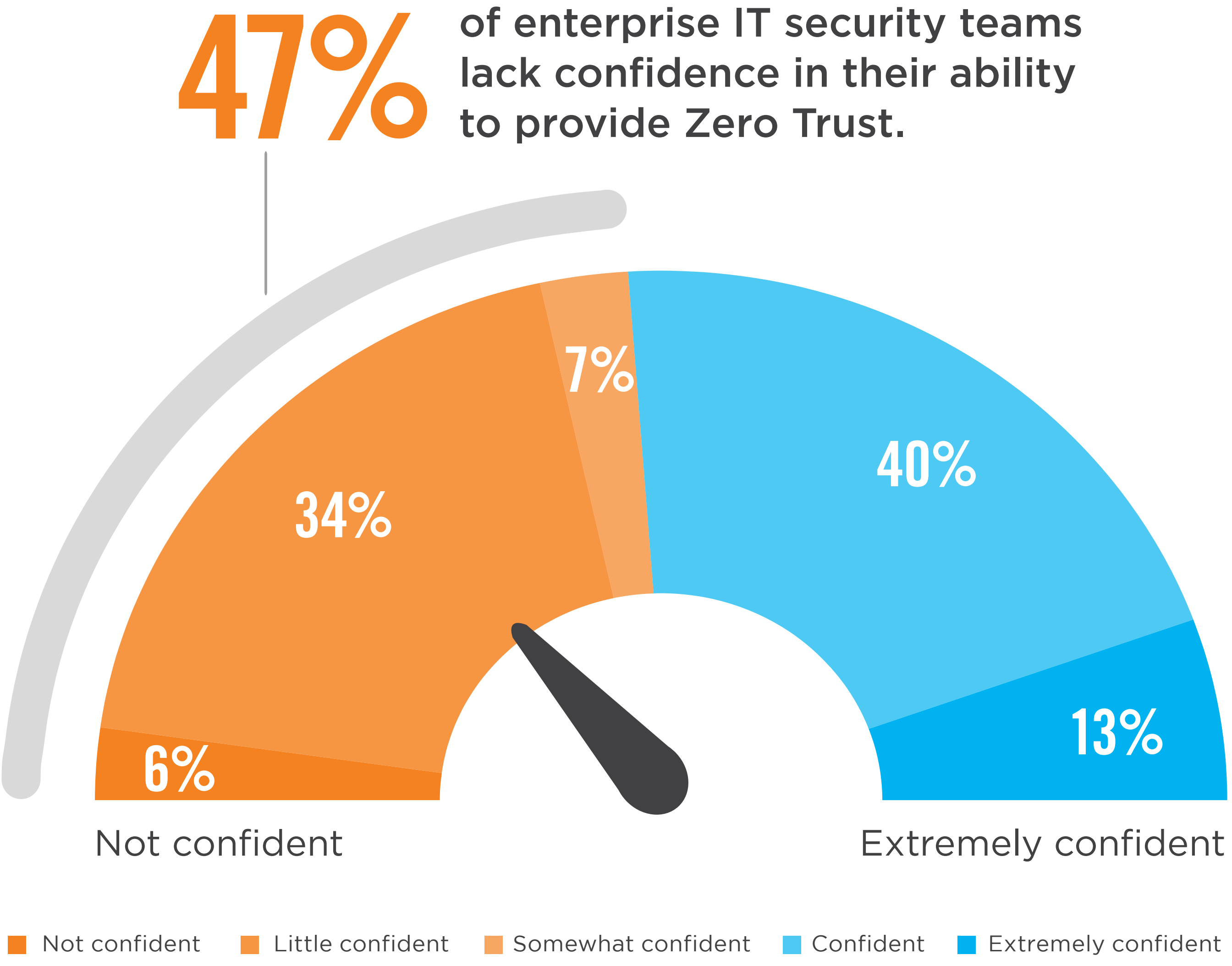
Centralized, granular access policy

Resource segregation 44% | No trust distinction between internal or external network 39% | Other 2%

ZERO TRUST CONFIDENCE

While 53% of organizations are confident or extremely confident in their ability to implement Zero Trust in their secure access architecture, 47% of enterprise IT security teams lack confidence in their ability to provide Zero Trust.

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



DRIVERS FOR ZERO TRUST

What motivates organizations to initiate or build out a Zero Trust program? Data security tops the list with 85%, followed by breach prevention (70%) and reduction of threats to endpoints (56%).

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

85%

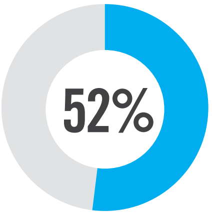
Security/
data protection

70%

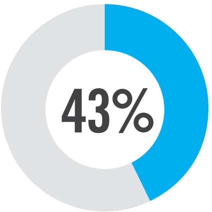
Breach
prevention

56%

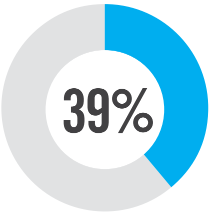
Reduce endpoint
and IoT security
threats



Reduce insider
threats



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



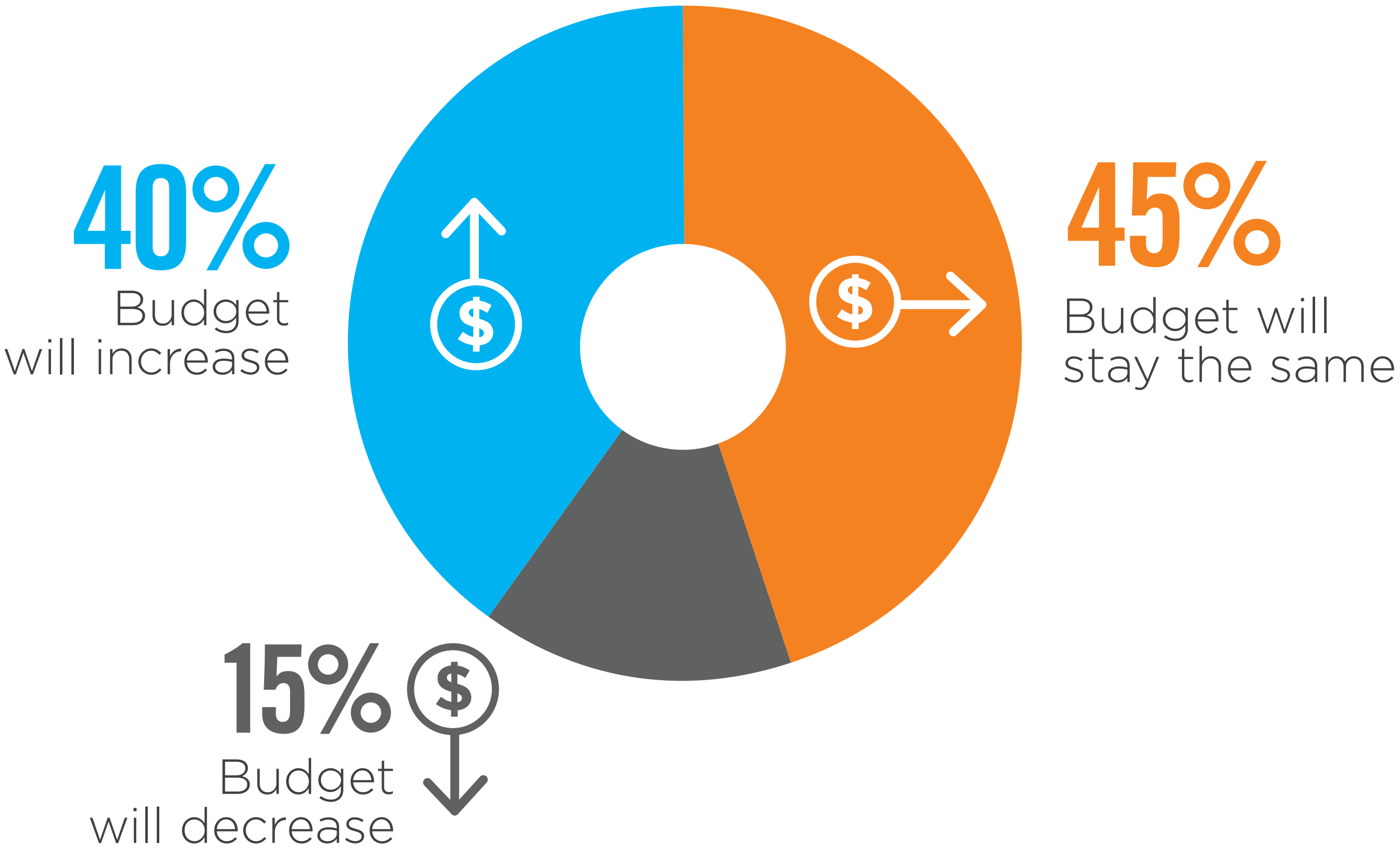
Internal
compliance

Response to audit or security incident 37% | Operational efficiency 33% | Address hybrid IT security issues 31% | Other 4%

ZERO TRUST BUDGET

Forty percent of organizations expect an increase of their access management related budgets over the next 18 months. Only 15% will see a decline.

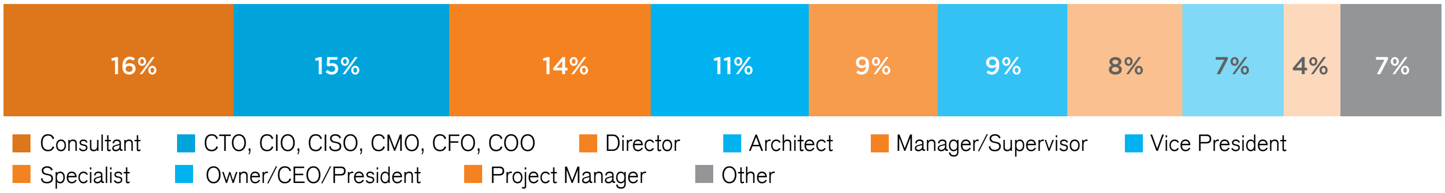
How do you expect your organization's access management related budget to change over the next 18 months?



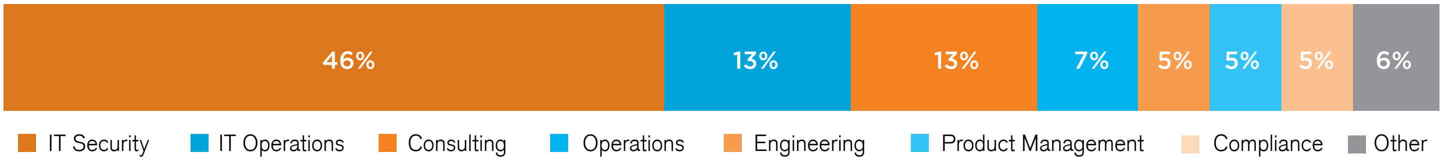
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of 413 IT and cybersecurity professionals in the US, conducted in February 2020 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.

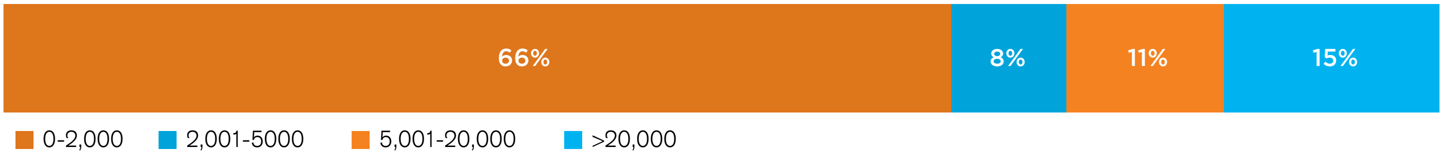
CAREER LEVEL



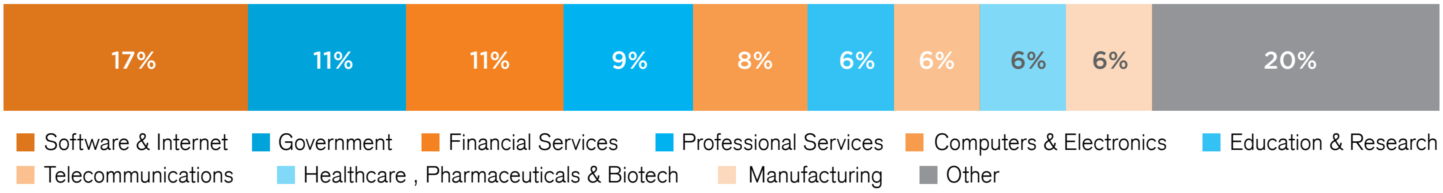
DEPARTMENT



COMPANY SIZE



INDUSTRY



netskope

The network perimeter is dissolving. A new perimeter is needed that can protect data and users everywhere, without introducing friction to the business. The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and delivers data-centric security from one of the world's largest and fastest security networks, empowering the largest organizations in the world with the right balance of protection and speed they need to enable business velocity and secure their digital transformation journey. Reimagine your perimeter with Netskope.

www.netskope.com