2020

ZERO TRUST PROGRESS REPORT

Cybersecurity INSIDERS

Research Sponsor

Pulse Secure®

OVERVIEW

Data breaches are on the rise, highlighting that no organization is immune from cyberattacks. One cause is that workforce mobility and cloud computing has placed most workloads beyond the shelter of corporate networks and traditional perimeter defense. Enterprise adoption of the Zero Trust security model is growing as part of key initiatives to mitigate cyber risk. With its principle of user, device and infrastructure verification before granting conditional access based least privilege, Zero Trust holds the promise of vastly enhanced usability, data protection and governance. This 2020 Zero Trust Progress report shows how enterprises are implementing Zero Trust security in their organization and reveals key drivers, adoption, technologies, investments and benefits.

The 2020 Zero Trust Progress report surveyed more than 400 cyber security decision makers, ranging from technical executives to IT security practitioners and representing a balanced cross-section of organizations of varying sizes across multiple industries. As 72% of organizations plan to assess or implement Zero Trust capabilities in some capacity in 2020 to mitigate growing cyber risk, nearly half (47%) of cyber security professionals lack confidence applying a Zero Trust model to their Secure Access architecture.

Key findings include:

- Nearly equal confidence and lack of confidence in applying Zero Trust model in their Secure Access architecture (53% have confidence, 47% are not confident);
- Fifty-three percent plan to move Zero Trust access capabilities to a hybrid IT implementation;
- Over 60% find the Zero Trust tenets of continuous authentication and authorization, trust earned through entity verification, and data protection as most compelling for their organization;
- Over 40% expressed privilege management, insecure partner access, cyberattacks, shadow IT risks, and vulnerable mobile and at-risk device resource access as top challenges to secure access to applications and resources;
- Forty-five percent are concerned with public cloud application access security, and 43% with BYOD exposures;
- Seventy percent of organizations plan to advance their identity and access management capabilities;
- Thirty percent of organizations are seeking to simplify secure access delivery including enhancing user experience and optimizing administration and provisioning;
- Forty-one percent are looking to re-evaluate their secure access infrastructure and consider Software Defined Perimeter (SDP) - with the majority requiring a hybrid IT deployment and a quarter adopting a SaaS implementation.

Many thanks to Pulse Secure 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

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 with 67 percent. This is followed by trust earned through verification of entities including users, devices (65%) and infrastructure components and data protection (e.g. secure connection) (63%)

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

67%

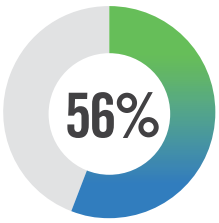
Continuous authentication, authorization

65%

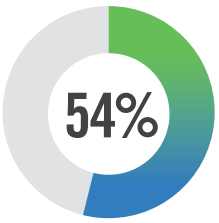
Trust earned through entity verification (e.g. user, device, infrastructure)

63%

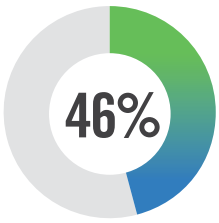
Data protection (e.g. secure connection)



End-to-end access visibility and audit



Facilitate least privilege access



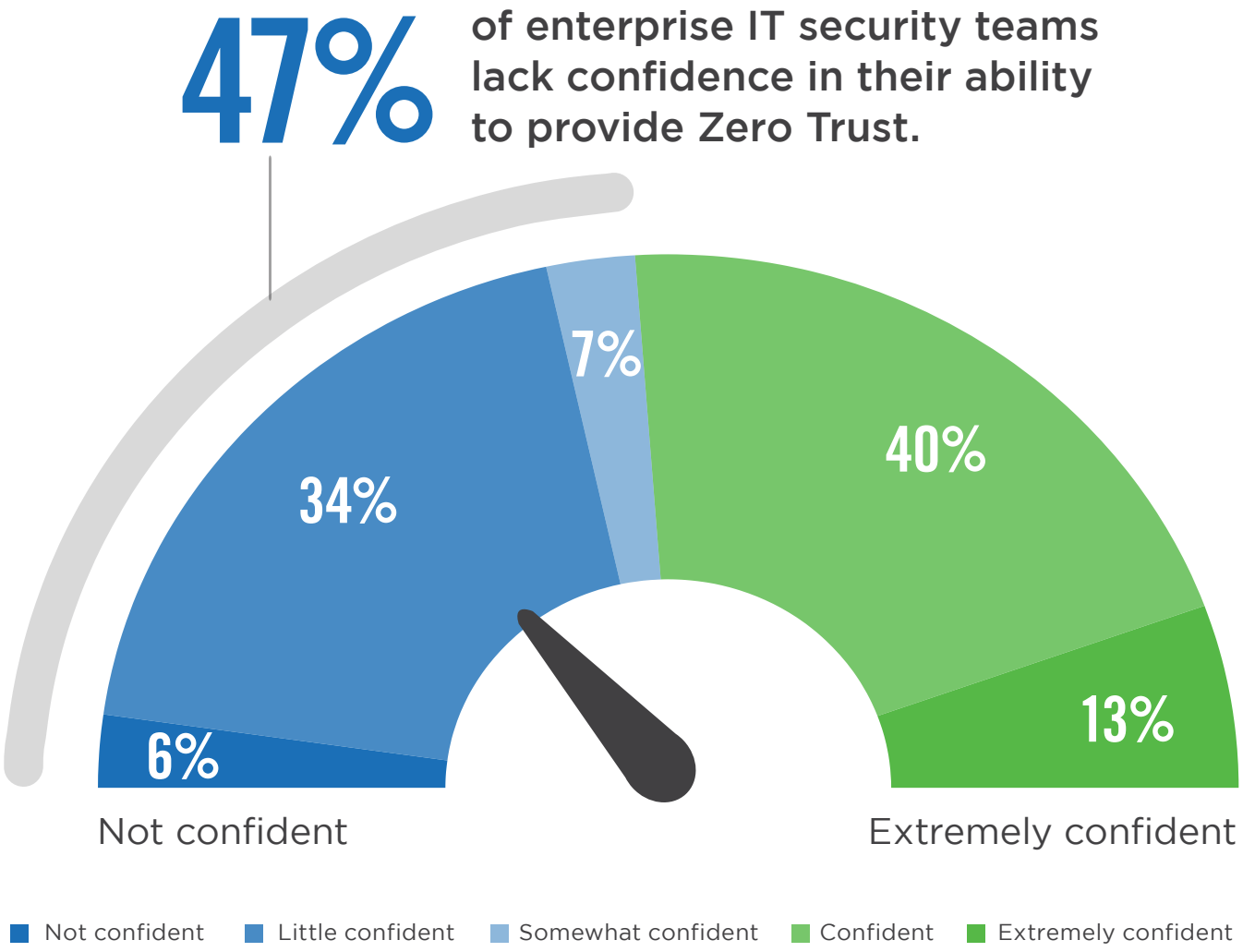
Centralized, granular access policy

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

ZERO TRUST CONFIDENCE

While 53 percent of organizations are confident in their ability to implement Zero Trust in their secure access architecture, over 40 percent 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 percent, followed by breach prevention (70%) and reduction of threats to endpoints (56%). Beyond industry, regulatory and internal compliance, nearly a third are seeking to address hybrid IT security issues.

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

85%

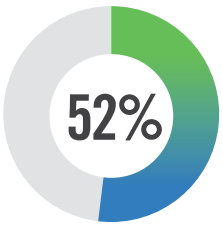
Security/ data protection

70%

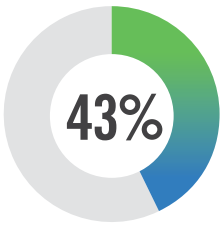
Breach prevention

56%

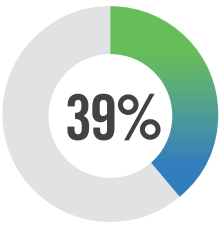
Reduce endpoint and IoT security threats



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%

SECURE ACCESS CHALLENGES

What are the key challenges organizations face when it comes to securing access? Overprivileged employees (62%), partner access to sensitive resources (55%, and vulnerable mobile and at-risk devices resource access (49%), challenges organizations experience.

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

62%

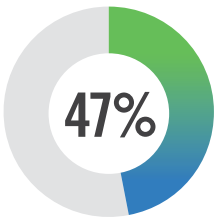
Over privileged employee access

55%

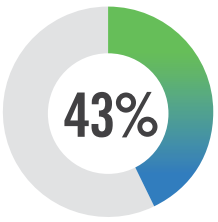
Partners insecurely accessing apps and resources

49%

Vulnerable mobile and at-risk device resource access
(unknown, unsanctioned, non-compliant, lost endpoints)



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 37% | Other 2%

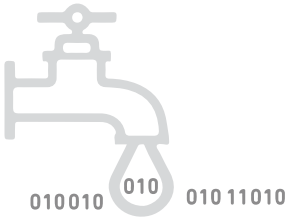
SECURITY PRIORITIES

Improving identity and access management is the top priority for 71% of organizations in our survey. This is followed by data loss prevention (59%) and secure access to cloud apps hosted on Cloud Service Providers (45%).

What are your organization's current security priorities?

71%

Improve Identity and Access Management (IAM)

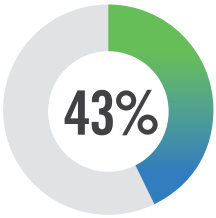


59%

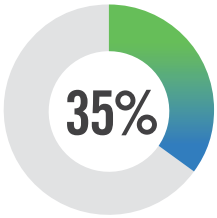
Data Loss Prevention (DLP)

45%

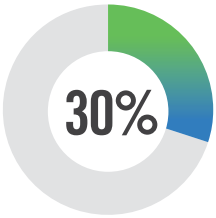
Ensure secure access to applications hosted on Cloud Service Providers
(e.g. Microsoft, Amazon, Google)



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)



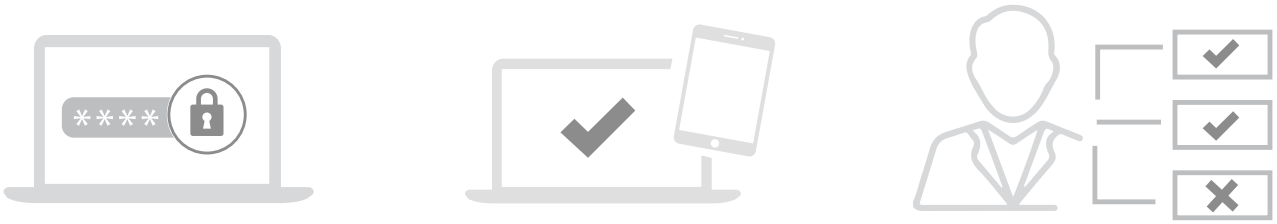
Simplify secure access delivery (e.g. user experience, administration)

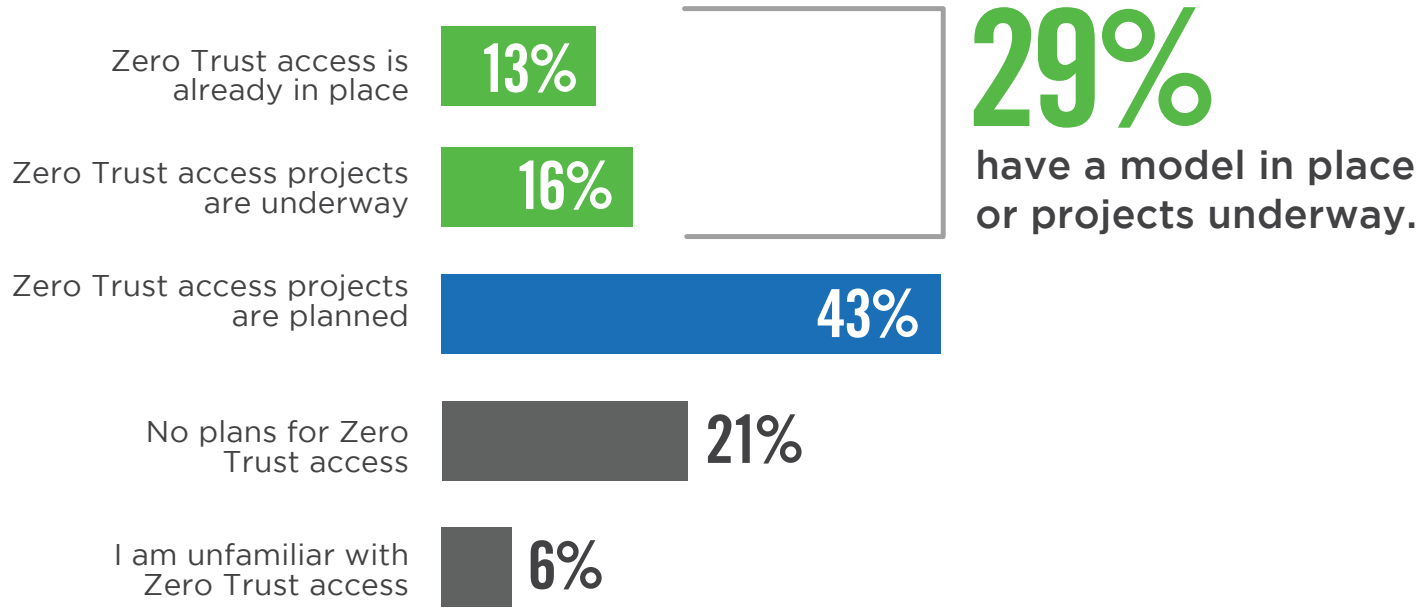
Enhance SD-WAN security functions 28% | Supplement Endpoint Detection and Response (EDR) 27% | Augment or replace existing remote access tools (e.g. VDI, VPN, RDP) 24% | Other 5% | None 2%

ADOPTION OF ZERO TRUST

When asked about their plans for adopting a Zero Trust access, nearly 29% have a model in place or projects underway, while 43% are in some sort of planning stage. Surprisingly, nearly a third have no plans or are not familiar with Zero Trust.

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

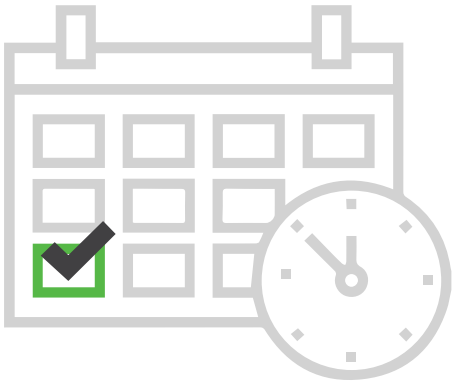




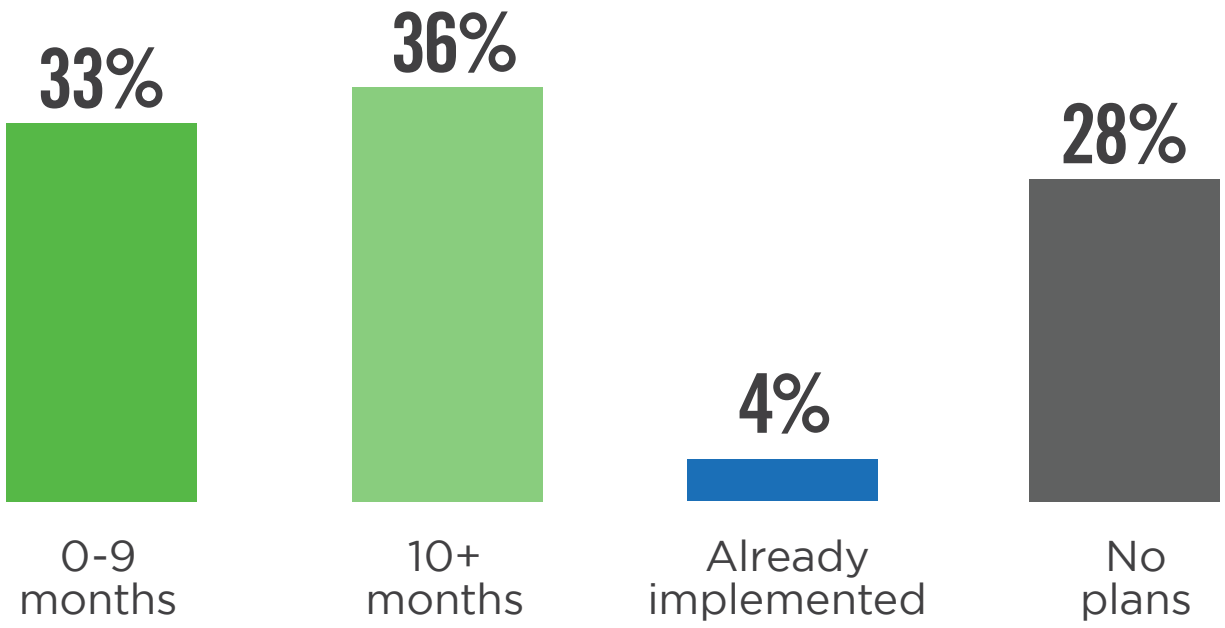
SPEED OF ADOPTION

Zero Trust interest is moving to initial deployments. In fact, 33% of enterprises will adopt Zero Trust within 9 months. Nearly a third have no plans suggesting some confusion on value or effort.

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



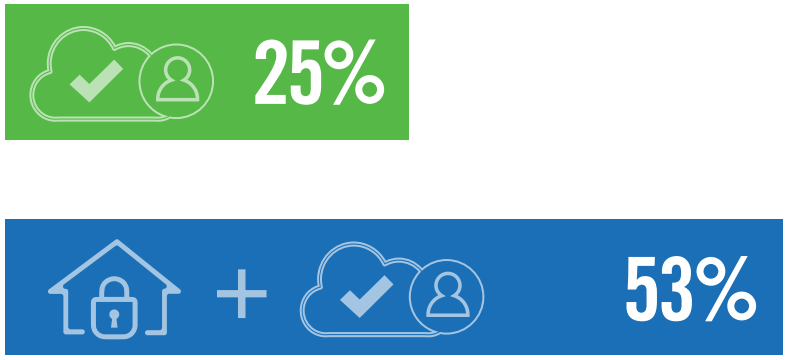
33%
of enterprises will adopt Zero Trust within 9 months.



ZERO TRUST SAAS

More than half of organizations plan to move Zero Trust access capabilities to a hybrid IT (on-premises/SaaS) implementation. A quarter plan to move solely to a SaaS-based Zero Trust solution. Twenty-two percent have no plan for SaaS-based Zero Trust deployment either due to legacy applications, compliance restrictions or satisfaction with current implemented access protection.

Over the next 18 months, to what extent do you and your organization plan to move Zero Trust Access capabilities to SaaS?



SSL Inspection 40% | Securing SD-WAN 27% | Simplification 26% | Replacing existing remote access security technology (i.e. VPN) 25% | EDR 20% | None 2% | Other 8%

ZERO TRUST ACCESS INVESTMENT PRIORITIES

The majority of investments in Zero Trust access technologies are directed toward multi-factor authentication (59%), identity management and governance (48%), and single sign-on (44%). This is followed by Network Access Control and Web Application Firewall (43%), Privileged Access Management and Micro-segmentation (41%), and Virtual Private Networks (35%).

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

59%

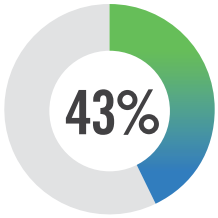
Multi-factor authentication (MFA)

48%

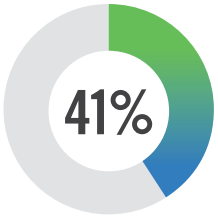
Identity management and governance

44%

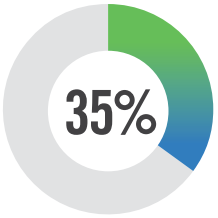
Single Sign-on (SSO)



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



Privileged Access Management (PAM), Micro-segmentation



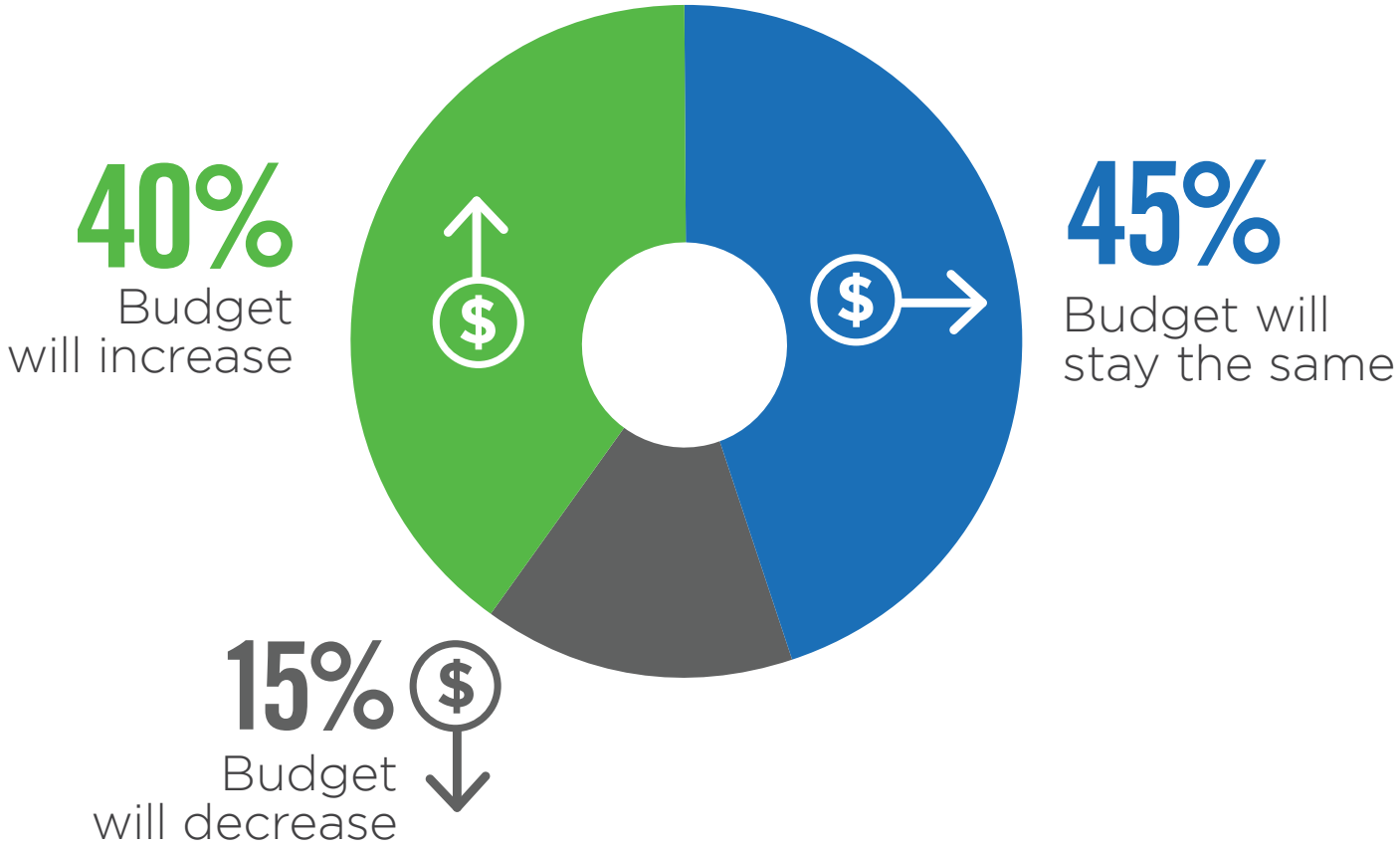
Virtual Private Networks (VPN)

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%

ZERO TRUST ACCESS 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.

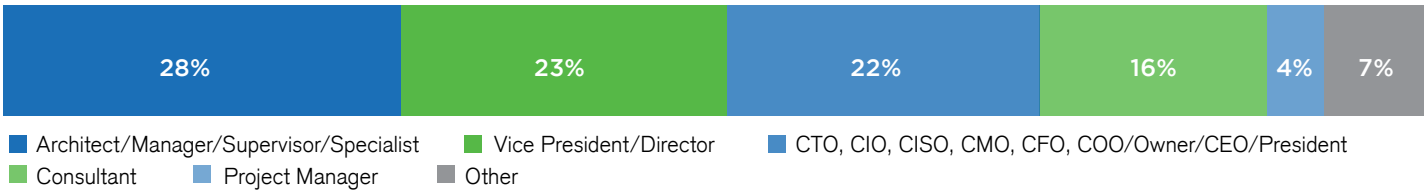
How do you expect your organization's access management related budget to change over the next 18 months?



METHODOLOGY & DEMOGRAPHICS

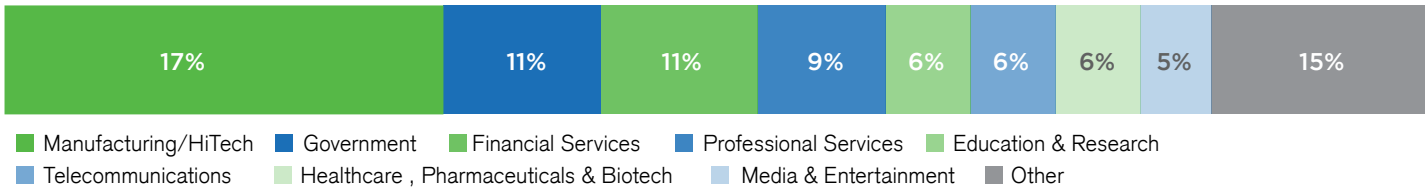
This report is based on the results of a comprehensive online survey of 413 IT and cybersecurity professionals in the US, conducted in January 2020 to identify the latest enterprise adoption trends, challenges, gaps and solution preferences related to Zero Trust security. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

CAREER LEVEL



COMPANY SIZE

INDUSTRY



Research Sponsor

Pulse Secure®

Pulse Secure provides easy, comprehensive software-driven Secure Access solutions for people, devices, things and services that improve visibility, protection and productivity for our customers. Our suites uniquely integrate cloud, mobile, application and network access to enable hybrid IT in a Zero Trust world. Over 23,000 enterprises and service providers across every vertical entrust Pulse Secure to empower their mobile workforce to securely access applications and information in the data center and cloud while ensuring business compliance. Learn more at www.pulsesecure.net