2019

Cybersecurity INSIDERS

ZERO TRUST ADOPTION REPORT

zscaler™

TABLE OF CONTENTS

INTRODUCTION

Zero Trust is rapidly gaining popularity as a new security model that provides least-privilege access to private apps based on contextual controls (user, device, apps, etc.). To enable this, many teams are adopting modern cloud-first technologies that can replace traditional infrastructure, like VPN and DMZs.

The 2019 Zero Trust Adoption Report reveals the value of zero trust to organizations by enabling businesses to remain secure as they move apps to public cloud and support an increasingly mobile workforce, providing a better user experience, greater visibility while minimizing risk.

Key Takeaways:

- Seventy-eight percent of IT security teams are looking to embrace zero trust network access in the future. 19% are actively implementing zero trust, and 15% already have zero trust in place. At the same time, about half of enterprise IT security teams (47%) lack confidence in their ability to provide zero trust with their current security technology.

- The highest security priority for application access is privileged account management of users and multi-factor authentication (68%). This is followed by detection of, and response to, anomalous activity (61%) and securing access from personal, unmanaged devices (57%).

- Sixty-two percent of organizations say their biggest application security challenge is securing access to private apps that are distributed across datacenter and cloud environments. This is followed by minimizing exposure of private apps to the internet (50%), tied with gaining visibility into user activity (50%).

- When asked about the benefits of zero trust, two-thirds of IT security professionals (66%) say they are most excited about zero trust's ability to deliver least privilege access to protect private apps. This is followed by apps no longer being exposed to unauthorized users or the Internet (55%), and access to private apps no longer requiring network access (44%).

Many thanks to Zscaler 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

SECURITY PRIORITIES

The highest security priority for application access is privileged account management of users and multi-factor authentication (68%). This is followed by detection of, and response to, anomalous activity (61%) and securing access from personal, unmanaged devices (57%).

When it comes to accessing private apps running in datacenter or public cloud environments, what are the security priorities for the next 1-2 years?

68%

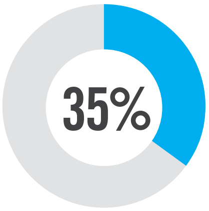
Multi-factor authentication/privileged account management

61%

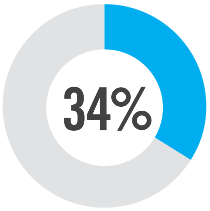
Anomalous activity detection and response

57%

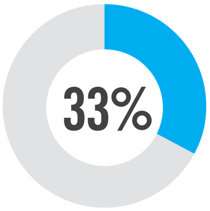
Securing access from personal, unmanaged devices



Stronger visibility and security metrics for executives



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



Microsegmentation

ACTIVE SECURITY INITIATIVES

The top four security initiatives currently underway in organizations are all related to zero trust network access: Identity and Access Management (72%), Data Loss Prevention (DLP) (51%), BYOD/mobile security (50%), and securing access to private apps running on public cloud (i.e. Microsoft Azure), Amazon Web Services, Google Cloud Platform (47%).

▶ **Which security initiatives do you currently have underway?**

72%

Identity and
Access Management

51%

Data Loss
Prevention (DLP)

50%

BYOD/mobile security

47%

Securing access to private
apps running on public cloud
(i.e. Microsoft Azure, Amazon Web Services,
Google Cloud Platform)

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%

SECURE ACCESS CHALLENGES

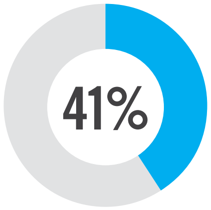
Sixty-two percent of organizations say their biggest application security challenge is securing access to private apps that are distributed across datacenter and cloud environments. This is followed by minimizing exposure of private apps to the internet (50%), tied with gaining visibility into user activity (50%).

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

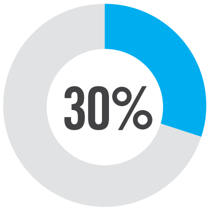
62%
Securing access to private apps that are now spread across datacenter and cloud

50%
Minimizing need to expose my internal app to the internet

50%
Gaining visibility into user activity



Finding budget to support a new security model



Bringing remote users and third parties onto my network

APPLICATION ACCESS CONCERNS

The highest areas of personal concern around private application access are internal users with overprivileged access (61%), tied with partners accessing internal apps utilizing weak security practices (61%). Leveraging network-centric makes segmentation and least-privileged access difficult to implement.

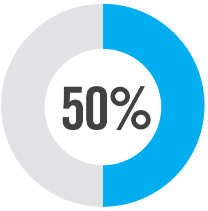
What are you personally most concerned with today when it comes to protecting access to private apps?

61%

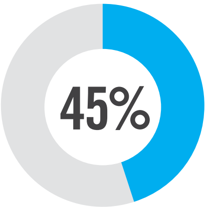
Internal users with overprivileged access

61%

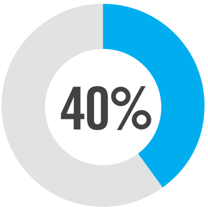
Partners with weak security practices accessing internal apps



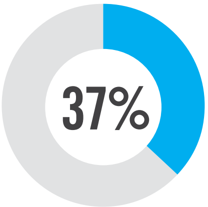
Internet based attacks (i.e. DDoS, Man in the Middle, Ransomware)



Stolen or infected mobile devices gaining access to the network



Shadow IT



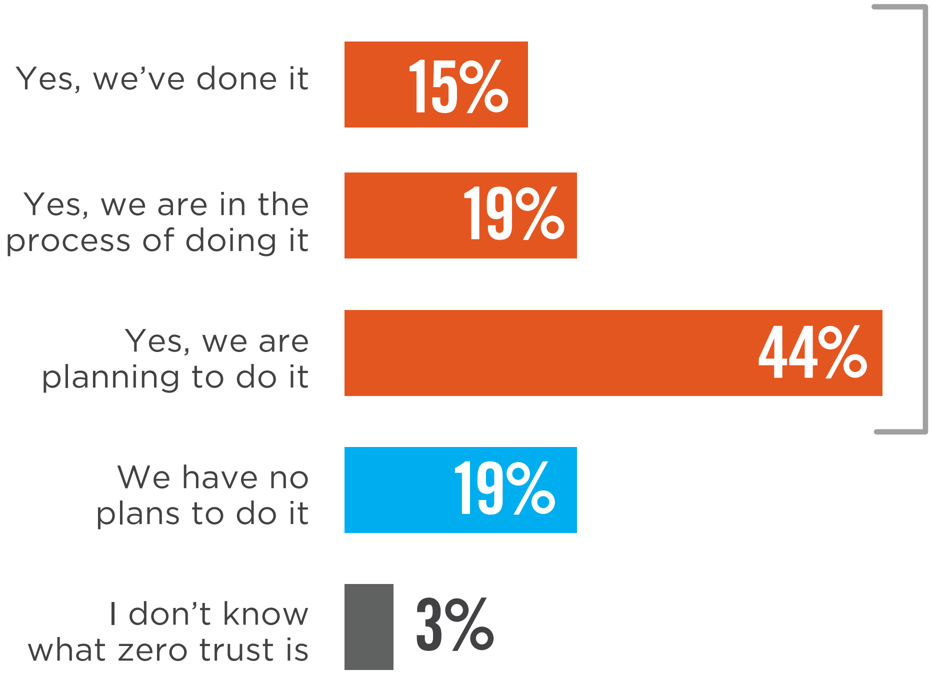
Manual processes are complex and slow downability to react quickly

Other 4%

ADOPTION OF ZERO TRUST

When asked about their plans for adopting zero trust strategies, 78% of IT security teams are looking to embrace zero trust network access in the future. Nineteen percent are actively implementing zero trust, and 15% already have zero trust in place.

Are you looking to adopt a zero trust strategy for access to your private apps?



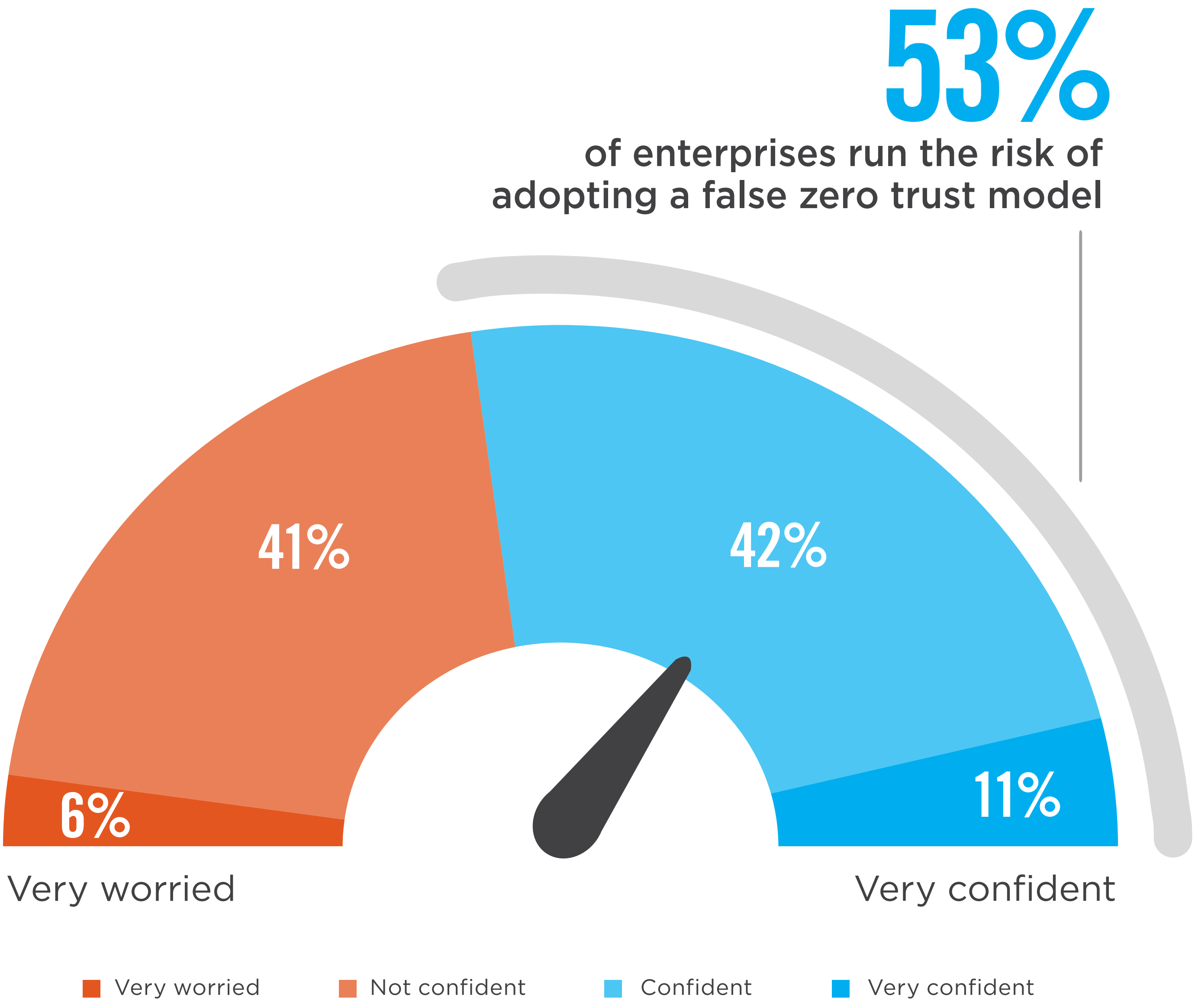
78%

of IT security teams are looking to embrace a zero trust model in the near future.

ZERO TRUST CONFIDENCE

While over three-fourths (78%) of enterprises are looking to adopt zero trust, almost half of enterprise IT security teams lack confidence in their ability to provide zero trust with current security technology. The more confident 53% will likely make the mistake of relying on legacy network security technologies in attempt to embrace a zero trust strategy.

What is your level of confidence in the ability to provide zero trust with your current security technology?



ZERO TRUST BENEFITS

When asked about the benefits of zero trust, two-thirds of IT security professionals (66%) say they are most excited about zero trust's ability to deliver least privilege access to protect private apps. This is followed by apps no longer being exposed to unauthorized users or the Internet (55%), and access to private apps no longer requiring network access (44%).

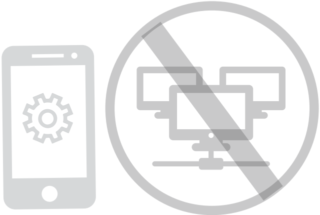
Which of the below most excites you about adopting a zero trust security model?

66%

The ability to limit excessive trust from employees and partners

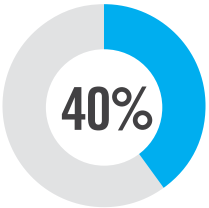
55%

Applications are no longer exposed to unauthorized users or the Internet

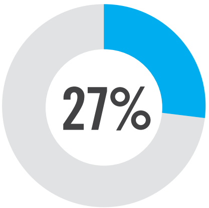


44%

Access to private apps will no longer require network access



Can achieve more effective means of application segmentation



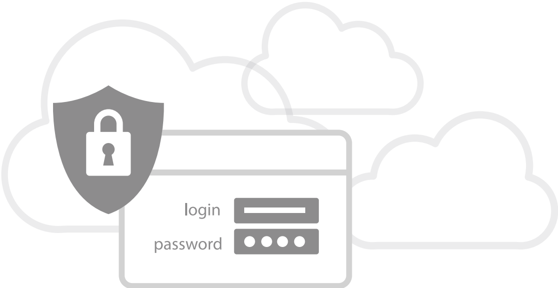
Modern services will help reduce the cost of traditional appliance-based technologies

None 5% | Other 5%

PRIORITY USE CASES

Zero trust is known to have many use cases which contributes to its popularity as a security solution. Below are the use cases found most recently in enterprises adopting a zero trust strategy. Secure access to private apps running in hybrid and public cloud environments (37%), closely followed by using modern remote access services to replace VPN (33%), and controlling third-party access to private applications (18%).

If you have already embraced a zero trust strategy or intend to in the near future, which of the below use cases did/will your team start with?

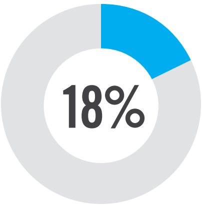


37%

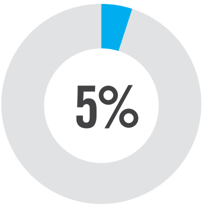
Securing access to private apps across multi-cloud environments

33%

Use modern remote access services as an alternative to VPN



Third-party access to private applications



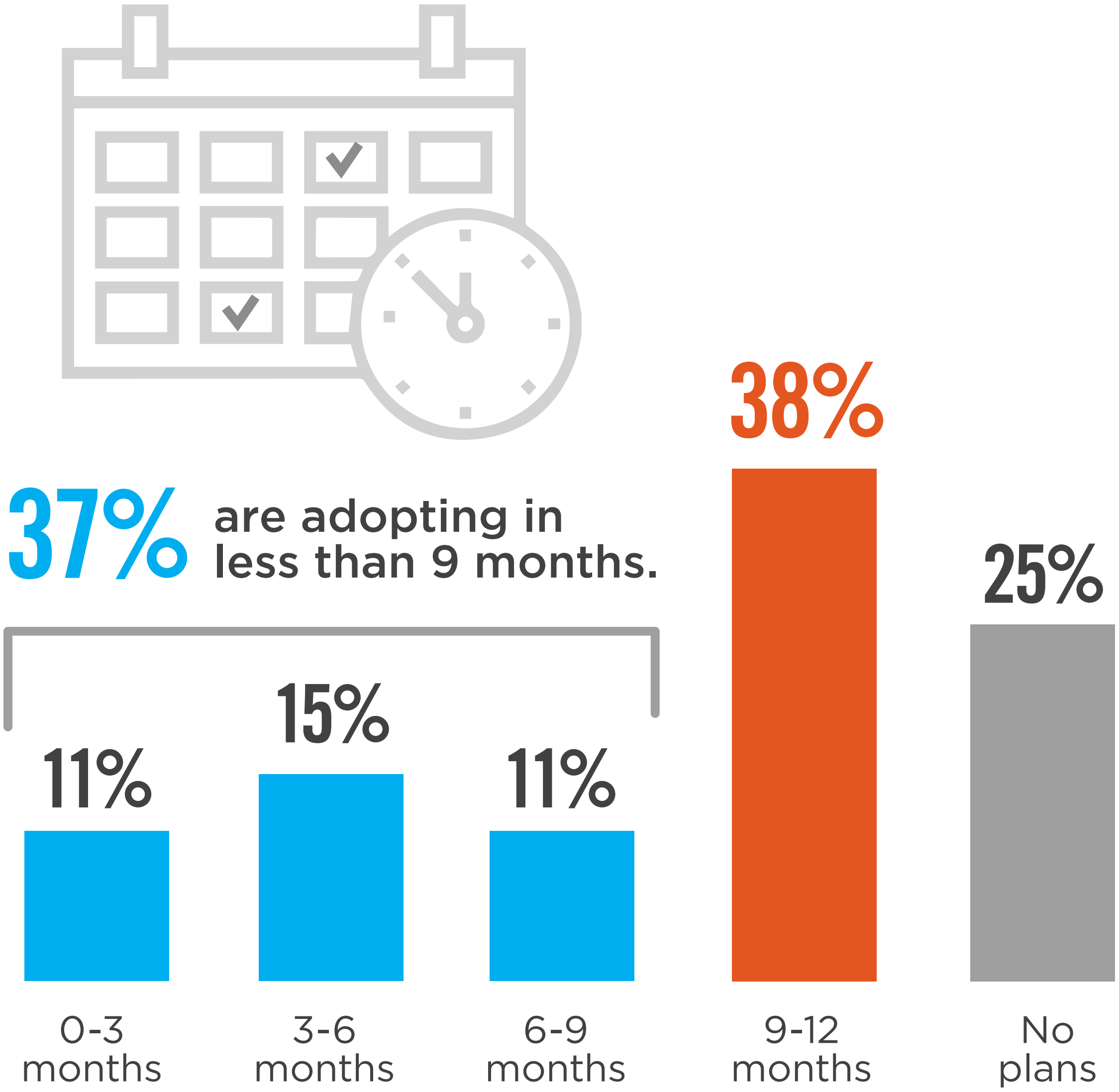
Accelerating M&A and divestitures by removing the need to converge networks

Other 7%

SPEED OF ADOPTION

Zero trust is happening very quickly. In fact, 75% of enterprises will adopt zero trust for a specific use case within the next 12 months. Thirty-seven percent will adopt in less than 9 months. The other 38% will follow suit within 12 months.

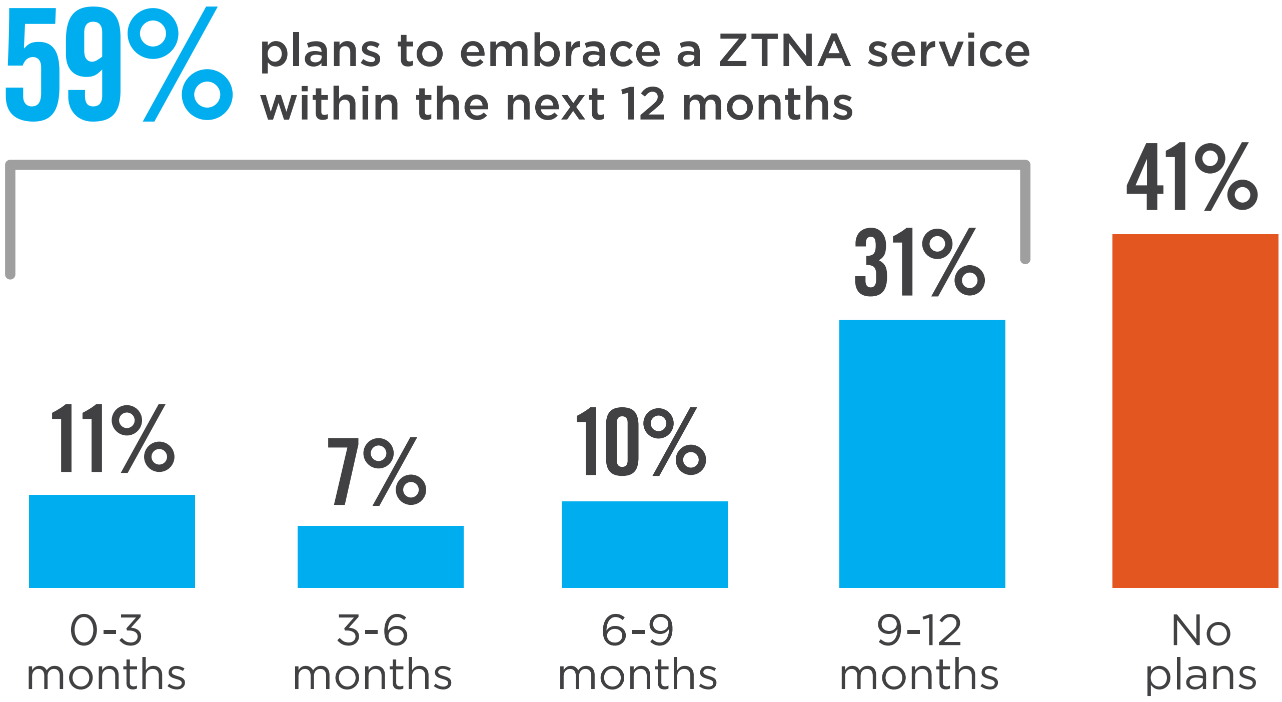
In what timeframe would you most likely adopt one of the zero trust use cases as defined above?



ZTNA ADOPTION

The majority of IT security teams (59%) plans to embrace a zero trust network access (ZTNA) service within the next 12 months. 1/10 will adopt ZTNA within the next 3 months.

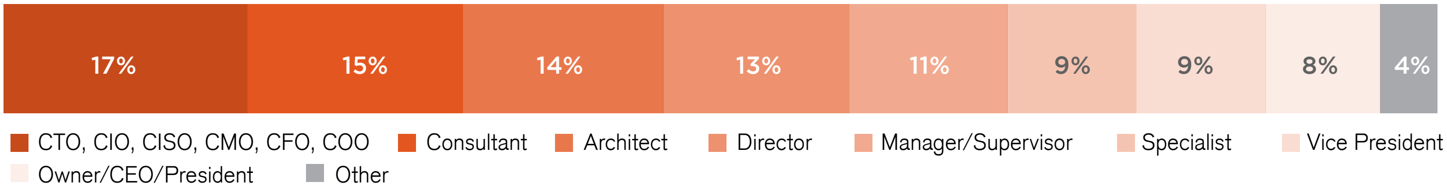
By 2022, Gartner believes 60% of enterprises will phases out VPN in favor of Zero trust network access (ZTNA) services. Do you have plans to adopt a ZTNA service?



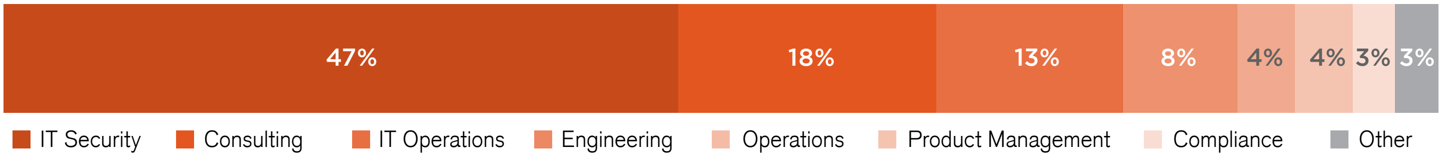
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of 315 IT and cybersecurity professionals in the US, conducted in July and August of 2019 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.

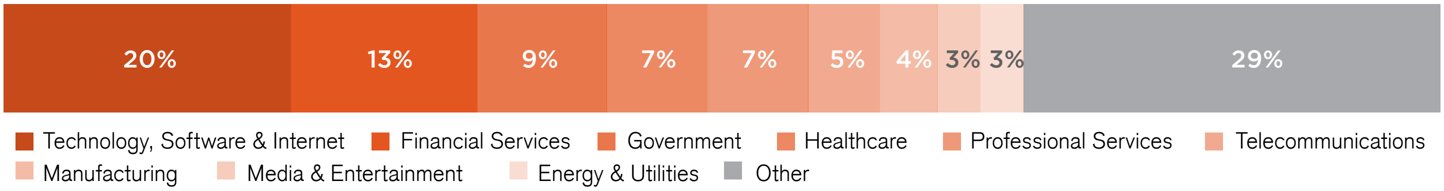
CAREER LEVEL



DEPARTMENT



INDUSTRY


Technology, Software & Internet
Financial Services
Government
Healthcare
Professional Services
Telecommunications
Manufacturing
Media & Entertainment
Energy & Utilities
Other