2021

Cybersecurity INSIDERS

# ZERO TRUST REPORT

Tempered

# Introduction

Enterprise adoption of the Zero Trust security model continues to gain momentum as 73% of organizations are in various stages of zero trust adoption to mitigate growing cyber risk. With its least privilege principle of user and device verification before granting conditional access, 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.

**Key findings include:**

- At the top of the list of key drivers for organizations to initiate or augment a Zero Trust program is security and data protection (85%), followed by breach prevention (70%), reduction of insider threats (49%), and reduction of endpoint and IoT security threats (49%).

- When asked about access challenges, over-privileged employee access is the top concern for 61% of organizations, followed by providing secure access to partners (53%). This is followed by cyber attacks (e.g. DOS, cross-site scripting, MiTM, phishing) (46%), and shadow IT (43%).

We would like to thank Tempered for supporting this important research project.

We hope you 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

Sixty-seven percent of organziations highlight authentication/authorization and data protection as the top core tenet of the Zero Trust value proposition. These tenets are followed by facilitating least privilege access (63%).

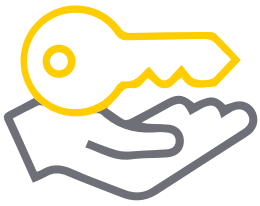
**What Zero Trust tenets are most compelling to you and your organization?**

**67%**

**Continuous authentication/ authorization**

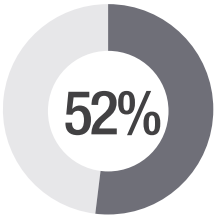
**67%**

**Data protection**
(e.g., secure connection)

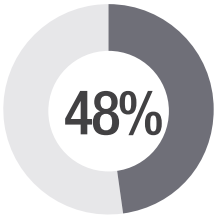


**63%**

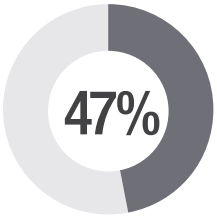
**Facilitating least privilege access**



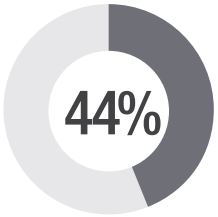

End-to-end access visibility and audit




Centralized, granular access policy




Resource segregation




No trust distinction between internal or external network

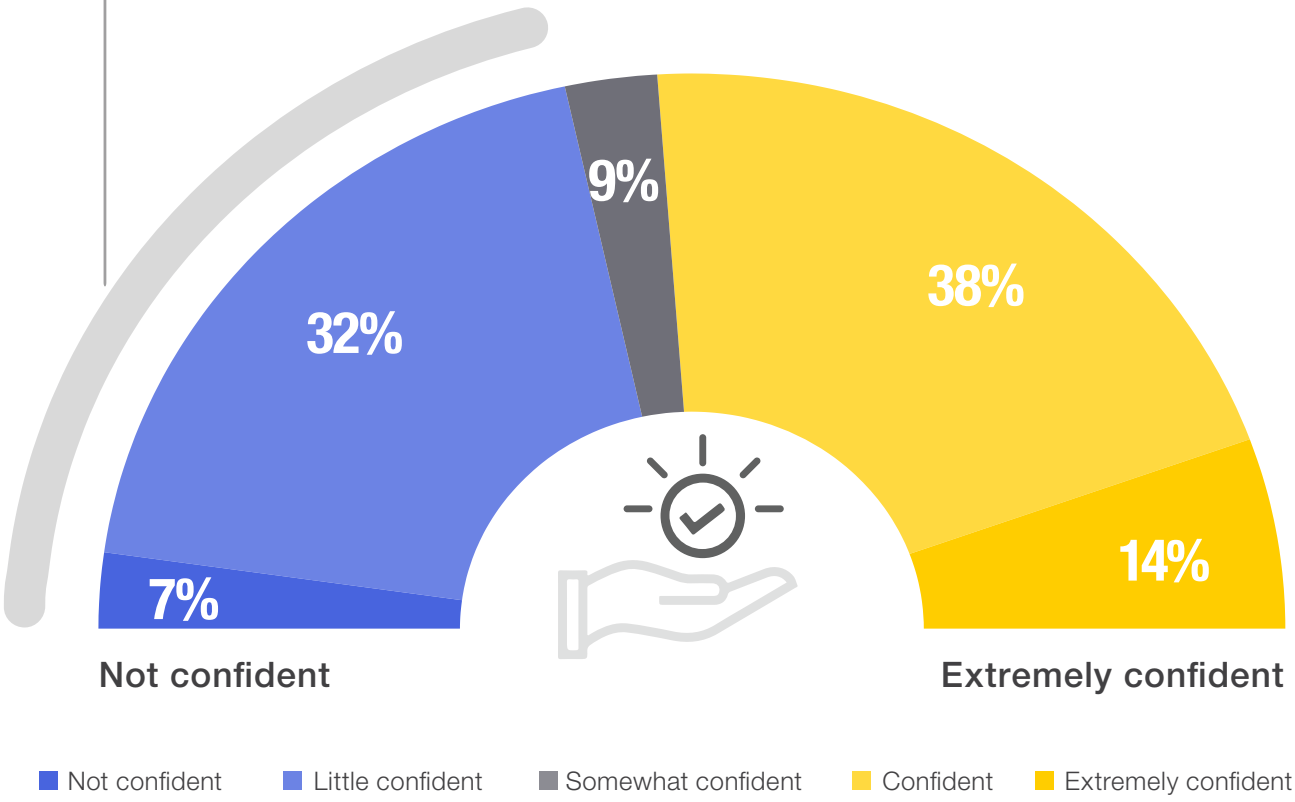
Other 3%

# Zero Trust Confidence

While 52% of organizations are confident or extremely confident in their ability to implement Zero Trust in their secure access architecture, 39% of enterprise IT security teams said they were little to not confident in applying Zero Trust to their secure access architecture.

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

**39%** Of enterprise IT security teams lack confidence in their ability to provide Zero Trust.



# Drivers for Zero Trust

Topping the list of key drivers that motivate organizations to initiate or build out a Zero Trust program is data security (85%). This drive is followed by breach prevention (70%), reduction of insider threats (49%), and reduction of endpoint and IoT security threats (49%).

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

**85%** Security/data protection

**70%**

Breach prevention

**49%**

Reduce insider threats

**49%**

Reduce endpoint and IoT security threats

Industry/regulatory compliance (e.g., HIPAA, GDRP, PCI DSS) 36% | Internal compliance 34% | Operational efficiency 33% | Response to audit or security incident 33% | Address hybrid IT security issues 32% | Other 5%

# Identity Access and Zero Trust Priorities

Organizations prioritize multi-factor authentication (60%) and identity management and governance (47%) as the top two priorities for investment in Zero Trust controls over the next 12 months.

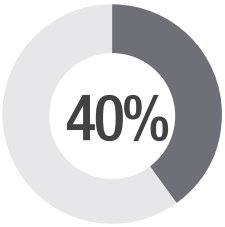
**Which of the following identity access/Zero Trust controls will you prioritize for investment in your organization within the next 12 months?**


**60%**

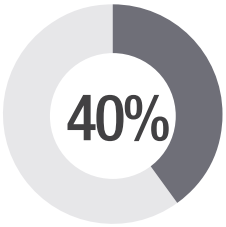
Multi-Factor Authentication (MFA)

**47%**

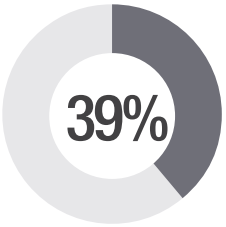
Identity management and governance




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




Privileged Access Management (PAM)



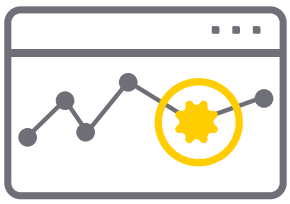

Micro-segmentation

Cloud Access Security Broker (CASB) 33% | Enterprise Mobile Management (EMM) 33% | Identity analytics 25% | Software Defined Perimeter (SDP) 24% | Enterprise directory services 18% | Other 7%

# Secure Access Priorities

Organizations' secure access priorities for the next one to two years are anomalous activity detection and response (58%), securing access from personal, unmanaged devices (57%), and re-evaluating legacy security infrastructure and considering software-defined access (42%).

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



**58%**

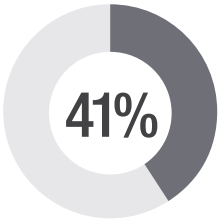
Anomalous activity detection and response

**57%**

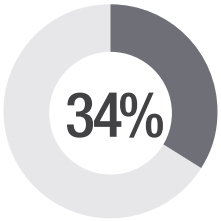
Securing access from personal, unmanaged devices

**42%**

Re-evaluating legacy security infrastructure and considering software-defined access




Stronger visibility and security metrics for executives




Micro-segmentation

# Secure Access Challenges

Over-privileged access is the top concern regarding securing access to apps and resources for 61% of organizations, followed by providing secure access to partners (53%). The next two challenges organizations highlight include cybert attacks (46%), (e.g., DOC, criss-site scripting, MiTM, phishing) and shadow IT (43%).

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

**61%**

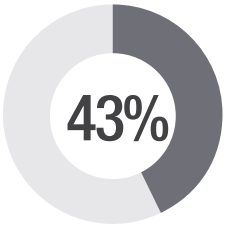
**Over-privileged employee access**

**53%**

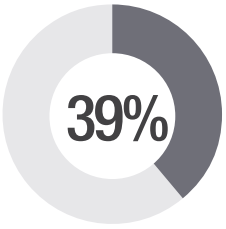
**Partners insecurely accessing apps and resources**

**46%**

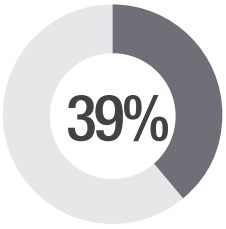
**Cyber attacks**
(e.g., denial of service, cross-site scripting, man-in-the-middle, phishing)




Shadow IT




Vulnerable, jailbroken or lost mobile devices accessing resources



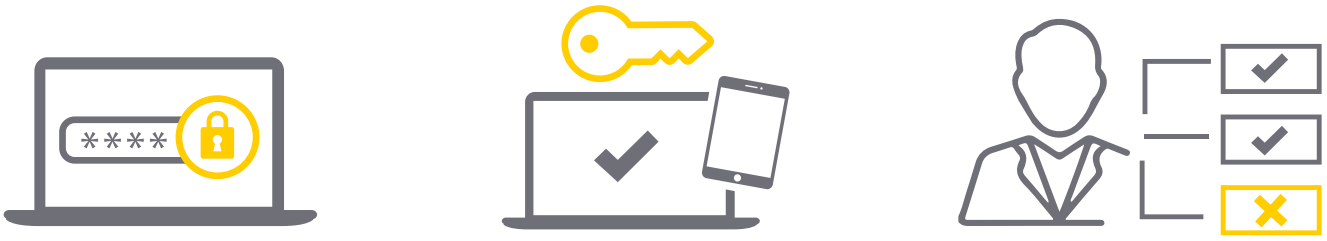

Manual processes are complex and slow down ability to react quickly

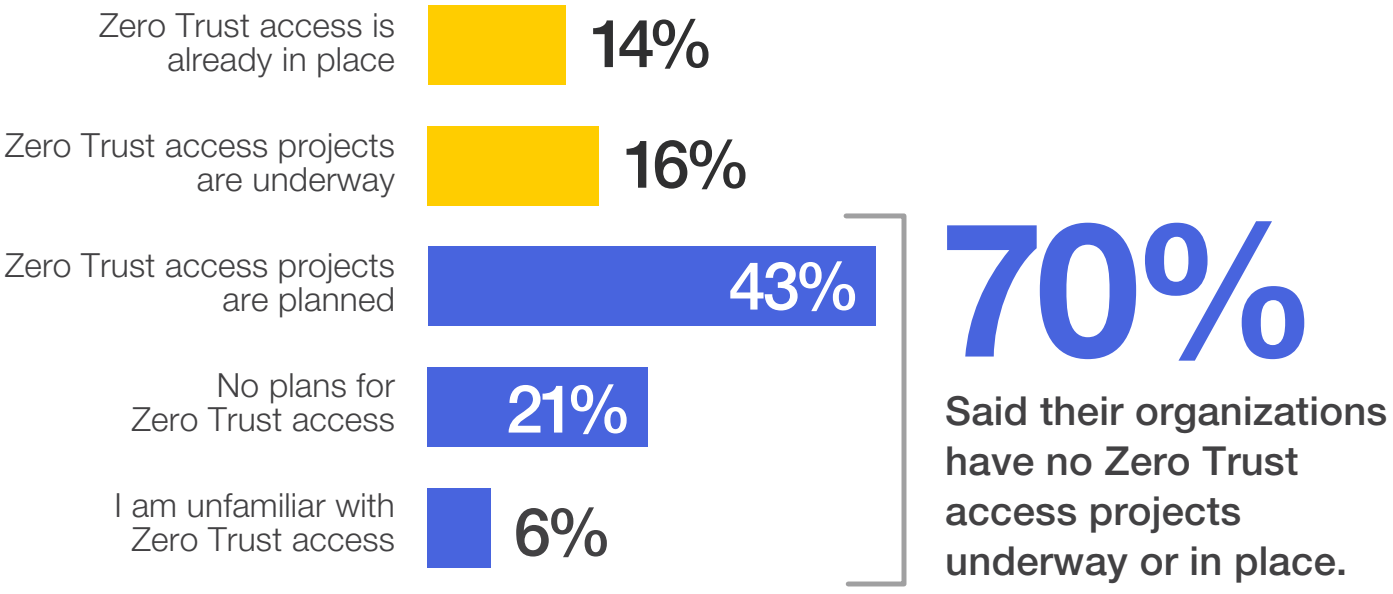
At risk devices accessing network resources (e.g., unknown, unsanctioned, non-compliance endpoints) 14% | Other 2%

# Adoption of Zero Trust

The concept of Zero Trust is quickly gaining momentum but 70% said their organizations have no Zero Trust access projects underway or in place. Only 14% of organizations are using a Zero Trust access model and 16% are in the process of implementing Zero Trust.

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



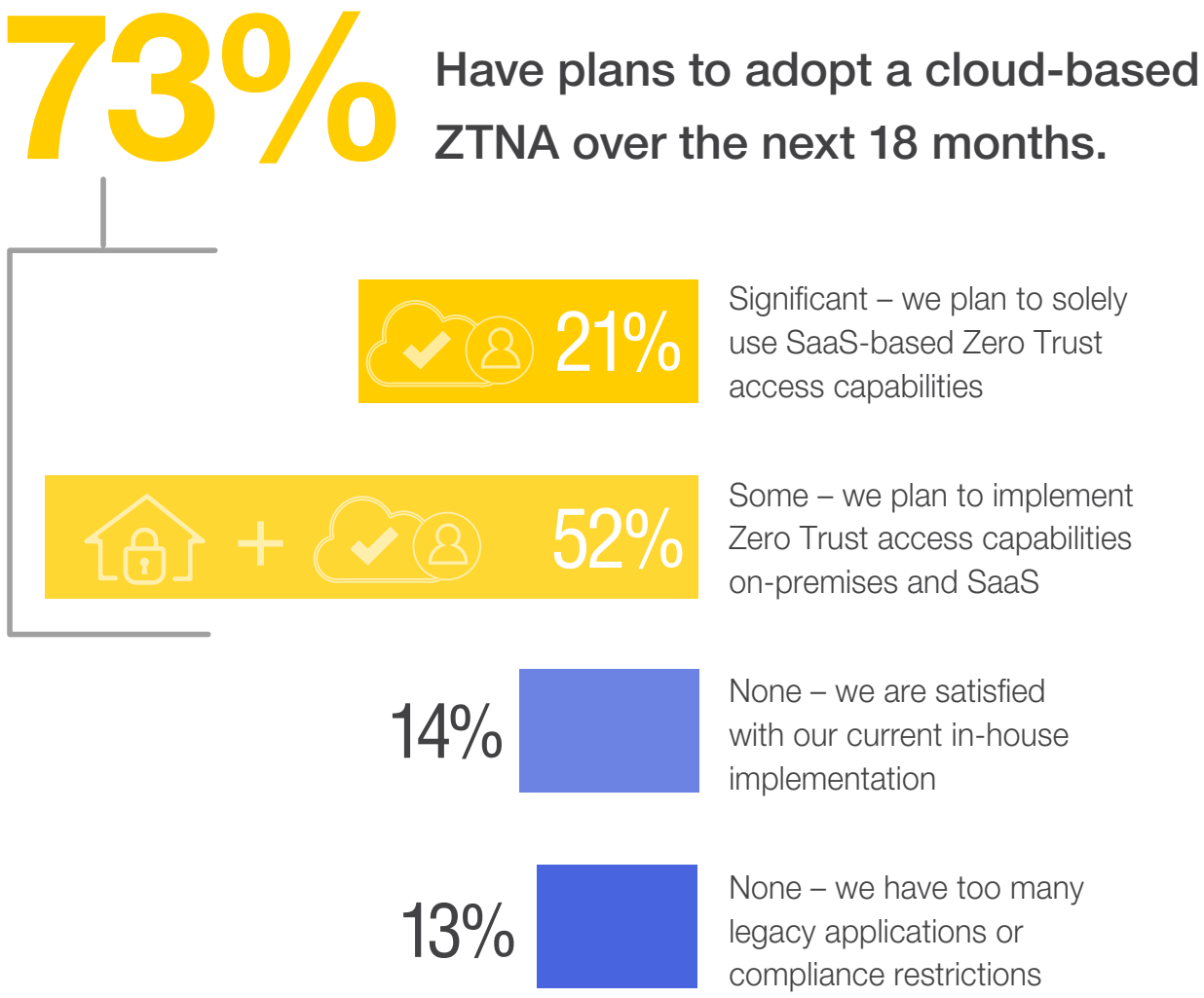

**70%**

**Said their organizations have no Zero Trust access projects underway or in place.**

# Zero Trust SaaS

Security is moving to the cloud, and ZTNA (Zero Trust Network Access) is no exception. Almost three-quarters (73%) of respondents are planning to adopt a cloud-based ZTNA solution over the next 18 months.

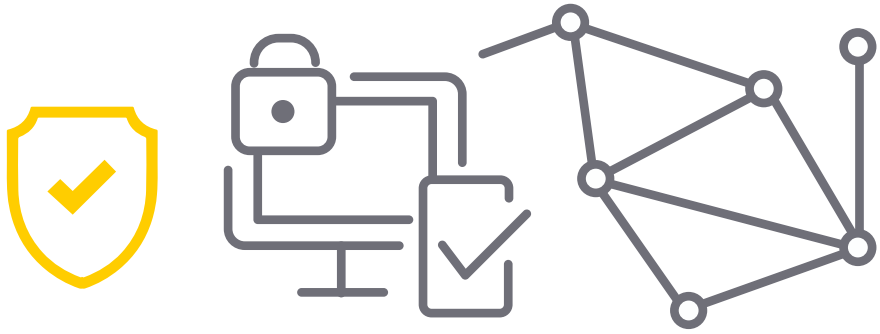
**Over the next 18 months, to what extent do you and your organization plan to move Zero Trust access capabilities to SaaS?**

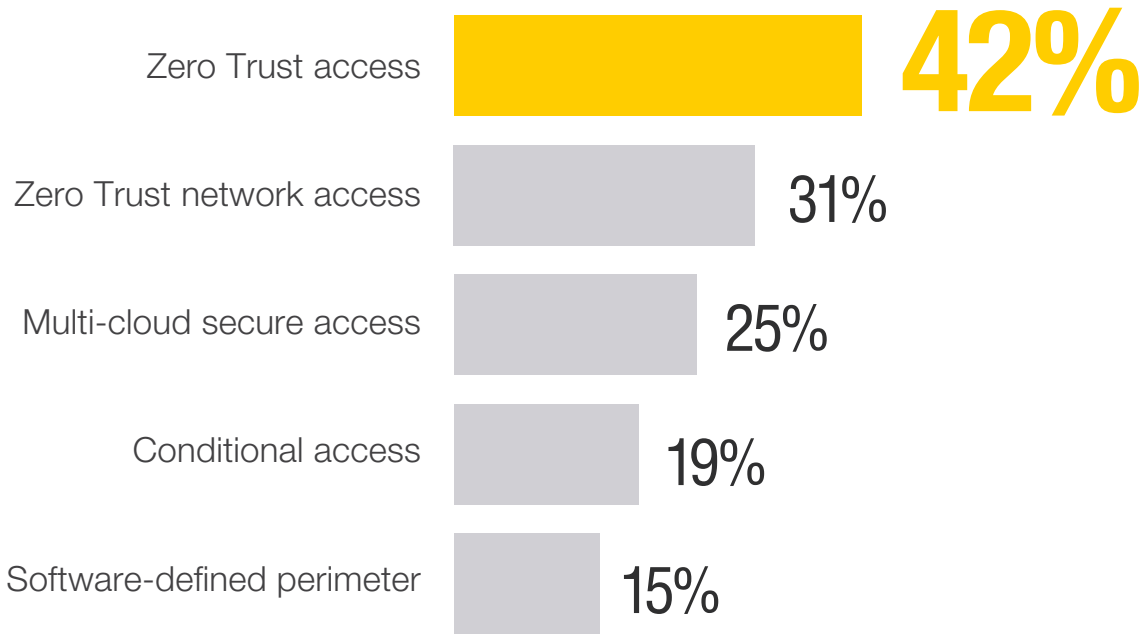


# Enterprise Access Security Direction

Forty-two percent of organizations said they preferred the title “Zero Trust Access” as the term that best describes their enterprise access security direction over terms such as ZTNA, multi-cloud secure access, conditional access, and software-defined perimeter.

**A new approach to access applications and resources is being discussed under multiple names. Select the term that best describes your enterprise access security direction?**

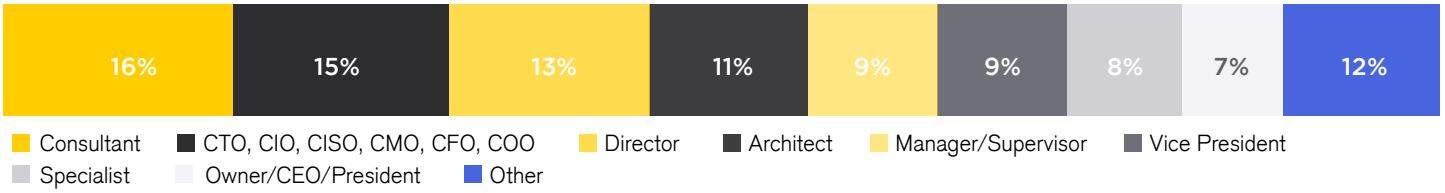




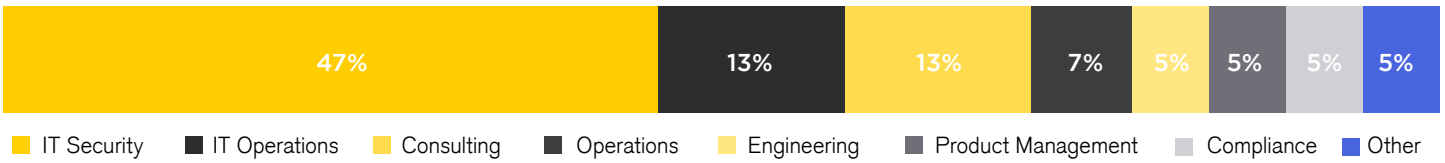
# Methodology & Demographics

This report is based on the results of a comprehensive online survey of 323 IT and cybersecurity professionals in the US, conducted in November 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.

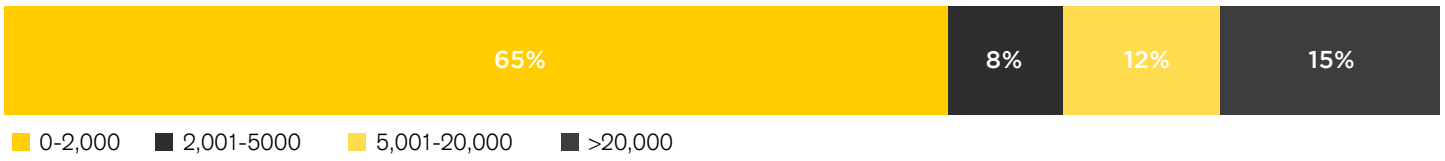
## CAREER LEVEL



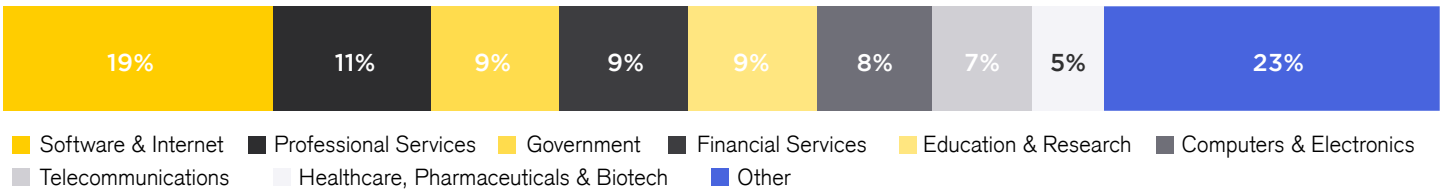

## DEPARTMENT




## COMPANY SIZE




## INDUSTRY




Tempered makes the industry's only truly native zero-trust Software-Defined Perimeter (SDP) solution. Airwall is the modern air gap for all connected things. Airwall makes it easy to create and maintain hyper-secure networks across complex infrastructure anywhere, including IT/OT/ICS/SCADA, remote and in the cloud. Airwalled networks are multi-factor authenticated, micro-segmented, encrypted end-to-end, and impervious to lateral movement. Ready to make your company's critical assets and infrastructure invisible to threats?

www.tempered.io