

CISSO Perspectives and Progress in Deploying Zero Trust



The permanent and official location for the CxO Trust Working Group is
<https://cloudsecurityalliance.org/research/working-groups/cxo-trust-working-group/>

© 2022 Cloud Security Alliance – All Rights Reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance at <https://cloudsecurityalliance.org> subject to the following: (a) the draft may be used solely for your personal, informational, non-commercial use; (b) the draft may not be modified or altered in any way; (c) the draft may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the draft as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance.

Acknowledgments

Lead Authors

Hillary Baron
John Yeoh

Contributors

Illena Armstrong
Josh Buker
Daniele Catteddu
Sean Heide
Alex Kaluza
Claire Lehnert (design)
Stephen Lumpe (design)
Jim Reavis

Executive Summary

The principles of Zero Trust have been around for over a decade. Yet recently, the term and its implementation have garnered a lot more attention for enterprises protecting their IT systems. With the advancement of digital transformation, the shift of the workforce during the pandemic, and the announcement of the US executive order on cybersecurity, Zero Trust has taken a front seat as a promise for protecting enterprises.

Standard Development Organizations (SDOs) have recently initiated their work on Zero Trust (e.g. NIST SP800-207), and similarly, other relevant agencies and organizations have started to publish guidelines, recommendations, and foundational literature. This relative immaturity of the standardization landscape, the lack of an agreed upon vocabulary and industry definitions, alongside multiple Zero Trust branded vendor solutions have created confusion. CSA was prompted to further investigate the industry's understanding, perception, and adoption of Zero Trust.

The goal of this CSA survey is to better understand Zero Trust strategies within organizations. Security practitioners were asked to evaluate the following:

- Maturity and level of priority Zero Trust has in the organization
- Benefits and drivers toward adopting Zero Trust
- Challenges and barriers to adopting Zero Trust
- Investments needed to support the Zero Trust strategy

Some of the other areas covered in this survey include where Zero Trust falls as a priority in the organization, the percentage of those who have completed related implementations, top business challenges, and top technical challenges.

The initial research shared is the result of 823 responses from IT and security professionals from various organization sizes and locations including 219 C-level executives. Some of the interesting findings from the survey include:

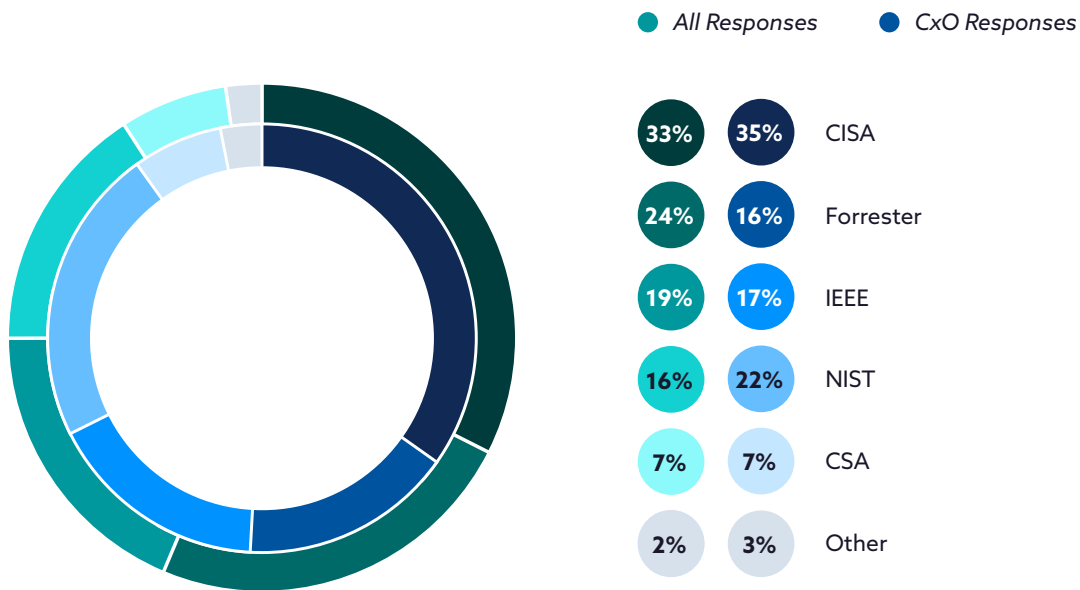
- 80% of C-level executives have Zero Trust as a priority for their organizations.
- 94% are in the process of implementing Zero Trust strategies
- 77% are increasing their spending in Zero Trust over the next 12 months.

Further analysis of the findings will allow CSA to help define guidance in access management, policy enforcement, Zero Trust scaling issues, and other challenges identified by practitioners in the survey. Through the survey and upcoming report, CSA is looking to learn where C-level executives are in terms of their Zero-Trust strategies, pain points, vendor needs, management requirements/oversight, technical considerations, legacy challenges, adoption rates, and stakeholder involvement. CSA is dedicated to educating the C-suite, board members, staff, and stakeholders on the benefits of Zero Trust.

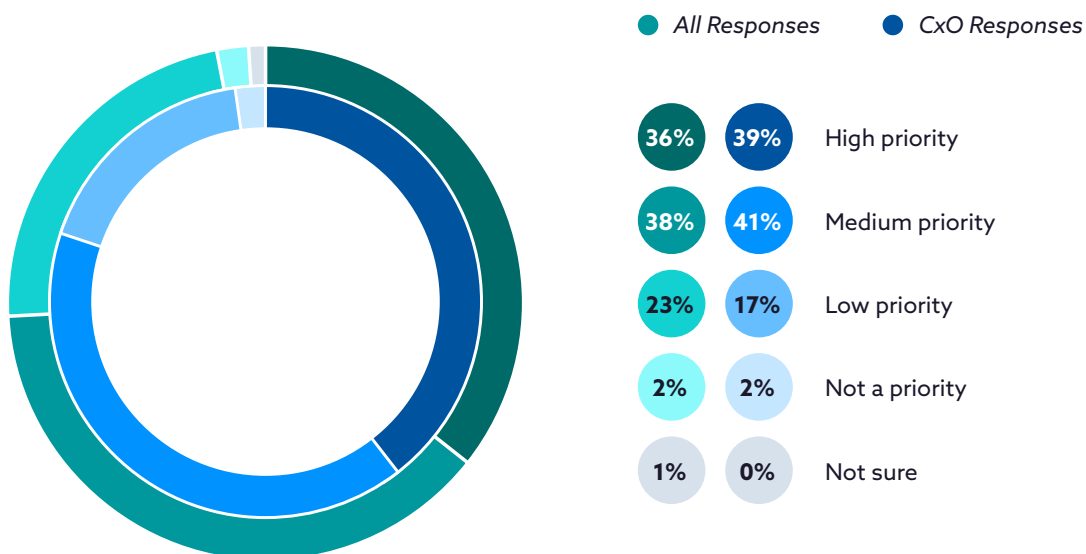
The survey report will be based on the perceptions and opinions of security professionals from survey responses and interviews collected by CSA in Q1-Q3 of 2022. Researchers, analysts, and industry experts on Zero Trust within the CSA community will present further observations and statistical correlations from the data collected.

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to widely promote best practices for ensuring cyber security in cloud computing and IT technologies. CSA also educates various stakeholders within these industries about security concerns in all other forms of computing. CSA's membership is a broad coalition of industry practitioners, corporations, and professional associations. One of CSA's primary goals is to conduct surveys that assess information security trends. These surveys provide information on organizations' current maturity, opinions, interests, and intentions regarding information security and technology.

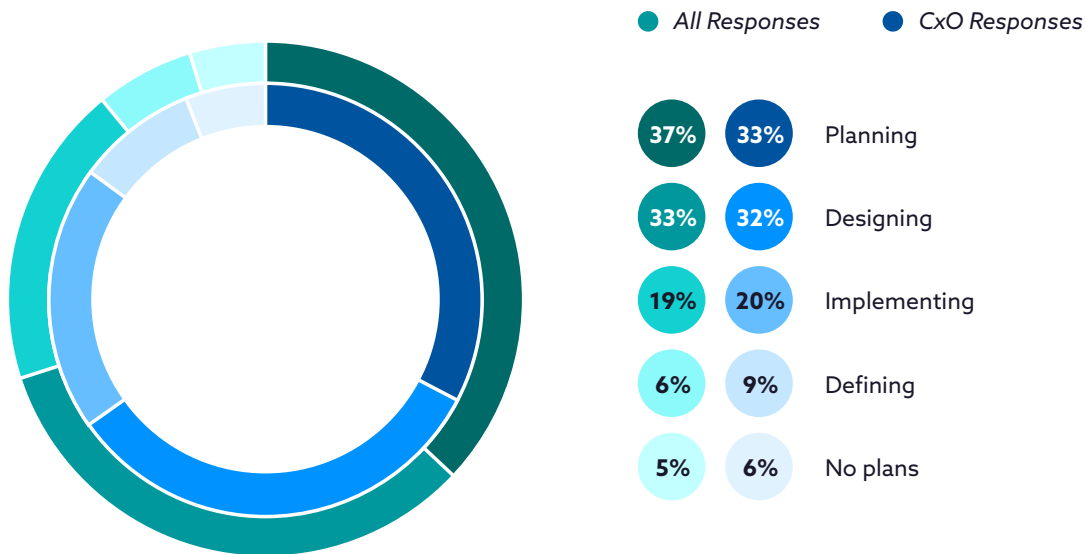
Which of the following industry references most closely aligns with your organization's definition/guidelines on Zero Trust?



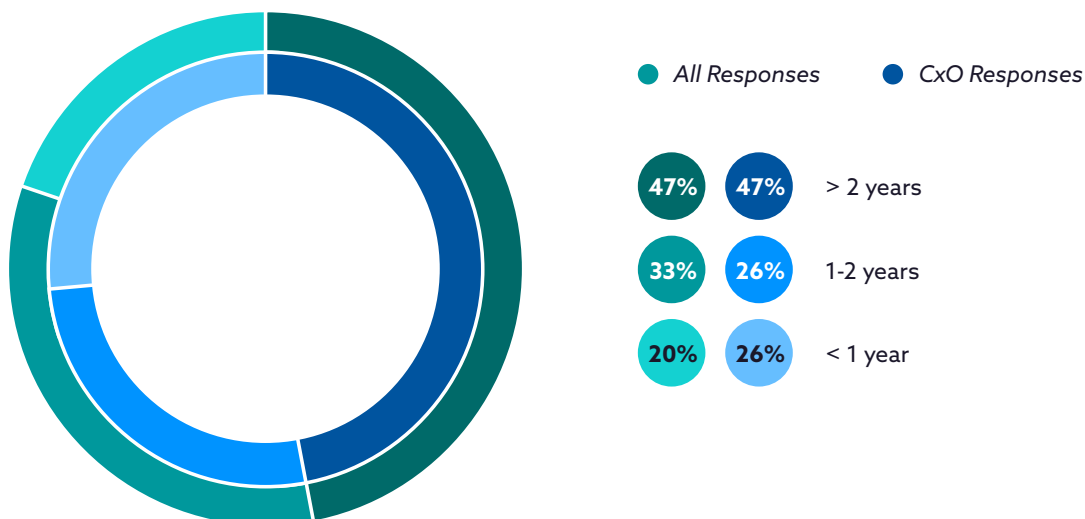
What level of priority does Zero Trust have in your organization?



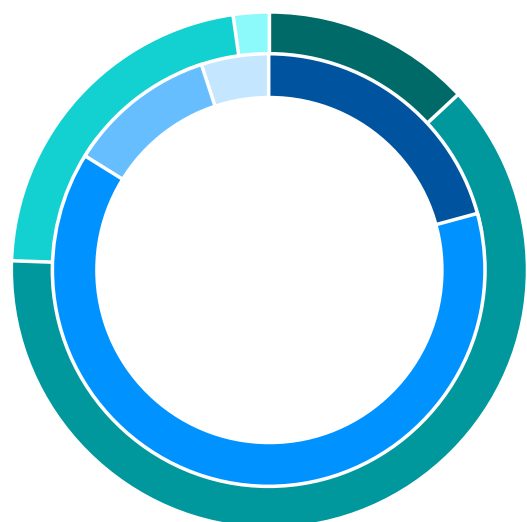
Where in the implementation process of its Zero Trust strategy is your organization?



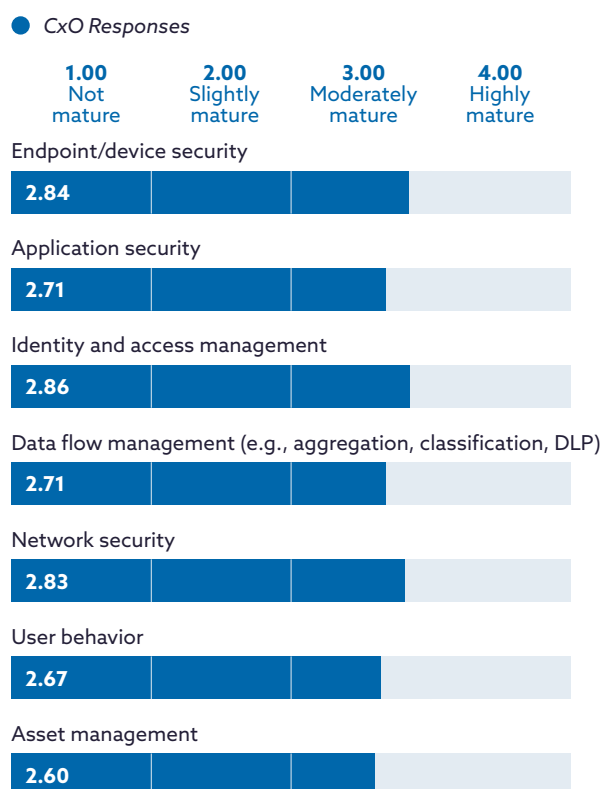
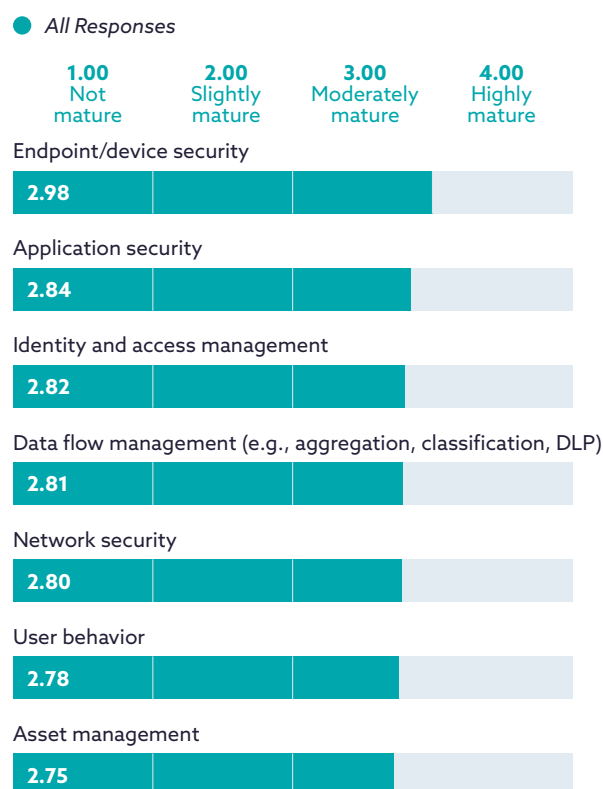
When did your organization initially implement its Zero Trust strategy?



Has your organization benefited from the Zero Trust initiative?



Rate the level of maturity of your organization's Zero Trust strategy in the following areas:



Where does your company feel most vulnerable?

● All Responses

Protecting against zero-day threats

53%

Protecting your work-from-home users

51%

Protecting against data loss

36%

Protecting against threats in encrypted traffic

32%

Protecting all ports and protocols

18%

● CxO Responses

Protecting against zero-day threats

54%

Protecting your work-from-home users

50%

Protecting against data loss

36%

Protecting against threats in encrypted traffic

32%

Protecting all ports and protocols

21%

Select up to 3 areas hindering your organization's adoption of Zero Trust.

● All Responses

Identity and access management

34%

Data flow management

31%

Network security

31%

Asset management

30%

Application dependencies

29%

Governance and policy

29%

Behavior monitoring

29%

Endpoints/devices security

29%

● CxO Responses

Identity and access management

37%

Data flow management

32%

Network security

30%

Asset management

24%

Application dependencies

32%

Governance and policy

26%

Behavior monitoring

32%

Endpoints/devices security

25%

What are the main drivers for your organization for adopting a Zero Trust initiative? (Select up to 3)

All Responses

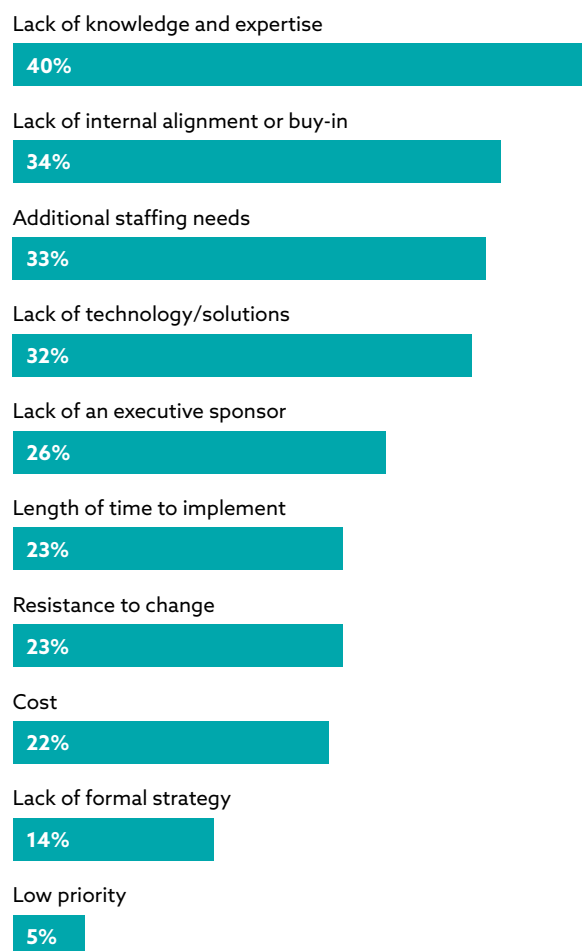


CxO Responses

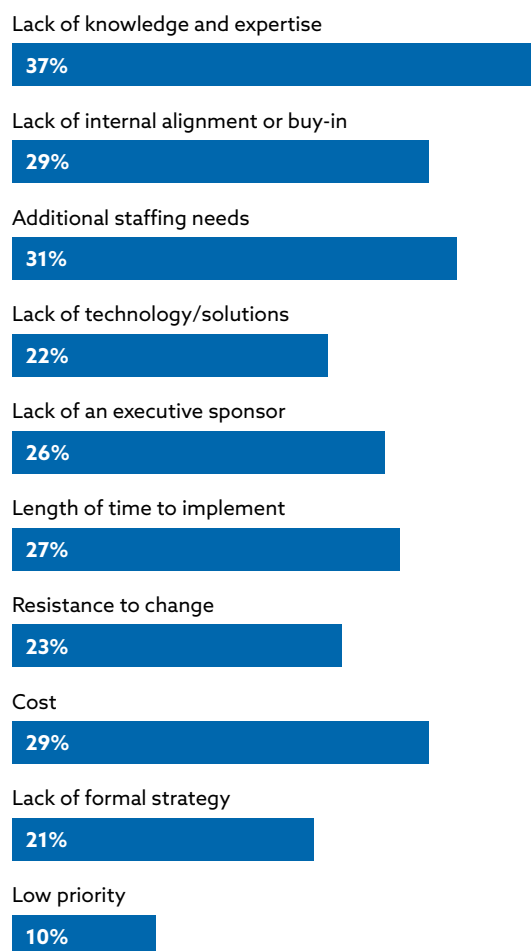


What are the top *business* barriers to adopting a Zero Trust strategy in your organization? (Select up to 3)

● All Responses

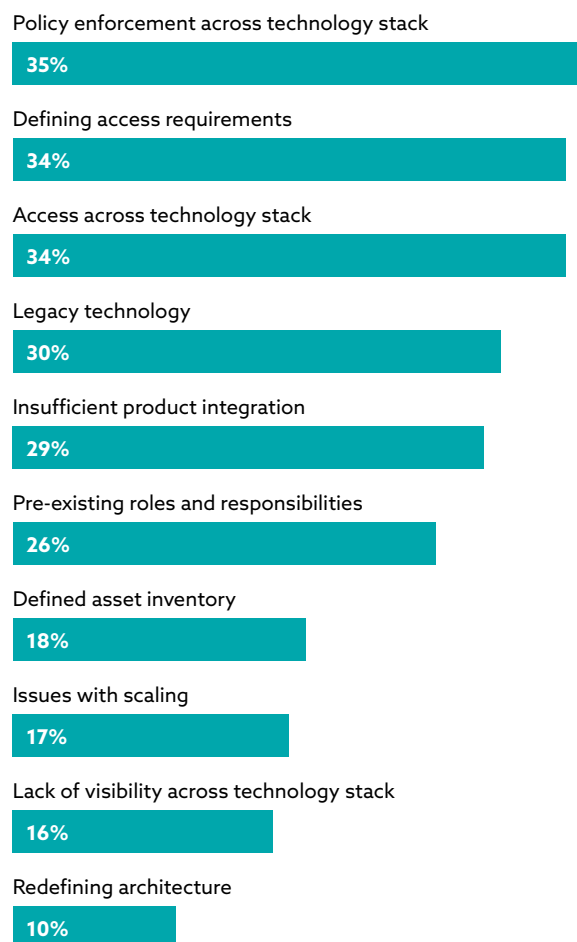


● CxO Responses

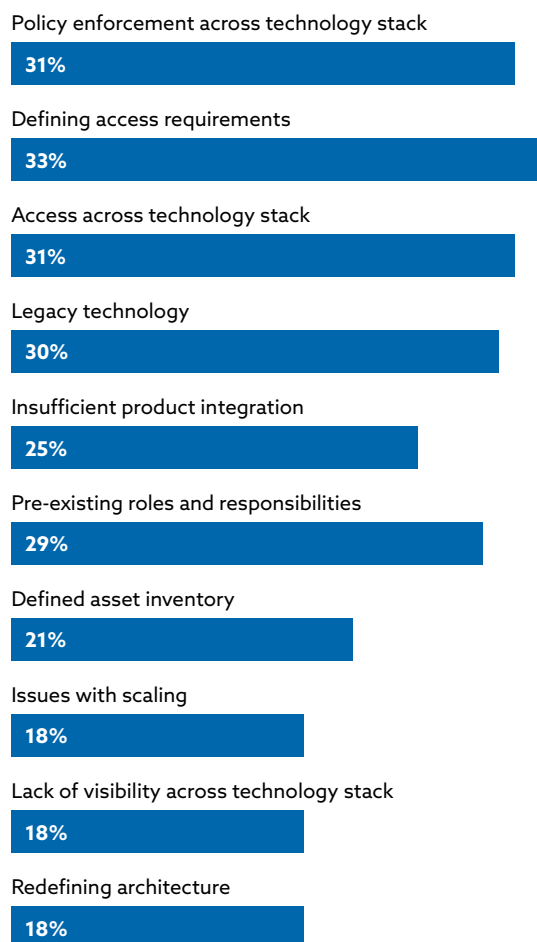


What are the top *technical* barriers to adopting a zero trust strategy in your organization? (Select up to 3)

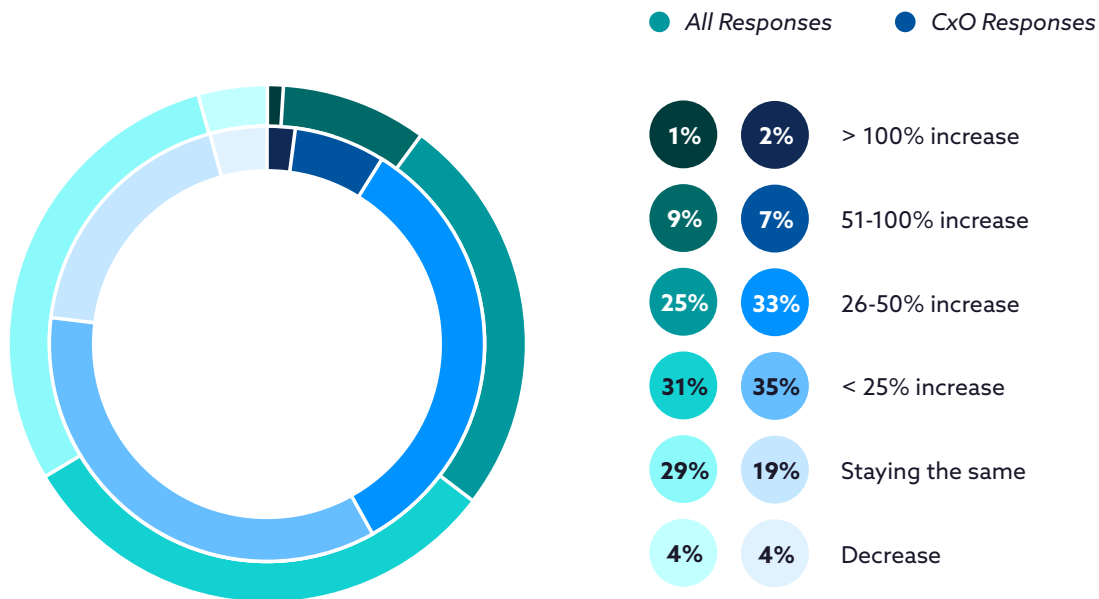
● All Responses



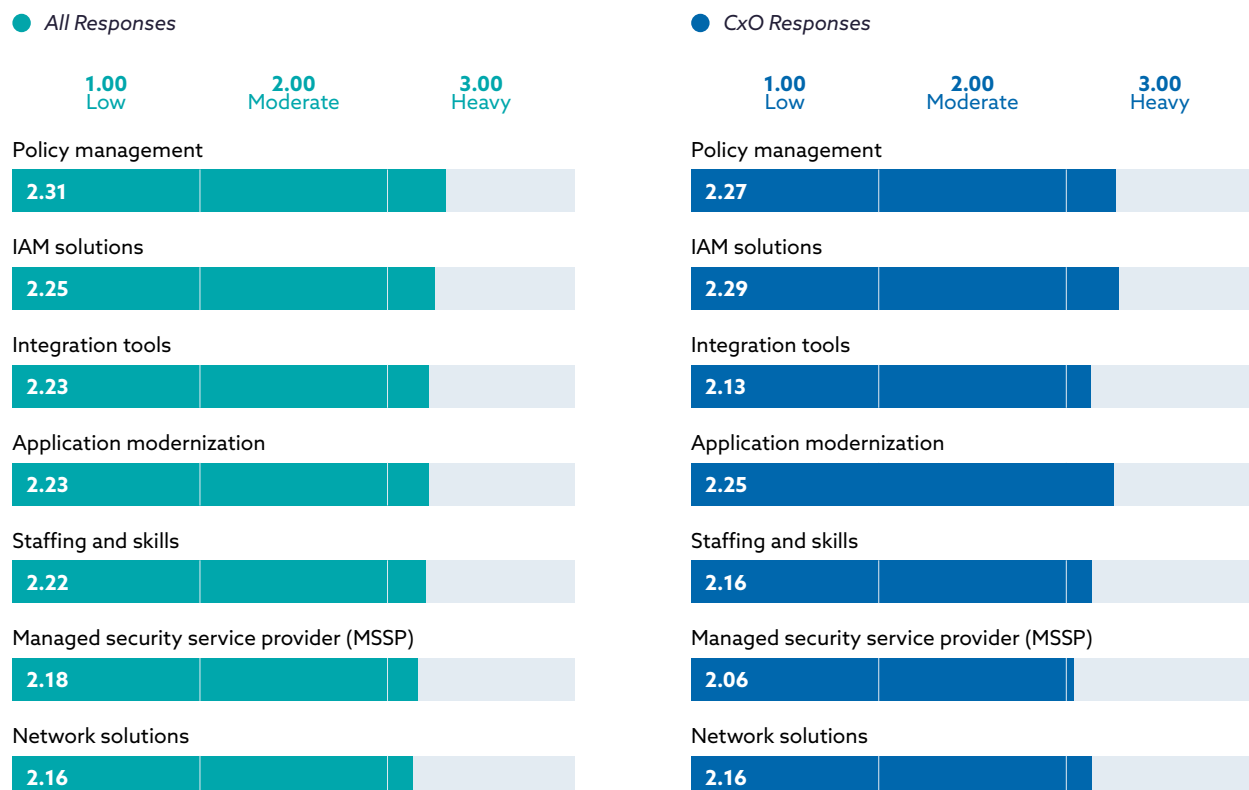
● CxO Responses



Describe your organization's investment in Zero Trust over the next 12 months.

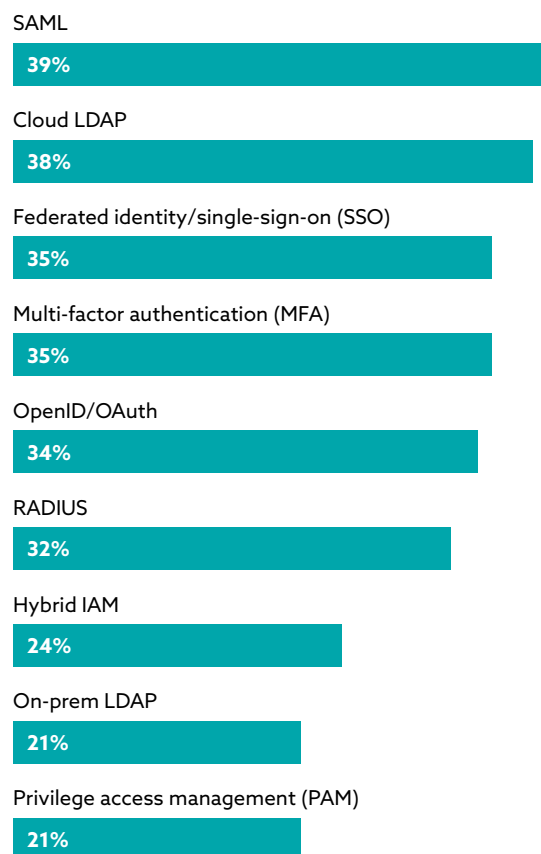


For your Zero Trust initiative, how much is your organization investing in the following types of solutions?

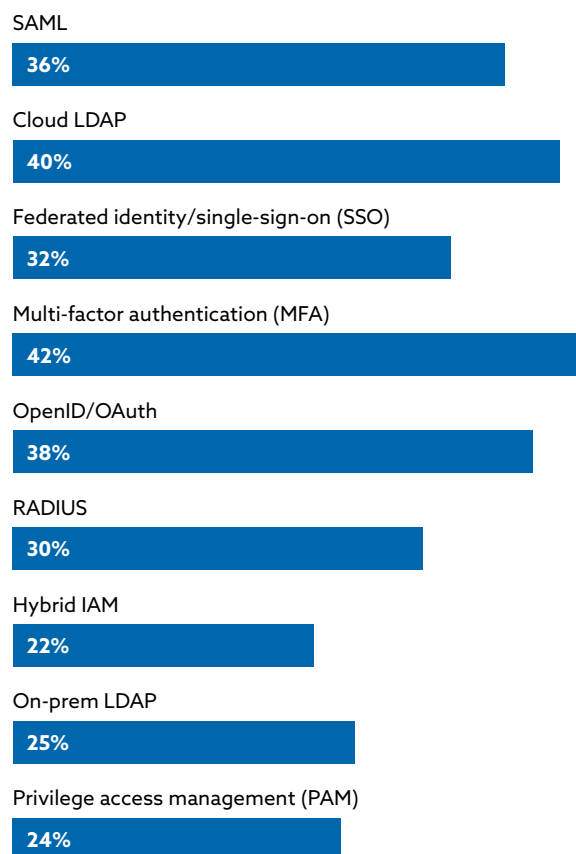


What types of *identity services* does your organization have? (Select all that apply)

● All Responses

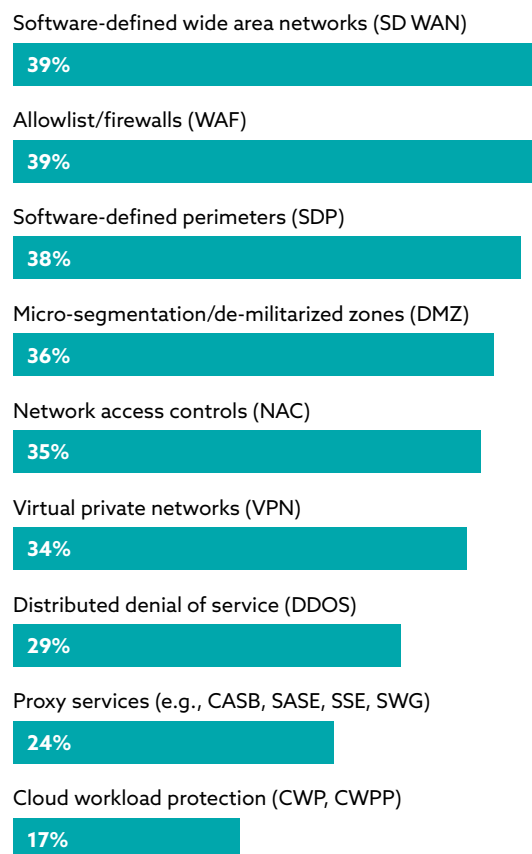


● CxO Responses

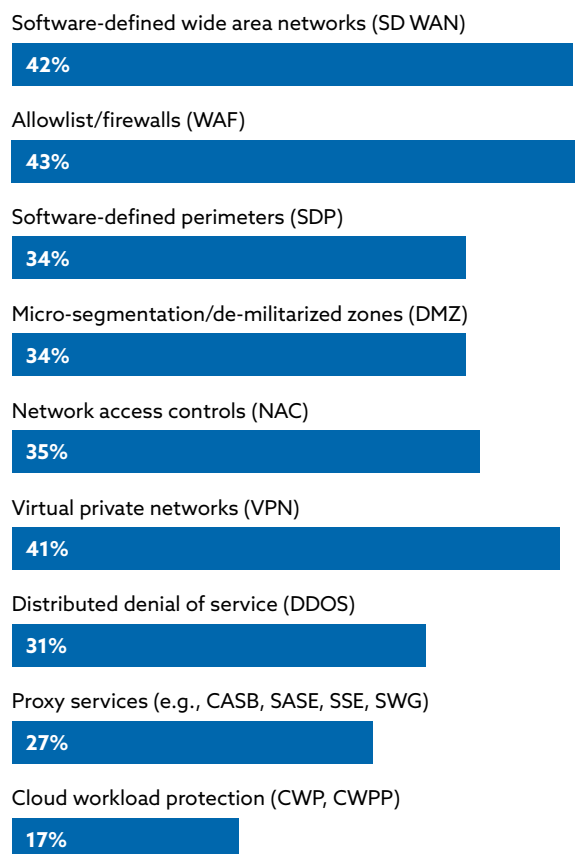


What types of *network solutions* does your organization have? (Select all that apply)

● All Responses

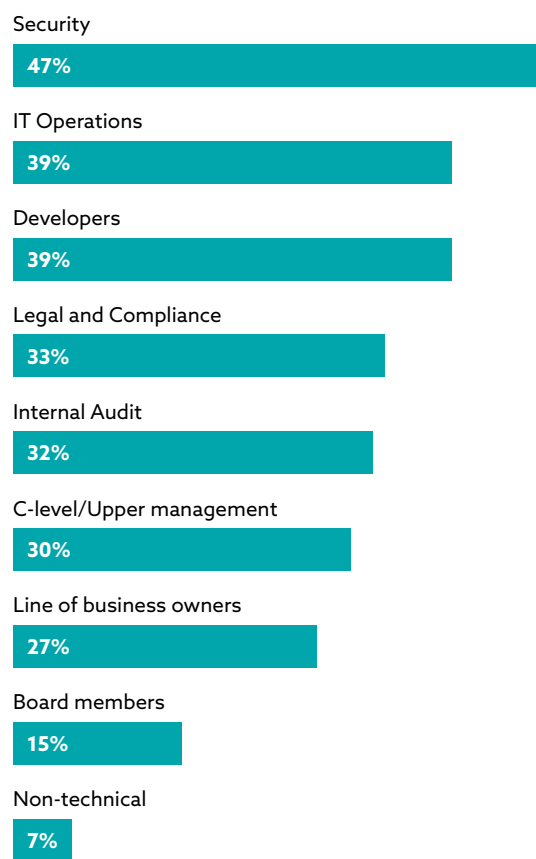


● CxO Responses

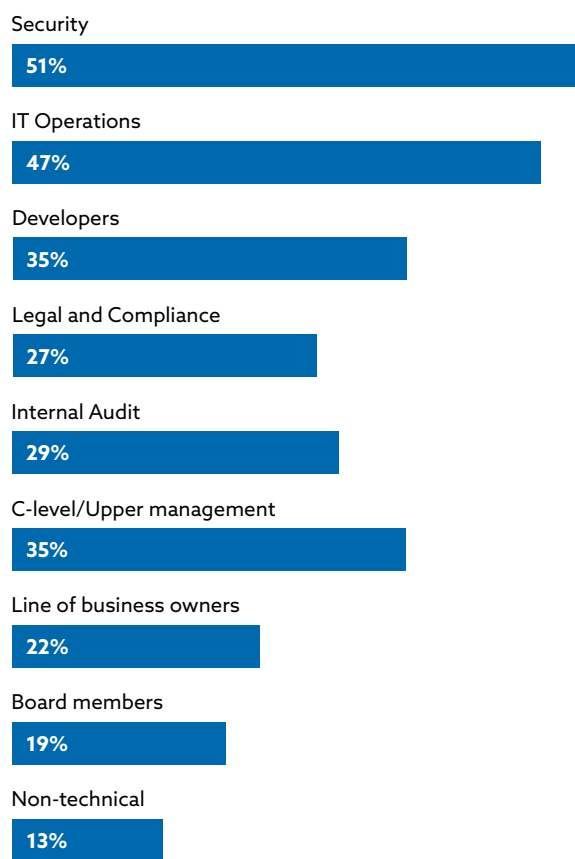


Which business functions are involved in your organization's Zero Trust implementation? (Select all that apply)

● All Responses

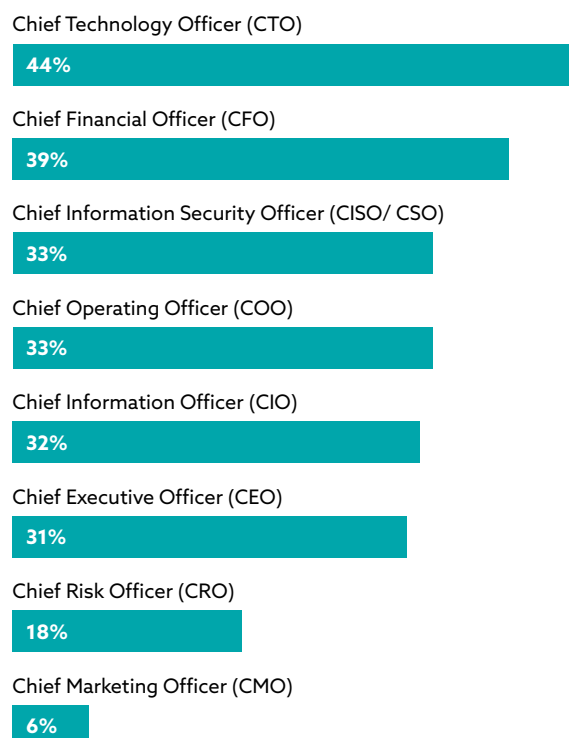


● CxO Responses

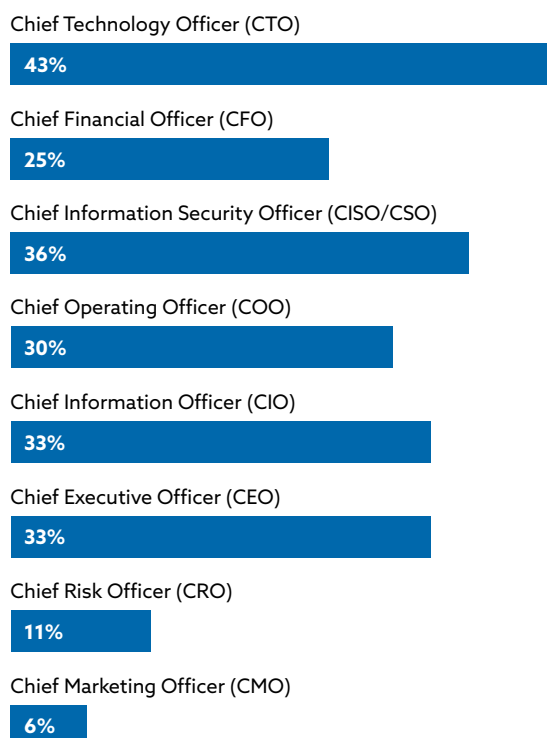


Which member(s) of your organization's C-suite own or sponsor the Zero Trust implementation? (Select all that apply)

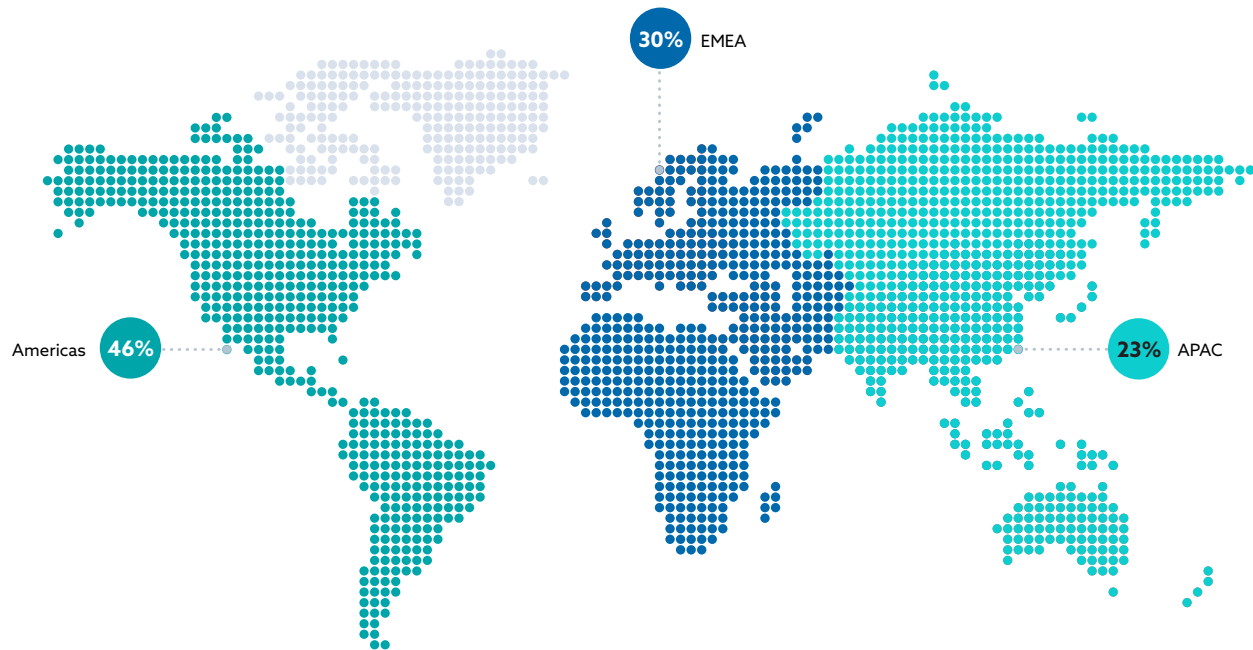
All Responses



CxO Responses



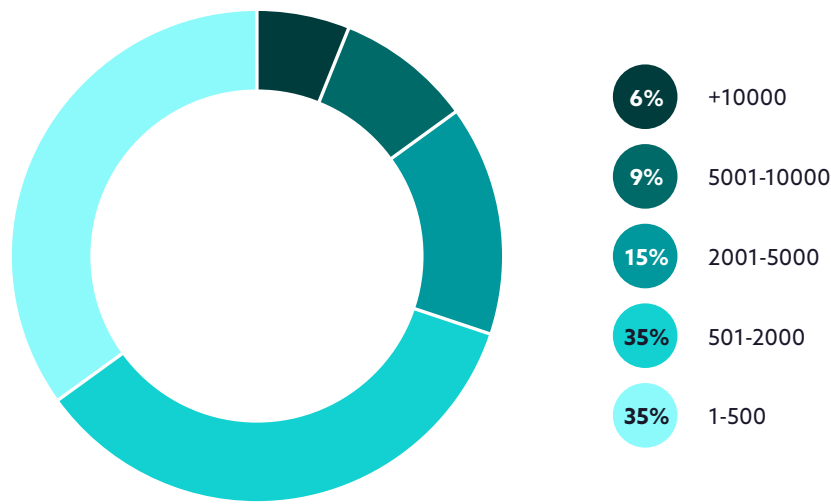
What region are you, as an individual, located in?



Which of the following best describes the principal industry of your organization?



How many employees does your organization have?



Which of the following best describes your role in your organization?

