BigID
Know Your Data
Privacy • Protection • Perspective

Zero Trust Security Strategy Adoption

Zero Trust is a concept of blanket skepticism when it comes to network access, even from internal users, requiring verification at all entry points and never assuming access privileges. But while Zero Trust is gaining momentum as a strategic ideal, rearchitecting the network to achieve Zero Trust might not be straightforward. After a year of distributed workforces and numerous headline-making cybersecurity incidents across industries, are decision-makers adopting a Zero Trust security strategy?

Pulse surveyed over 200 digital decision-makers to understand:

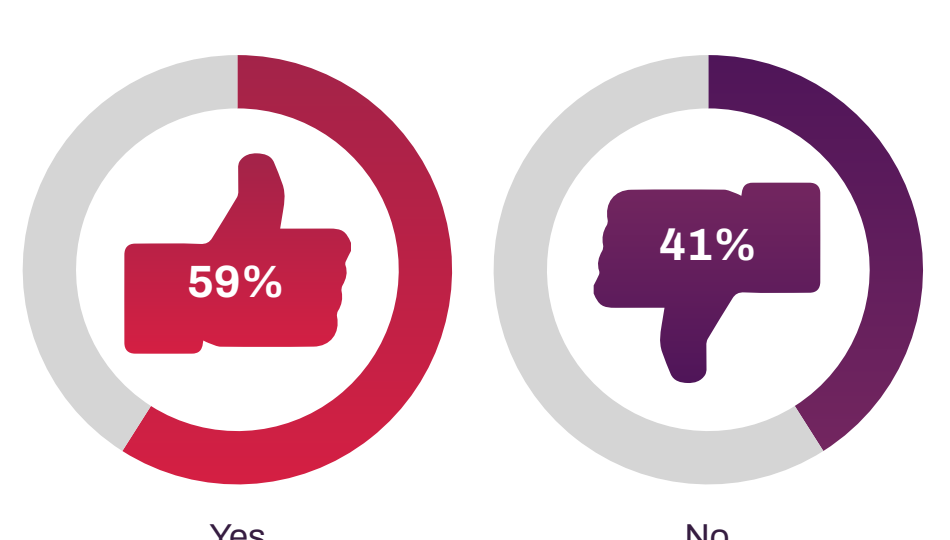
- Levels of Zero Trust adoption, or timelines for implementation
- Perceived benefits of Zero Trust, as well as barriers to adoption
- Essential components for Zero Trust, and whether organizations have them in place

Data collected from May 3 - June 13, 2021
Total respondents: 245 tech decision-makers

Just over half of IT leaders already have a Zero Trust security strategy in place—and most others will follow, eventually

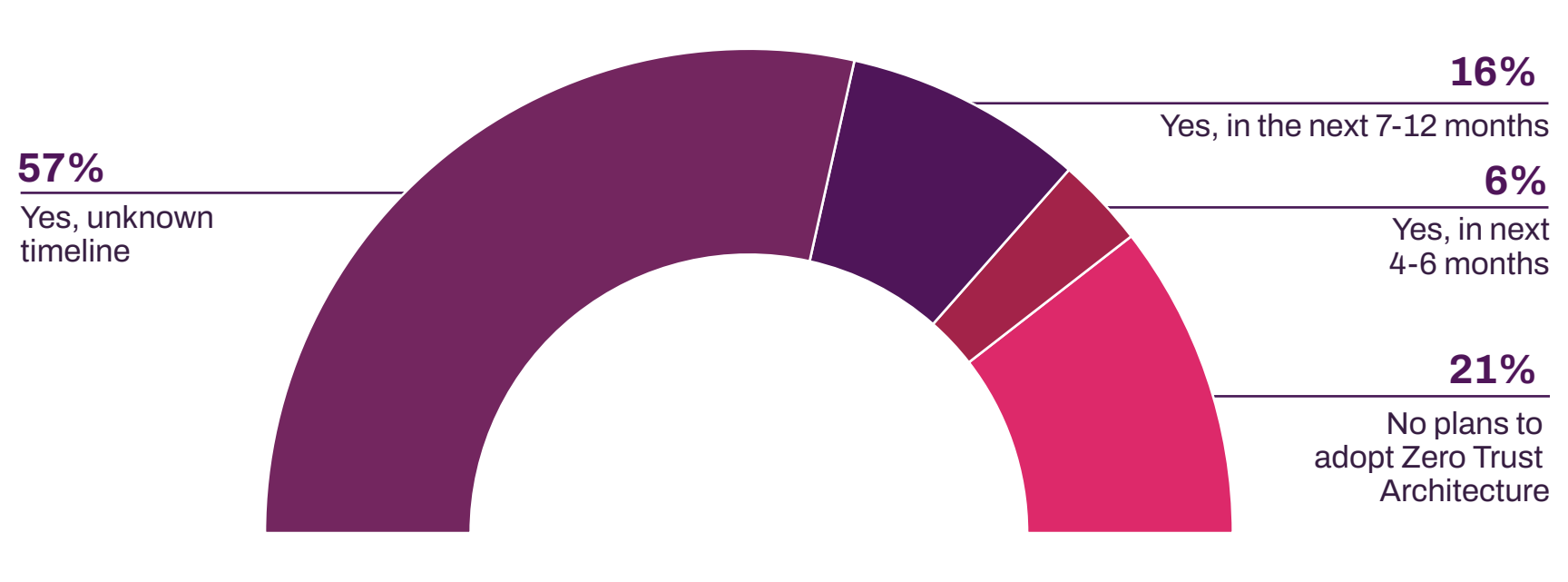
Most decision-makers (59%) are currently deploying a Zero Trust security strategy, but 41% have yet to.

Are you currently deploying a Zero Trust security strategy in your organization?



Of those who aren't currently deploying a Zero Trust security strategy, 79% have plans for adoption at some future point.

Do you have plans to adopt a Zero Trust security strategy in the future?



"Zero Trust has transformed (for the better) many processes and our ability to protect our internal assets."

- C-Suite, small-medium business

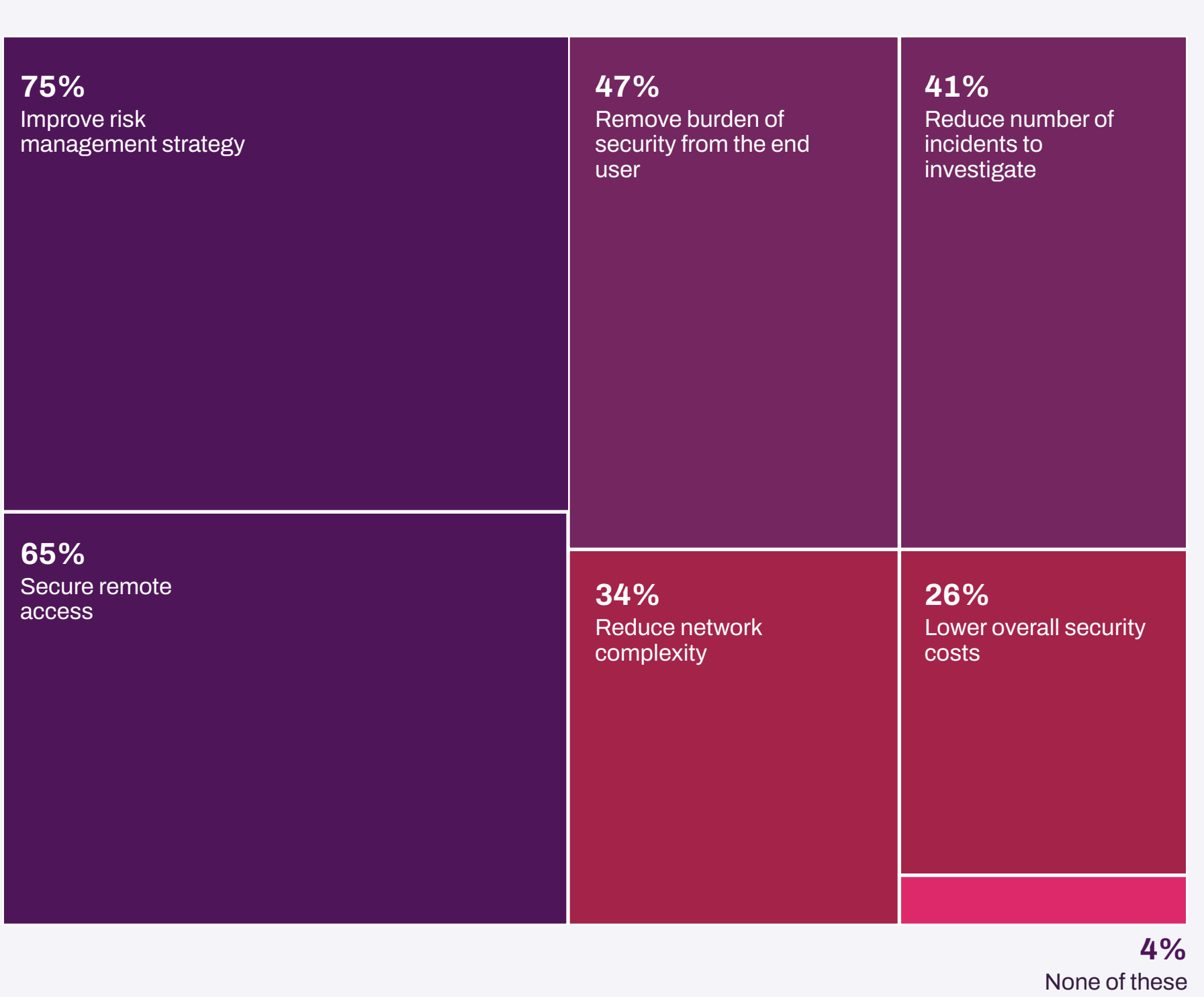
"I'm very interested in implementing [Zero Trust] at my organization, but we have such a complicated network architecture that I worry it might be impossible."

- C-suite, public sector

Zero Trust adoption driven by risk management and secure remote access—and protecting customer data the top business case

Improving risk management strategy (75%) and securing remote access (65%) are the top reasons to adopt a Zero Trust security strategy.

What are the main reasons to adopt a Zero Trust security strategy?

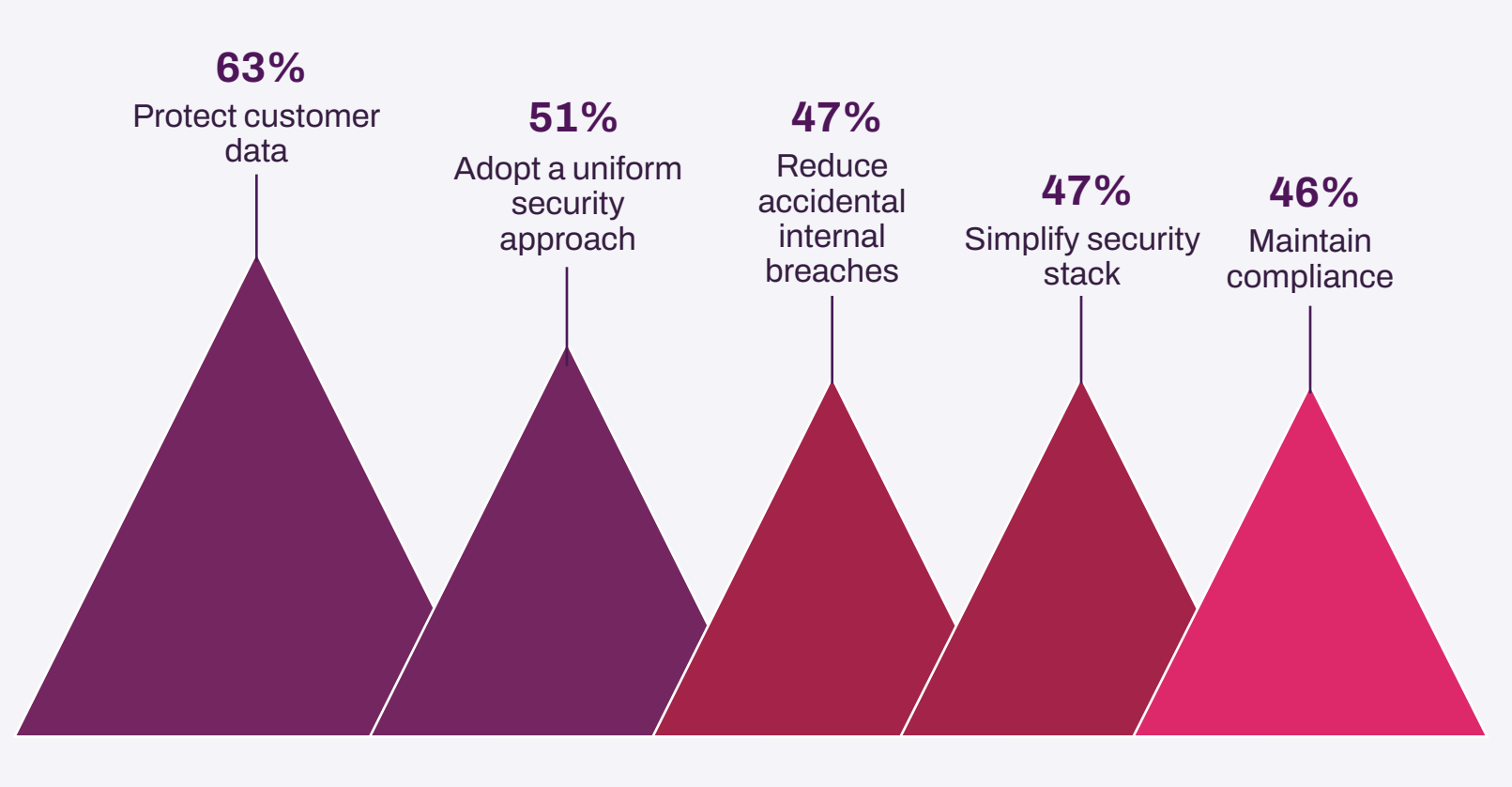


"[Zero Trust] is a business imperative driven by the explosive number of threat vectors and incidents. It is only a matter of time before every company is impacted. Zero Trust gives companies a fighting chance."

- C-suite, start-up

As for the businesses, protecting customer data (63%) and a uniform security approach (51%) are the main drivers for Zero Trust adoption.

What are the top business cases for a Zero Trust security strategy?



Reduce malicious internal breaches (41%), Centralize security oversight of public clouds (30%), Foster business continuity (26%), Reduce costs (26%), Minimize need for highly skilled security professionals (21%), Other (1%)

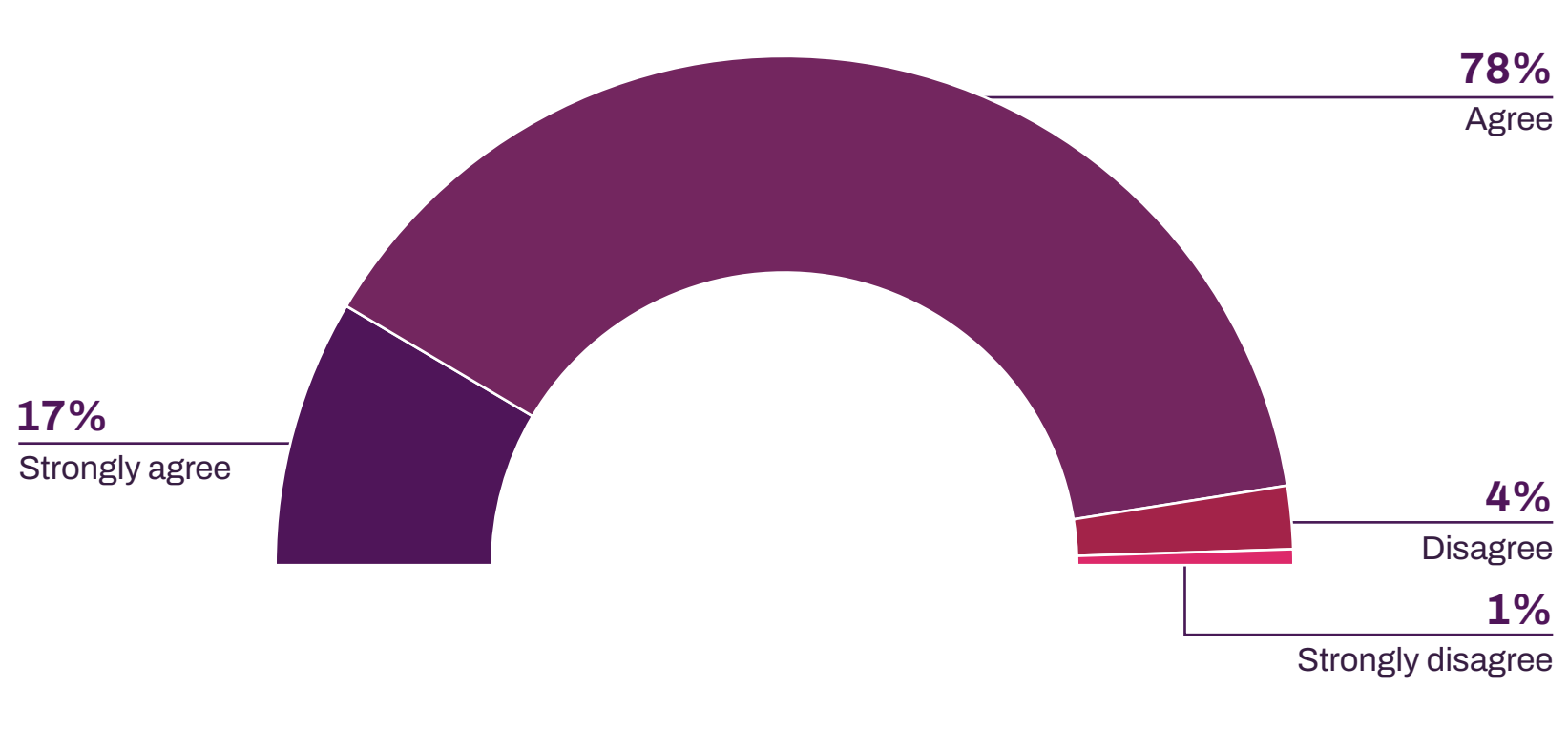
"Zero Trust is a perfect fit in companies where data sets are highly protected and usage patterns are consistent."

- VP, large enterprise

Most agree that a Zero Trust security strategy reduces security incidents, particularly data leakage and internal threats, and also simplifies security architecture

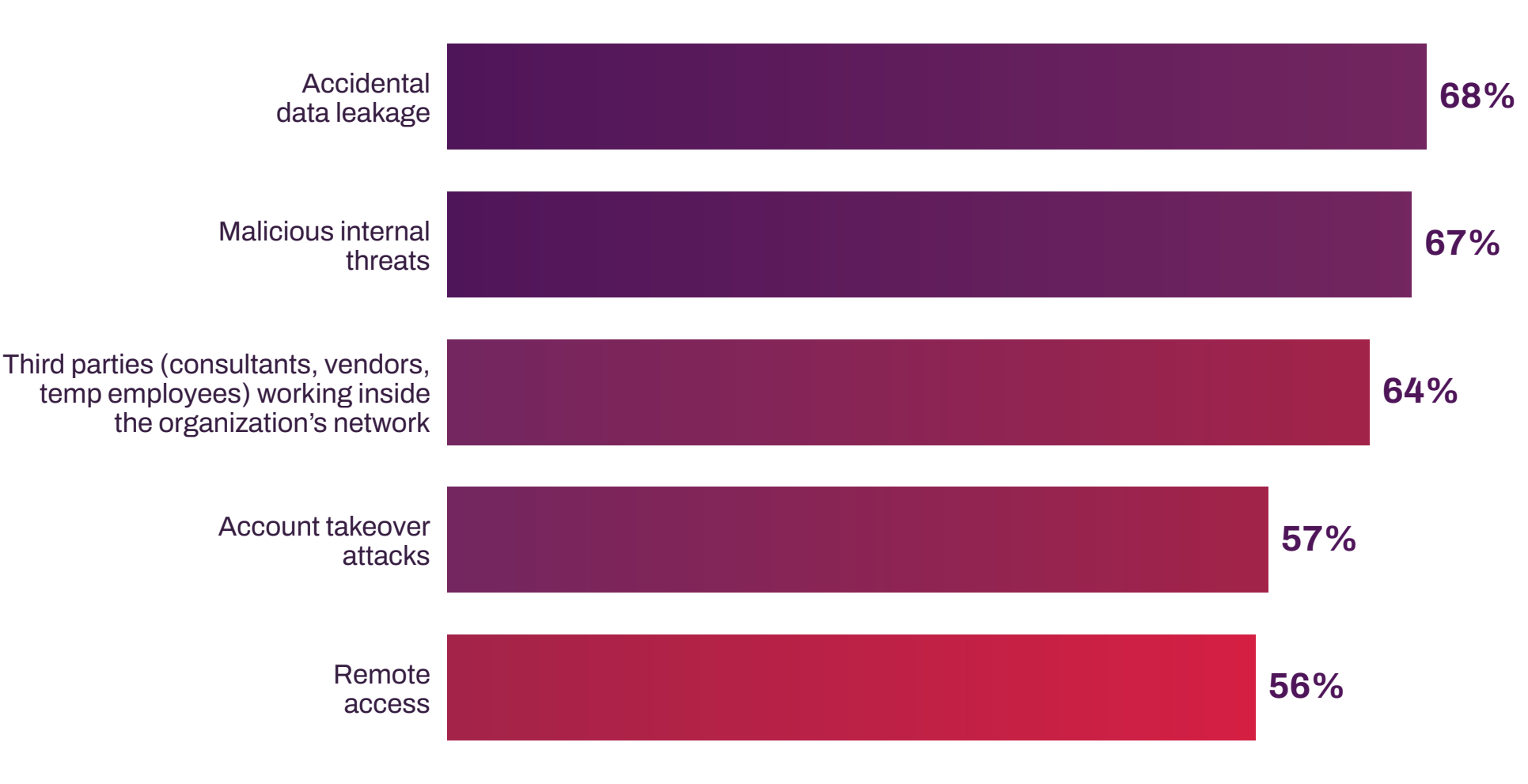
A strong 95% of decision-makers agree that Zero Trust reduces security incidents.

Do you agree a Zero Trust security strategy reduces security incidents?



A Zero Trust security strategy should mostly protect against accidental data leakage (68%), followed by malicious internal threats (68%) and third parties working within the network (64%).

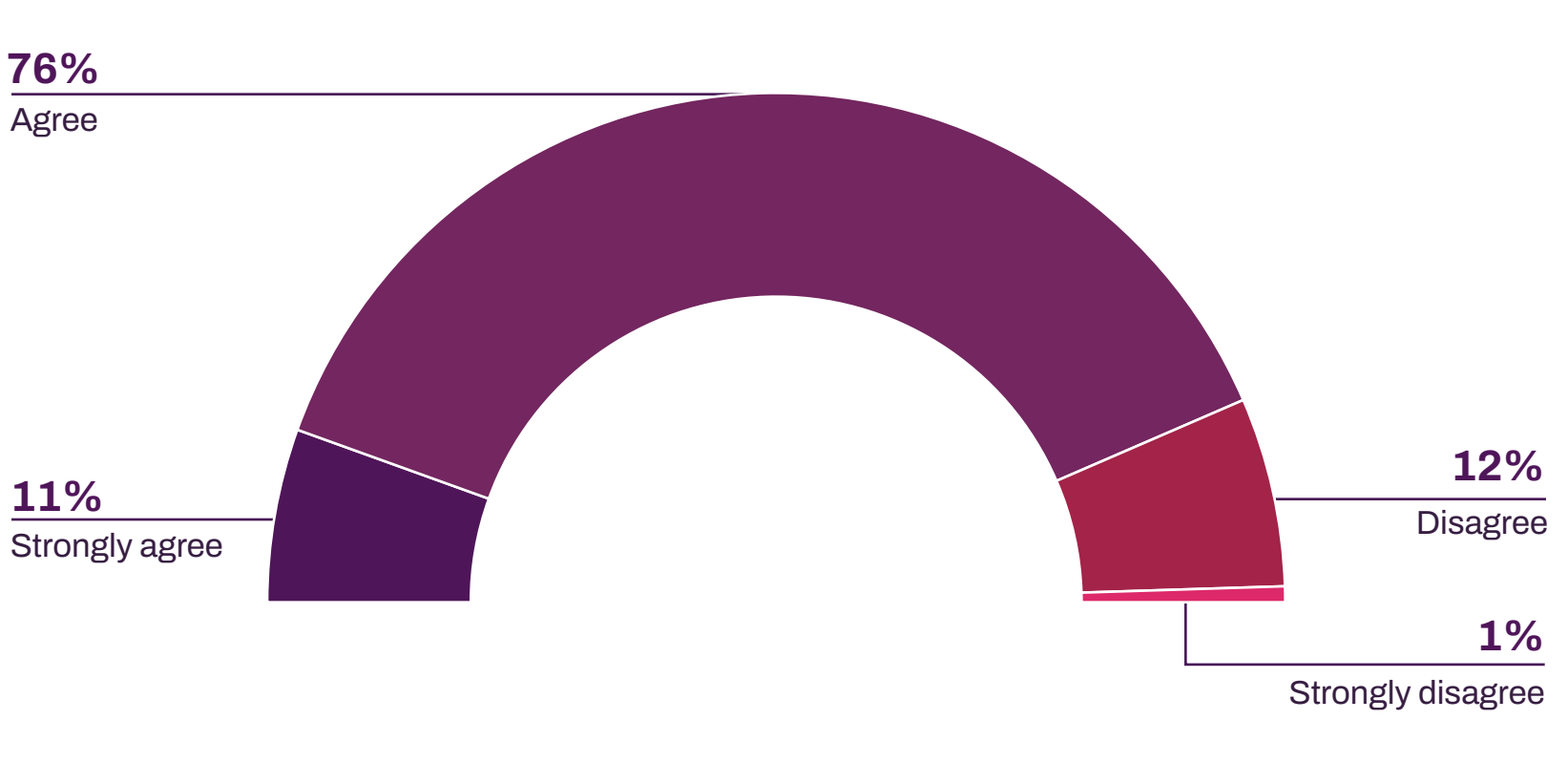
What should a Zero Trust security strategy protect against?



Lateral movement attacks (41%), Public cloud access (40%), Private cloud access (33%), IoT vulnerabilities (26%)

87% of decision-makers believe that a Zero Trust security strategy will also simplify their organization's security architecture.

To what extent do you agree with the following: "I believe that a Zero Trust strategy will simplify my organization's security architecture."

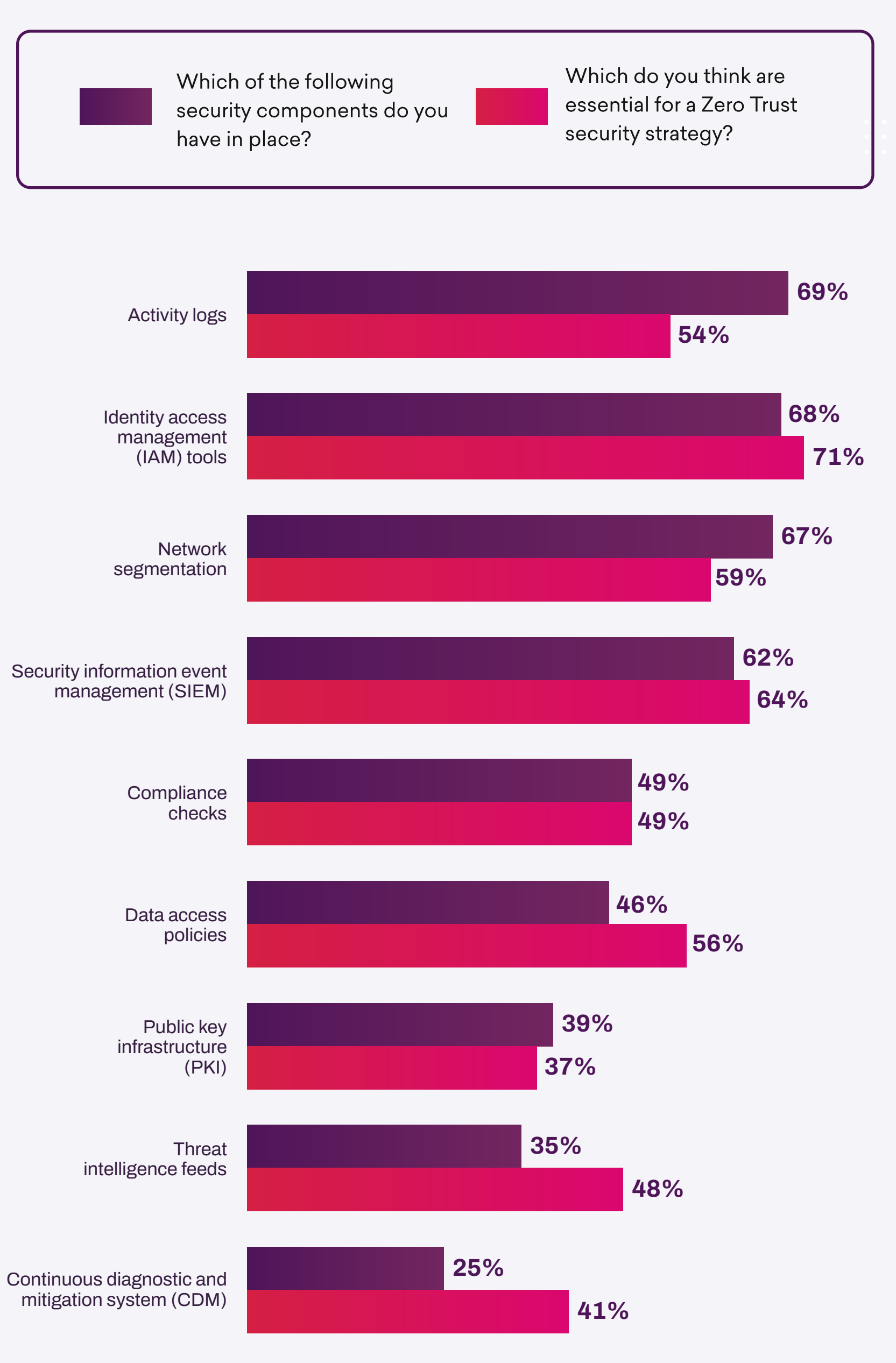


"I'm sold [on Zero Trust], the non-technical [leadership] isn't. Key materials to help win the battle are few and far between."

- Director, small-medium business

Most already have the essential components to a Zero Trust strategy within their security stack—but costs and skills gaps are challenges to implementation

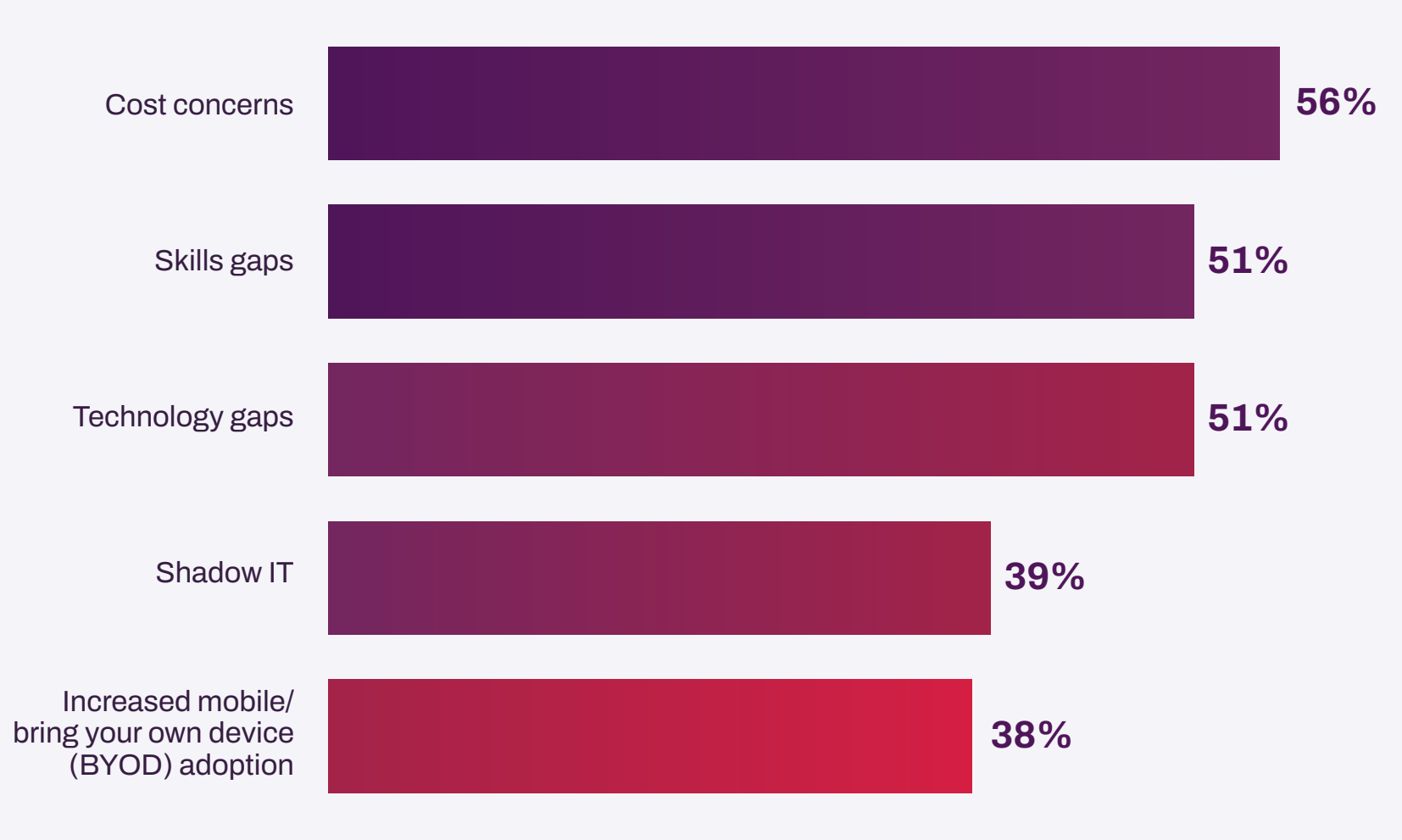
Most decision-makers have the following security components in their security stack: Activity logs (69%), identity and access management (IAM) tools (68%), network segmentation (67%), and security information and event management (SIEM) (62%).



From the same list, decision-makers highlighted IAM tools (71%), SIEM (64%), and network segmentation (59%) as the top essential components of a Zero Trust security strategy, meaning that many already have these components in place.

When it comes to adoption challenges, however, cost concerns ranked highest (56%), followed by skills gaps (51%) and technology gaps (51%).

What are the challenges to adopting a Zero Trust security strategy?



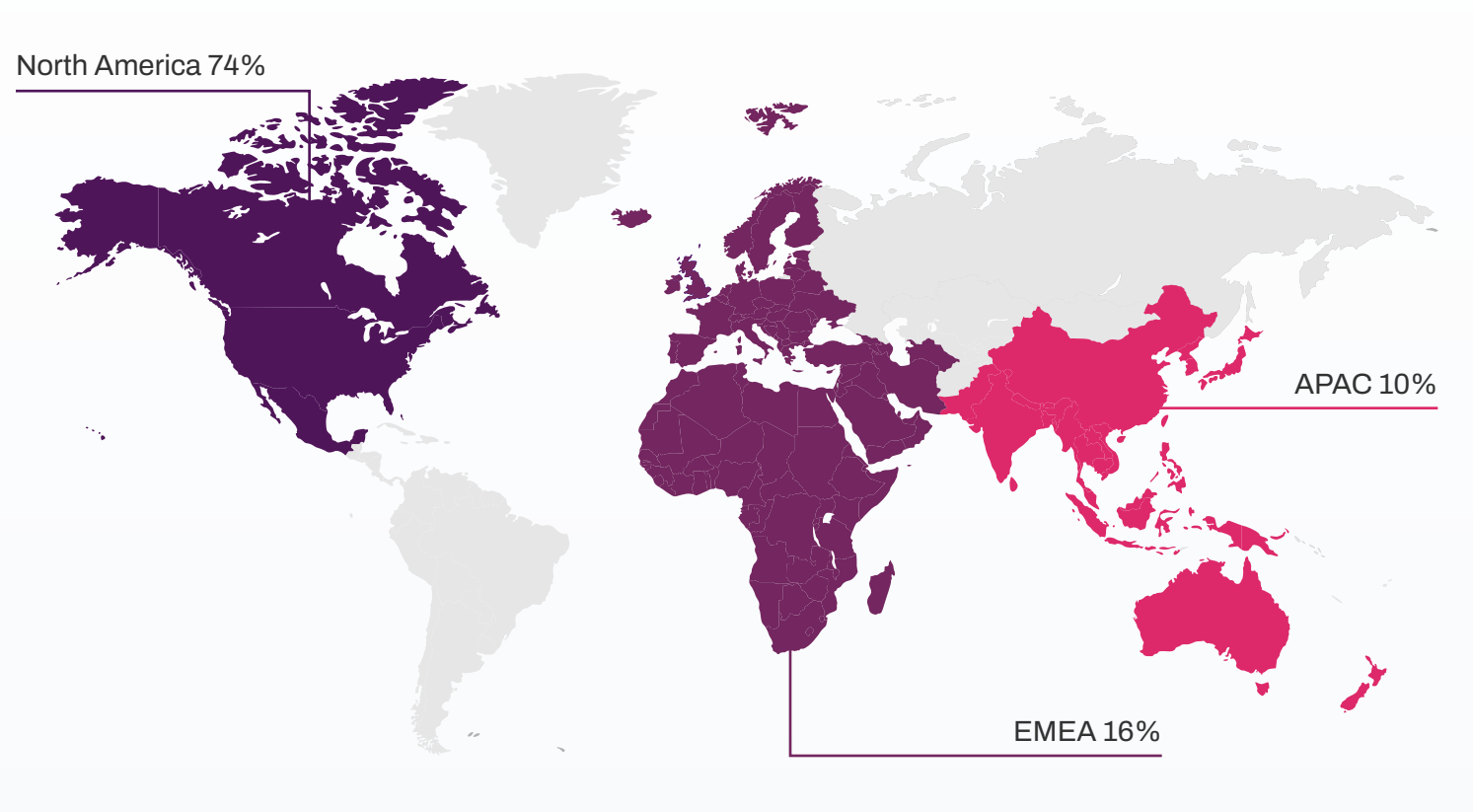
Gaining buy-in from non-technical stakeholders (37%), End-user skepticism (32%), SaaS sprawl (28%), None of these (2%), Other (1%)

"Changing the culture of our organization has been challenging. So many users have had access privileges that they think they need but don't."

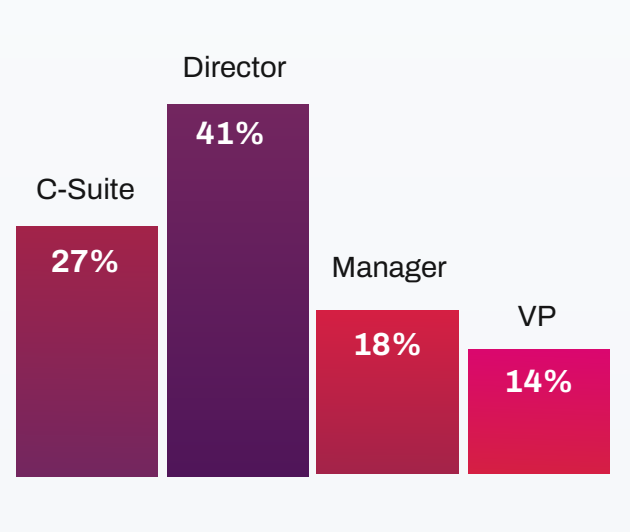
- Director, small-medium business

Respondent Breakdown

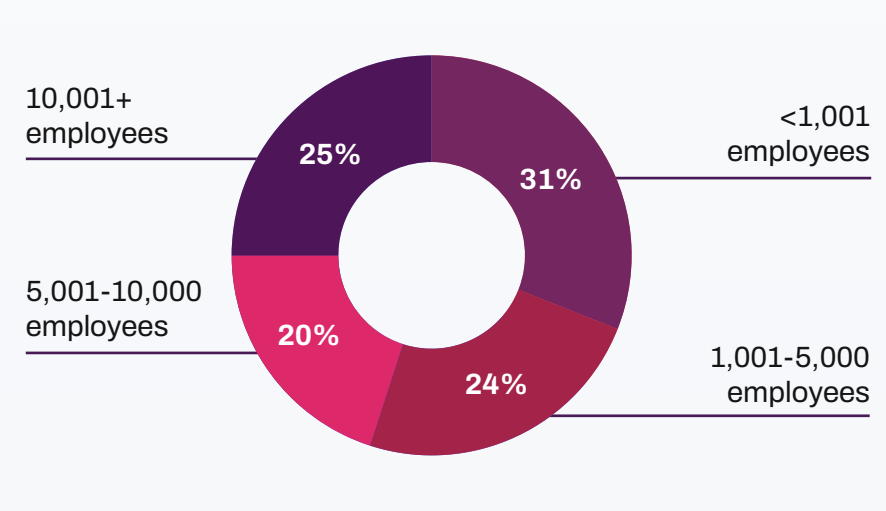
REGION



TITLE



COMPANY SIZE



Insights powered by PULSE