Enterprise Strategy Group™ by TechTarget

Trends in Zero Trust

Strategies and Practices Remain Fragmented, But Many Are Seeing Success

John Grady | Principal Analyst
ENTERPRISE STRATEGY GROUP

DECEMBER 2023

© 2023 TechTarget, Inc. All Rights Reserved.

Research Objectives

The need to modernize cybersecurity strategies to keep pace with IT innovation is clear. Zero-trust architectures have taken the pole position as the best approach to achieve this goal. Unfortunately, the breadth of the initiative and the nuance between zero-trust strategies and the tools supporting these strategies can become lost, causing confusion. IT and security leaders need guidance and proof points from early adopters to avoid false starts and more quickly see positive results.

To assess how businesses are faring with zero-trust initiatives, TechTarget's Enterprise Strategy Group surveyed 379 IT and cybersecurity professionals at organizations in North America (US and Canada) involved with technology and processes supporting zero trust.

This study sought to:

Understand the progression of zero-trust initiatives and how organizations are developing their strategies.

Determine where the most impactful starting points for a zero-trust journey are, and whether progressing further through a zero-trust project impacts effectiveness.

Identify the tools and practices most commonly used to support zero trust.

Validate whether cybersecurity teams can tie benefits such as improving security, simplifying compliance, and reducing costs to their zero-trust strategies.

© 2023 TechTarget, Inc. All Rights Reserved.

KEY FINDINGS

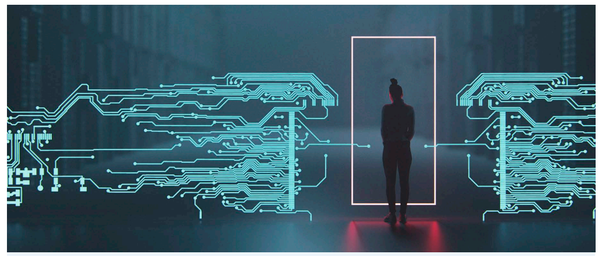
CLICK TO FOLLOW

Security and Zero Trust Are Often Viewed Through the Lens of Modernization

PAGE 4

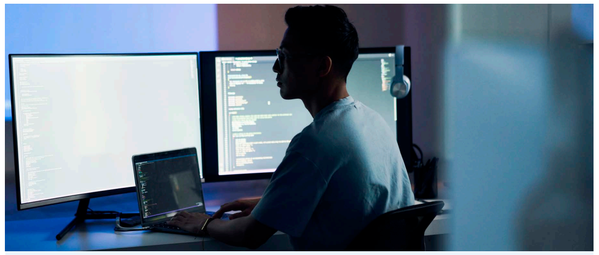
Many Organizations Begin With an Ad Hoc Approach to Zero Trust, But Executive Support Is Critical

PAGE 8



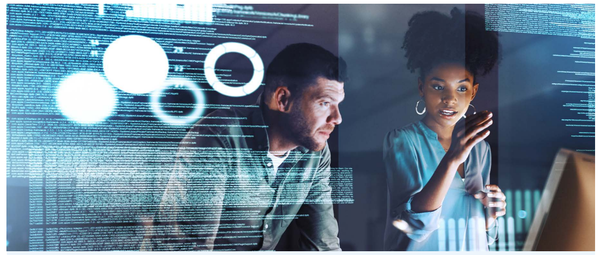
A Variety of Tools Support Zero Trust, But ZTNA Leads in Effectiveness

PAGE 13



Zero-trust Starting Points and Practices Vary, But Risk Assessment and Tracking Progress Are Critical

PAGE 17



Most Organizations Report Success With Zero Trust

PAGE 21

Research Methodology and Demographics

PAGE 26

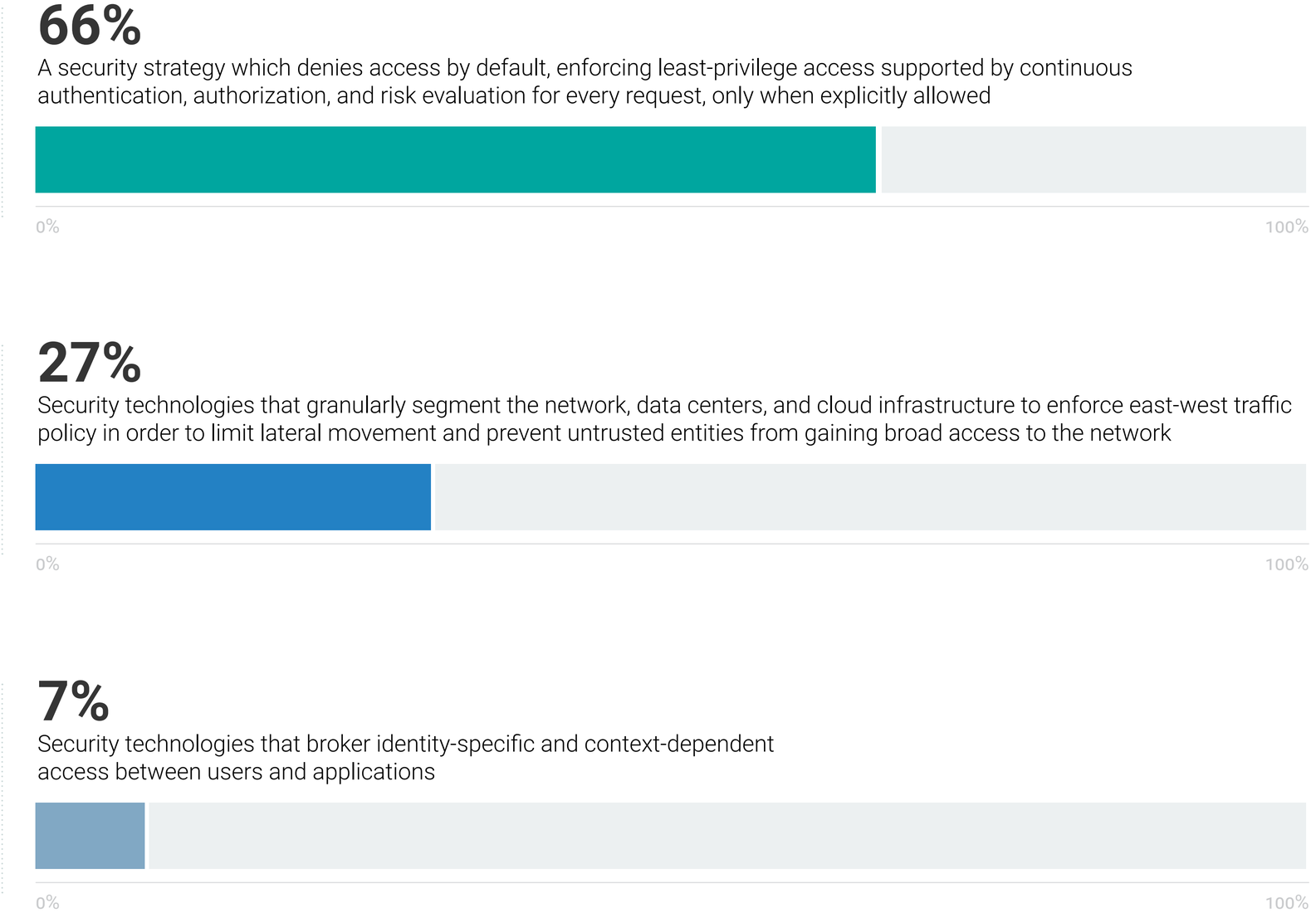
© 2023 TechTarget, Inc. All Rights Reserved.

Security and Zero Trust Are Often Viewed Through the Lens of Modernization

Agreement Is Growing that Zero Trust Is a Strategy

Historically, one of the main points of confusion around zero trust has been how to define it. While the market has reached general agreement on high-level tenets such as “never trust, always verify,” “employ least-privilege access,” and “assume breach,” the heavy focus on zero trust from product vendors has resulted in many practitioners conflating strategy with technology. Yet in a positive sign, respondents are in strong agreement that zero trust is a security strategy, with 66% saying that definition most closely aligns with that of their organization. In the aggregate, roughly one-third (34%) pointed to technology-centric definitions, meaning there is still work to do to align the industry on a strategy-based definition.

Statement most closely aligned with organization’s zero-trust definition.



© 2023 TechTarget, Inc. All Rights Reserved.

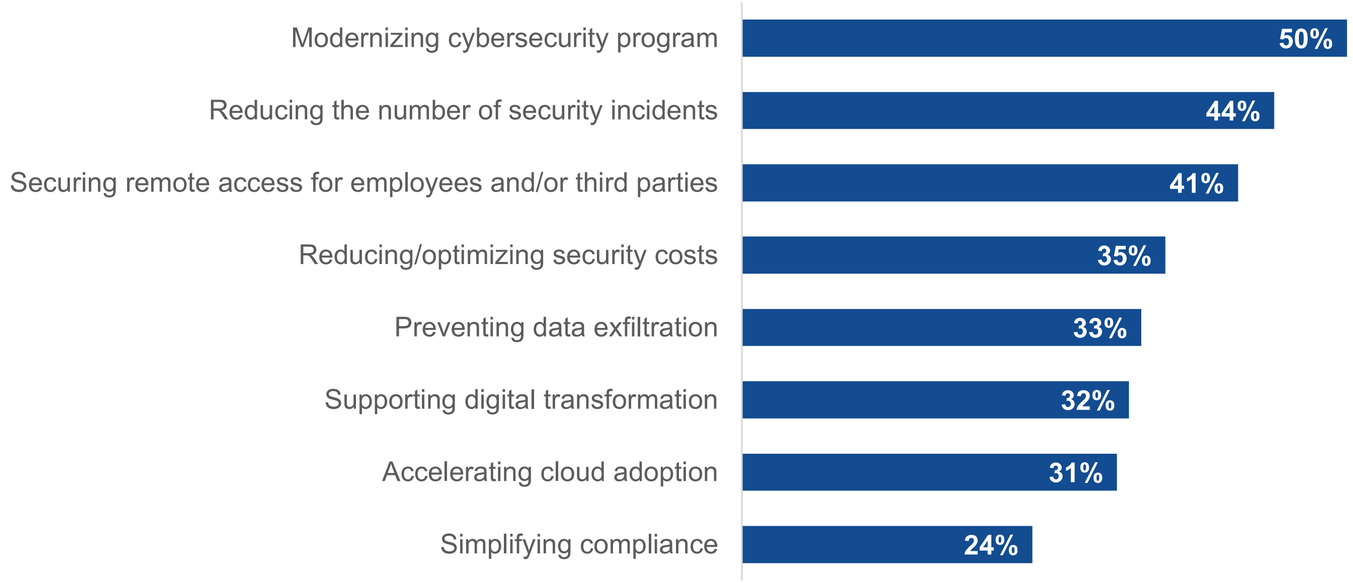
BACK TO CONTENTS

Security Modernization Remains a Key Driver of Zero Trust

When asked what drives their organization's overall cybersecurity spending the most, 47% of respondents said keeping pace with evolving or modernizing IT environments, compared with 30% who pointed to an expanding threat landscape and 24% who said maintaining compliance. This aligns with the drivers for zero-trust adoption as well, with half of respondents (50%) citing cybersecurity program modernization as a top reason for adoption or consideration of zero trust. This is not to say that improving security outcomes is not important, as 44% cited the reduction of security incidents as a driver and 41% pointed to securing remote access for employees and/or third parties. But many view zero trust as an avenue to elevate cybersecurity to better address the realities of modern enterprise architectures.

Biggest macro driver of cybersecurity spending.

Top adoption drivers for zero trust.

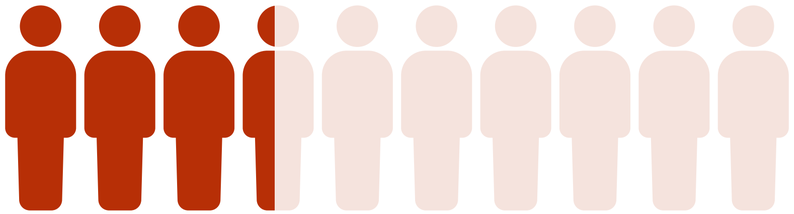


© 2023 TechTarget, Inc. All Rights Reserved.

BACK TO CONTENTS

False Starts With Zero Trust Are Common for a Variety of Reasons

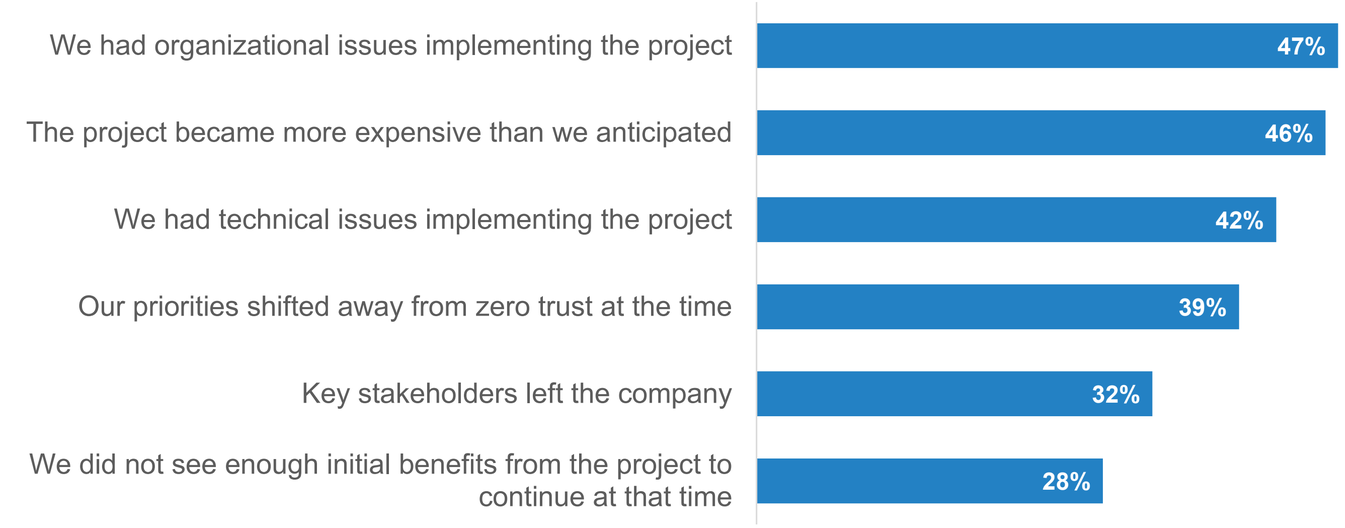
As noted, many are moving forward with zero trust. Among respondents, 69% said they had implemented or were in the process of implementing zero trust across the organization, while 26% were implementing zero trust for specific use cases. At the same time, 34% indicated they had either paused or abandoned a zero-trust project in the past. Organizations identified a variety of reasons for this, ranging from organizational issues (47%) to cost (46%) and technical issues (42%). The likelihood of these false starts among organizations that are currently implementing zero trust points to the need for a well-defined, top-down strategy for zero trust to ensure all stakeholders are on the same page and aligned to the same goals.



Has your organization had to **pause or abandon a zero-trust project** at any point in the past?

34% **SAY YES**

Reasons for pausing or abandoning a zero-trust project.



© 2023 TechTarget, Inc. All Rights Reserved.

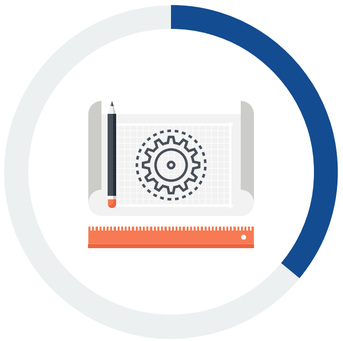
BACK TO CONTENTS

Many Organizations Begin With an Ad Hoc Approach to Zero Trust, But Executive Support Is Critical

Most Begin With a Use Case-based or Ad Hoc Approach to Zero Trust

There are a variety of ways to approach a zero-trust initiative. Among respondent organizations, a majority began with specific use cases or ad hoc implementations. Nearly half (47%) solved for a specific use case prior to having a broader strategy and expanded from there over time, while 11% solved for a specific use case but have not expanded. Just more than one-third (36%) indicated that leadership developed a plan that was implemented over multiple years.

Historical approach to zero trust.

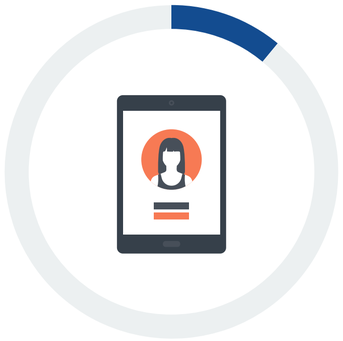


36%

Our leadership developed a plan for zero trust that we implemented/plan to implement over multiple years

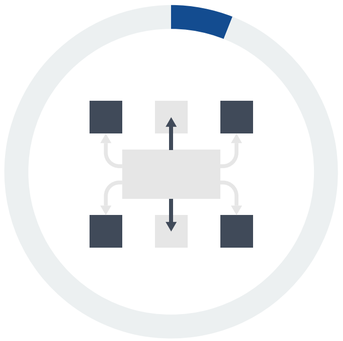
47%

In solving for a specific use case, we began to implement zero trust prior to having a broader strategy and have expanded overtime



11%

We solved for a specific use case through zero trust but have not expanded the strategy



6%

Tools that support zero trust were independently purchased, and over time we built a zero-trust strategy around those tools

An additional 1% said that implementing zero trust is up to individual product owners and teams.

© 2023 TechTarget, Inc. All Rights Reserved.

BACK TO CONTENTS

> “Only 36% say one of the most important factors for a successful implementation **is starting small and expanding over time.”**

John Grady | Principal Analyst
ENTERPRISE STRATEGY GROUP

While Many Have Started Small, a Clear, Executive-led Strategy Is Critical

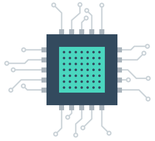
Interestingly, despite the fact that many organizations begin with a use case-based or ad hoc approach to zero trust, only 36% say one of the most important factors for a successful implementation is starting small and expanding over time. Conversely, nearly half (47%) point to having executive support outside of IT and security, emphasizing the need to align to the business, and 47% cited having a multi-year plan and roadmap and staying the course. Remaining flexible (44%), selecting the right technology vendors (40%), and working with service providers (38%) were all prominently mentioned, but clearly a well-defined, centralized plan is an important component for any zero-trust initiative.

Most important factors for zero-trust success.

47%
Having executive support outside of IT and security

47%
Having a clear multi-year plan and roadmap and staying the course

44%
Remaining flexible and adjusting as needed



40%
Selecting the right technology vendors to work with to support the initiative

38%
Working with service providers

36%
Starting small and expanding over time

© 2023 TechTarget, Inc. All Rights Reserved.

BACK TO CONTENTS

Security Teams See Value in Federal Resources for Zero Trust

At this point, there's no shortage of information on zero trust, and security teams leverage a variety of sources for guidance. The most commonly cited source of zero-trust information was the CISA Zero Trust Maturity Model. The zero-trust reference architecture from NIST Special Publication 800-207 was also called out frequently, cited by 42% of respondents. Vendor information still plays a large role as well. Nearly half (46%) of respondents said specific advice given to their organization by technology vendors was influential, while 39% pointed to vendor reference architectures and/or maturity models. Finally, service providers continue to play a significant role as well, with 47% saying paid engagements for consulting or the implementation of a zero-trust strategy were influential.

Top five most influential information sources for zero trust.

1.

67%
Cybersecurity & Infrastructure Security Agency (CISA) Zero Trust Maturity Model

2.

47%
Paid engagement with service providers for consulting/implementation of zero-trust strategy

3.

46%
Advice/guidance from technology vendors given specifically to our organization

4.

42%
National Institute of Standards and Technology (NIST) Special Publication 800-207

5.

39%
Vendor reference architectures and/or maturity models that are publicly available

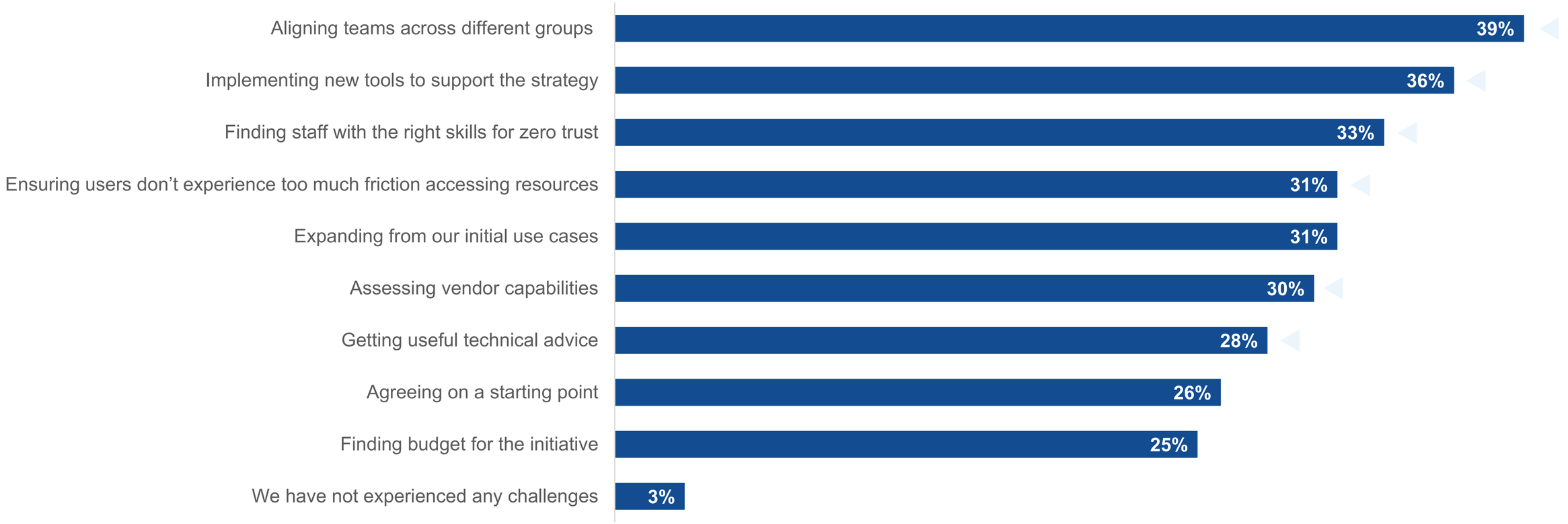
© 2023 TechTarget, Inc. All Rights Reserved.

BACK TO CONTENTS

Organizational Issues Remain Top of Mind

While proper planning can certainly help foster successful zero-trust efforts, challenges are inevitable. Overall, only 3% of respondents said they had not experienced challenges with zero trust. While a variety of challenges were cited, organizational and personnel issues were at the top of the list. Specifically, 39% said aligning teams across different groups was an issue, while 33% noted difficulty in finding staff with the right skills for zero trust. From a technology perspective, implementing tools (36%), assessing vendor capabilities (30%), and getting useful technical advice (28%) were all commonly cited. Finally, maintaining the balance between security and user experience clearly remains an issue for some, with 31% noting that preventing friction when users access resources is a challenge.

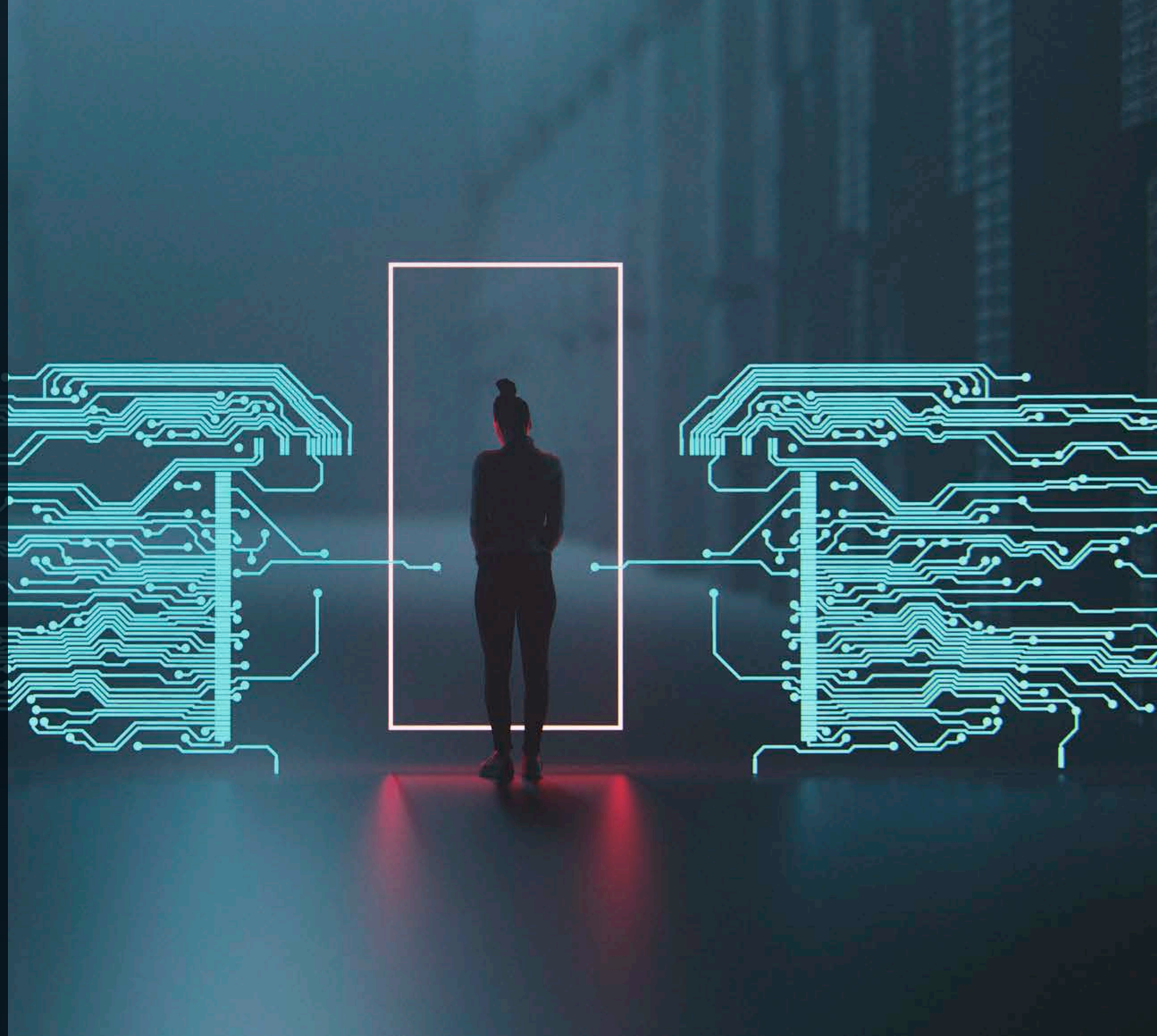
Greatest zero-trust challenges.



© 2023 TechTarget, Inc. All Rights Reserved.

BACK TO CONTENTS

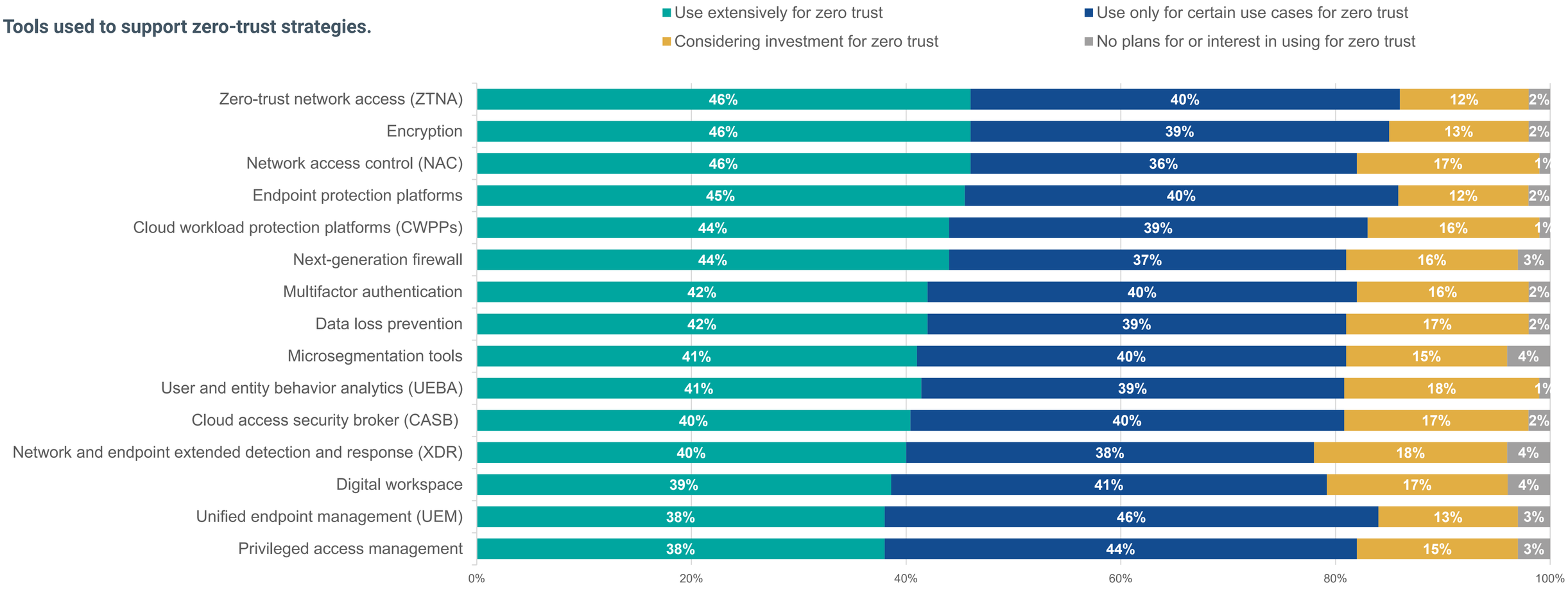
A Variety of Tools Support Zero Trust, But ZTNA Leads in Effectiveness



A Variety of Tools Can Support Zero Trust

The breadth of zero trust necessitates a wide range of enabling technologies when these initiatives are broadly implemented. This was borne out among respondent organizations, with at least 78% reporting using each tool either extensively or for certain use cases for zero trust. Clearly, as zero trust has extended from users and networks to data and workloads, tools such as encryption, data loss prevention, and cloud workload protection platforms have gained mindshare. Similarly, the need to include response as part of a zero-trust architecture has paved the way for XDR to be considered as a supporting technology for the initiative.

Tools used to support zero-trust strategies.



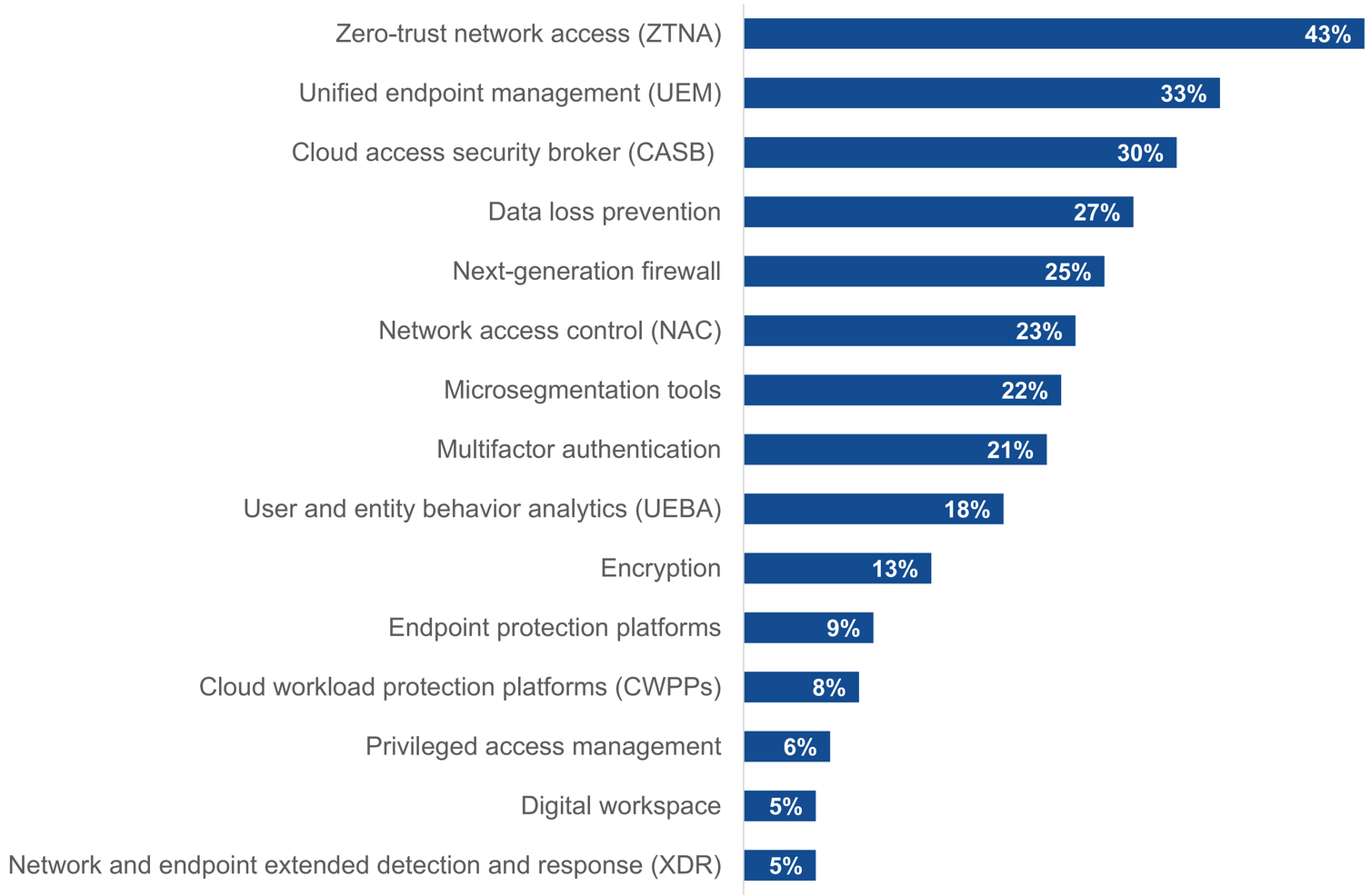
© 2023 TechTarget, Inc. All Rights Reserved.

BACK TO CONTENTS

Zero-trust Network Access (ZTNA) Currently Rated Most Effective

While many tools are used to support zero-trust initiatives, there is more differentiation as to which technologies are most effective. ZTNA is at the top of the list of most effective tools, but by a wider margin than in the list of all tools used to support zero trust, with 43% of respondents selecting it as the most effective at enabling a zero-trust strategy. UEM (33%) and CASB (30%) were also rated highly. But despite the expansion of zero trust to include applications and response, few respondents selected CWPP (8%) or XDR (5%) as one of the most effective zero-trust tools. This is likely to change over time as initiatives expand and more advanced use cases come into play.

Most effective tools for enabling zero-trust strategies.



© 2023 TechTarget, Inc. All Rights Reserved.

BACK TO CONTENTS

AI, Coverage, and Ecosystems Are Most Important

Over the last year, it has become an expectation that AI is a part of any cybersecurity solution. As such, it follows that 40% of organizations cited AI/ML as one of the most important attributes of tools supporting zero trust. This could take many forms, like threat detection, management automation, and large language models (LLMs), but practitioners should closely examine vendor AI claims before believing the hype. Separately, because zero trust seeks to remove the concept of location from access decisions, consistent coverage across both cloud and on-premises environments is also viewed as vital, as was noted by 40% of respondents. Similarly, because of the range of tools organizations are interested in to support zero trust, vendor ecosystems with prebuilt integrations are becoming important. This was cited by 39% of respondents. Finally, one of the most important aspects of zero trust is basing decisions on risk. Along these lines, 36% pointed to risk assessment capabilities as an important attribute.

Most important attributes for tools supporting zero trust.

40%
Artificial intelligence/ machine learning

40%
Consistent coverage for cloud and on-premises environments

39%
Part of an ecosystem with integrations among different vendors

36%
Risk assessment capabilities

33%
Part of a broader platform from a single vendor

32%
Automation of policy creation/management

31%
Ease of deployment

26%
Anomaly detection

© 2023 TechTarget, Inc. All Rights Reserved.

BACK TO CONTENTS

Zero-trust Starting Points and Practices Vary, But Risk Assessment and Tracking Progress Are Critical

> Zero-trust strategies are typically oriented around five pillars: **users/identity, networks, data, devices, and applications/workloads.”**

No Consensus on Zero-trust Starting Points

Zero-trust strategies are typically oriented around five pillars: users/identity, networks, data, devices, and applications/workloads. There was little variation between where respondents began their zero-trust journey. Networks (23%) were slightly ahead of data (21%), but devices (19%), users/identity (19%), and applications/workloads (18%) were close behind. When asked where their organization would begin the process if they knew what they know now, networks and devices became less popular options, with data, users/identity, and applications/workloads rising in prominence. That said, the changes were fairly small, showing limited consensus on where to start with zero trust.

Initial focus for zero trust.

© 2023 TechTarget, Inc. All Rights Reserved.

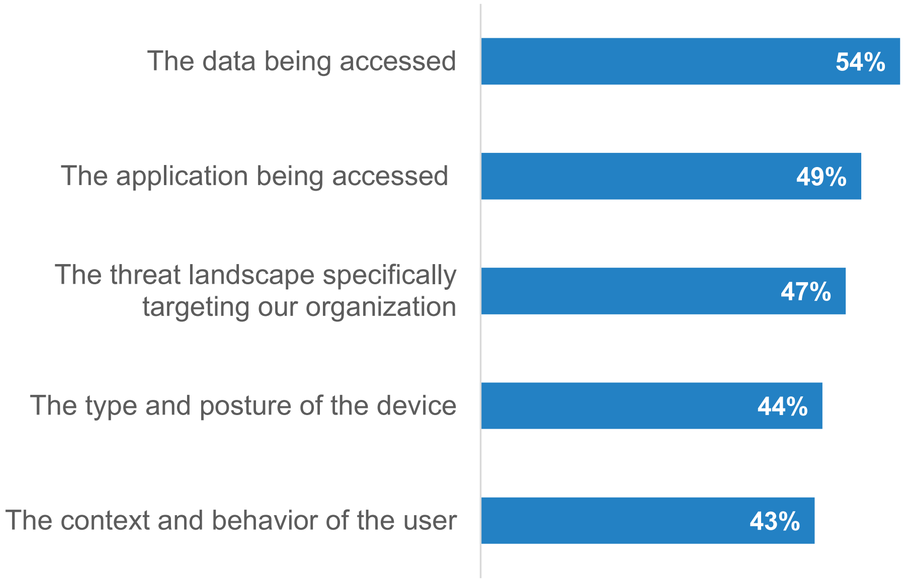
BACK TO CONTENTS

Most Assess Risk and Use a Variety of Inputs, But Work Remains

Assessing risk and basing allow/block decisions on that factor is an integral component of zero trust. Most respondents appear to agree with that sentiment, as only 13% said they make no determinations for risk when applying policy. By the same token, less than one-third (30%) indicated they assess risk in real time and continually with fully dynamic policies. The remainder assess risk manually or with some level of automation but not in real time or continually. On average, respondents who perform risk assessments indicated their organization uses 2.3 risk inputs. Data was cited most commonly (54%) as an input, but all inputs had at least 43% agreement. While this is positive, it shows there is room for improvement as data, applications, the threat landscape, device type and posture, and user context and behavior are all critical inputs for risk assessment.

Risk assessment for zero trust.

Risk inputs used for zero trust.



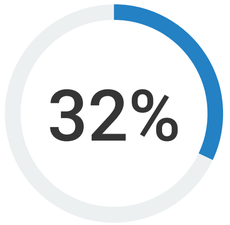
© 2023 TechTarget, Inc. All Rights Reserved.

BACK TO CONTENTS

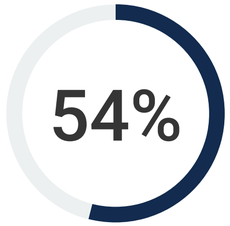
Nearly All Track Specific Zero-trust Metrics to Gauge Progress

Nearly all respondents (98%) report they have identified specific metrics around zero trust to help track progress. However, there is variation in the frequency of assessment. More than half of organizations (54%) report and assess progress at least quarterly. Only 12% indicated they do so at least annually, leaving just under one-third (32%) who report and assess at least monthly. As noted earlier, flexibility and the ability to respond to changes was cited as an important component of success, making regular assessment critical to informed decision-making.

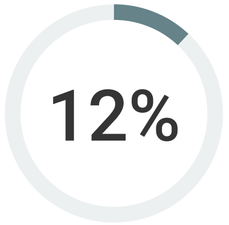
How zero-trust progress is tracked.



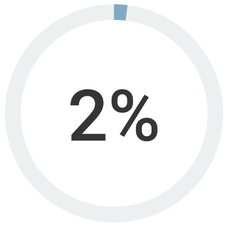
We have identified specific metrics around zero trust that are reported on and assessed at least **monthly**



We have identified specific metrics around zero trust that are reported on and assessed at least **quarterly**



We have identified specific metrics around zero trust that are reported on and assessed at least **annually**



We measure the progress of zero trust through the overall success of our cybersecurity program

98%

report they have identified specific metrics around zero trust to help track progress.

© 2023 TechTarget, Inc. All Rights Reserved.

BACK TO CONTENTS

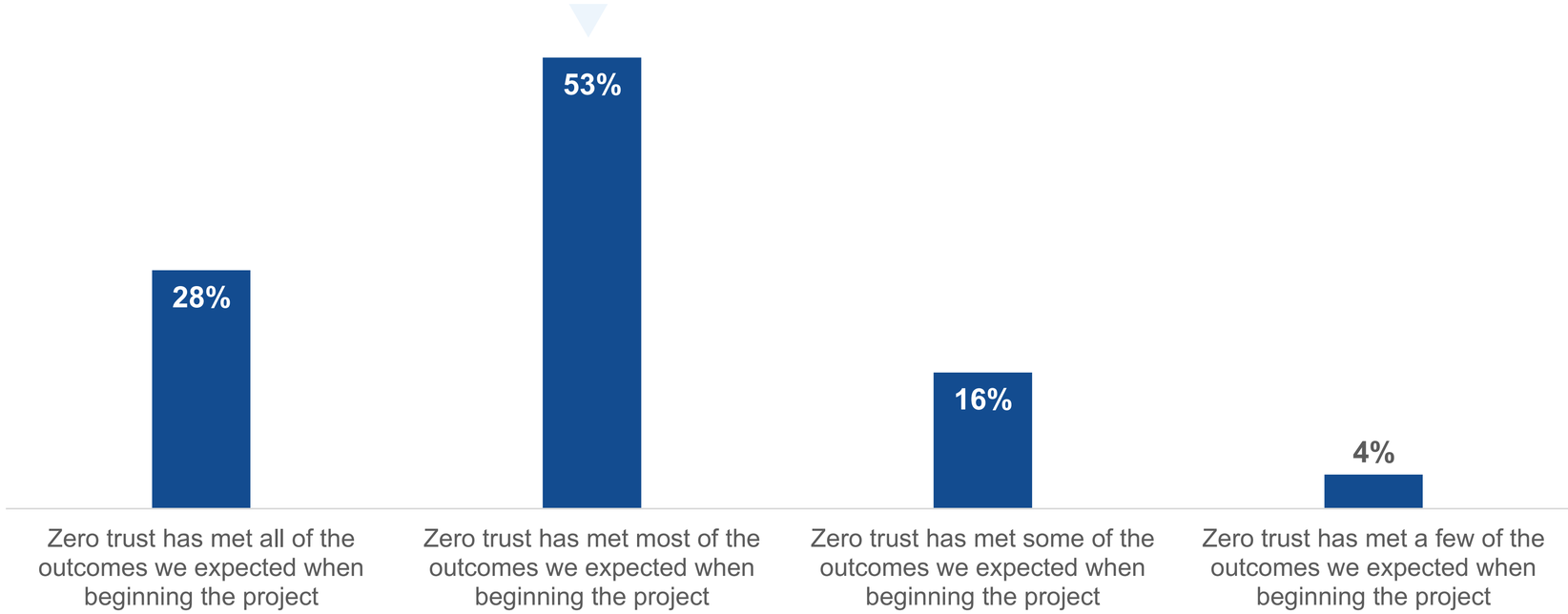
Most Organizations Report Success With Zero Trust

> More than half say their zero-trust initiative **has met most of the outcomes they anticipated** at the beginning of the project."

Zero-trust Outcomes Have Typically Aligned with Expectations

With regard to outcomes, respondents report good progress. More than half (53%) say their zero-trust initiative has met most of the outcomes they anticipated at the beginning of the project. More than one-quarter (28%) say their initiative has met all their expected outcomes. Only 20% noted that zero trust had only met some or a few of the outcomes they expected. So, while work remains for many to see broader success, a number report they are on the right track.

How zero trust has met expectations.



© 2023 TechTarget, Inc. All Rights Reserved.

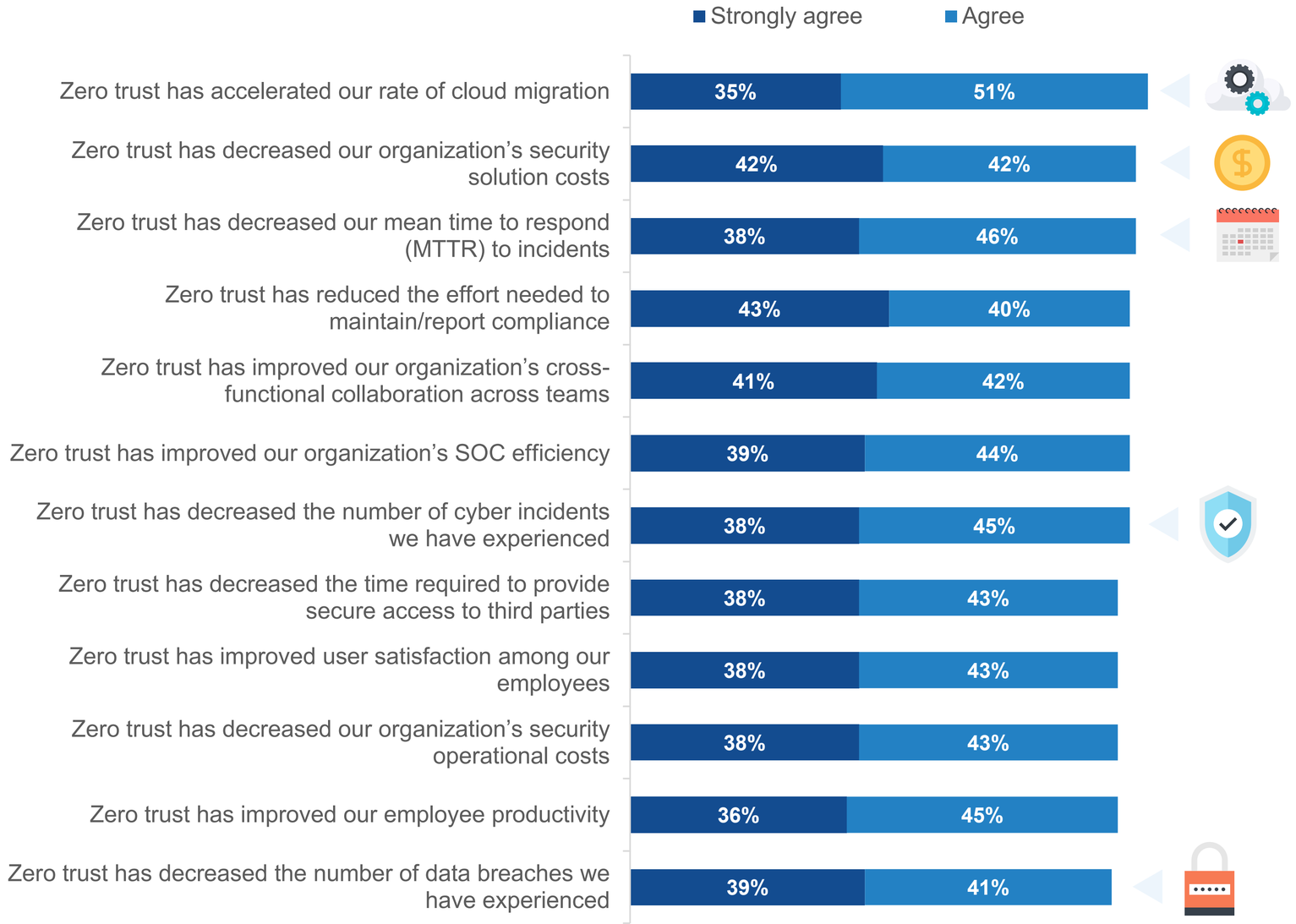
BACK TO CONTENTS

Zero Trust Leads to Fewer Breaches, Cost Savings, and Faster Cloud Migration

More specifically, respondents were in strong agreement that zero trust had produced positive outcomes across both security and business metrics. At least 80% agreed that zero trust had led to each positive outcome listed, with at least 35% strongly agreeing. In particular, respondents noted that zero trust helped, **on average:**

- **Reduce security costs by $675,000.**
- **Reduce the number of cyber incidents by 32%.**
- **Reduce data breaches by 34%.**
- **Reduce their mean time to respond (MTTR) by 10 days.**
- **Improve their rate of cloud migration by 33%.**

Agreement with zero-trust outcomes.



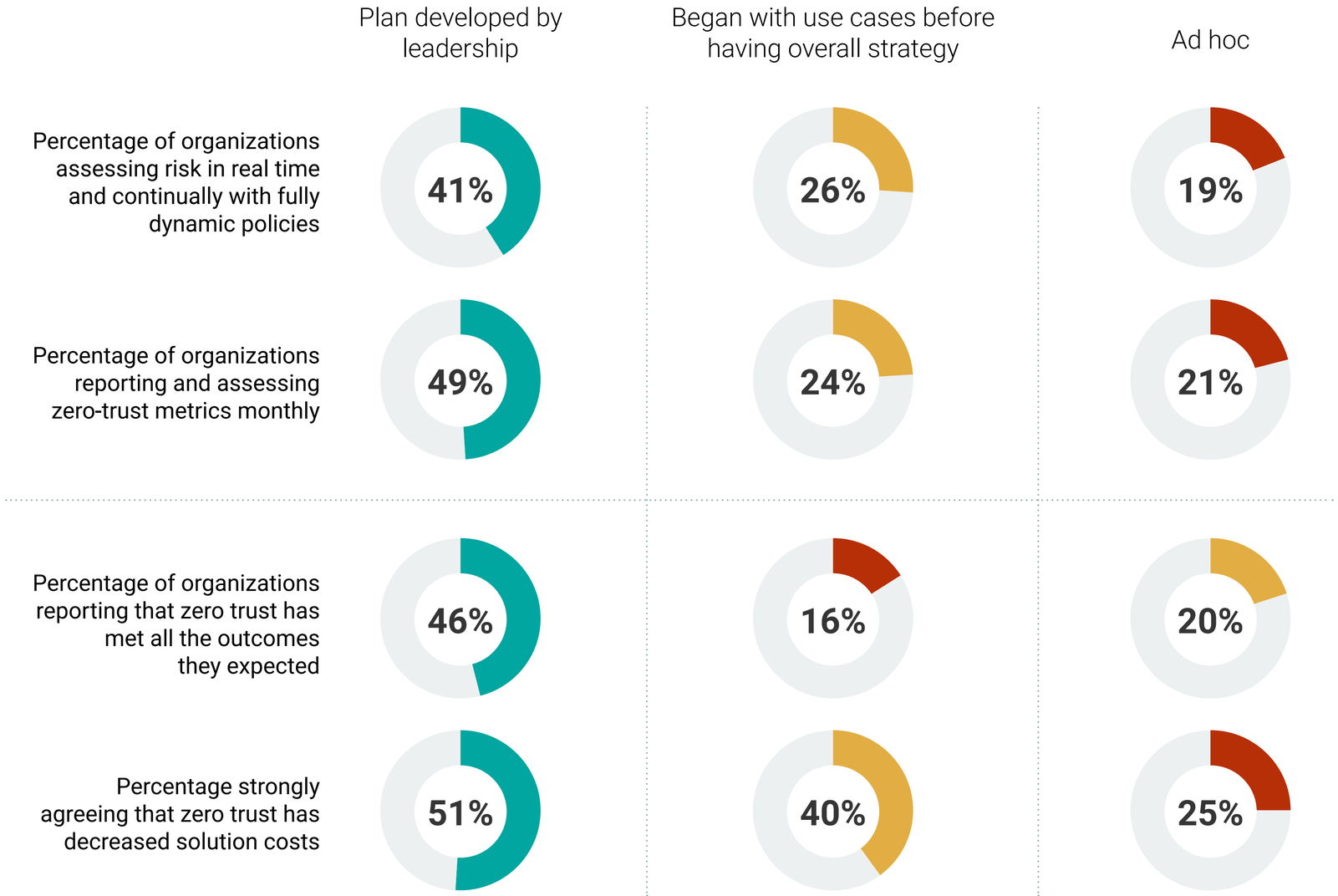
© 2023 TechTarget, Inc. All Rights Reserved.

BACK TO CONTENTS

Developing an Overarching Strategy Seems to Point to Maturity and Ultimately Pay More Dividends

What should security and IT leaders take away from these findings? First, zero trust is incredibly broad, and there is no definitively correct starting point. Where to begin will depend on the goals of the project, existing core competencies, the areas of greatest need, and more. That said, there was a connection between the upfront development of an overall strategy, maturity, and positive outcomes. Those organizations that reported their leadership developed a plan for zero trust that was implemented over multiple years were much more likely to assess risk in real time and continually with fully dynamic policies and report and assess zero-trust metrics monthly. Perhaps consequently, these organizations were then more likely to say that zero trust had met all the outcomes they expected and that zero trust had decreased solution costs. So, while practices may vary, proper planning is important for zero-trust success.

Process followed for zero-trust implementation.



© 2023 TechTarget, Inc. All Rights Reserved.

BACK TO CONTENTS

portnox™

The Portnox Cloud delivers cloud-native zero trust access control and cybersecurity essentials that enable agile, resource-constrained IT teams to proactively address today's most pressing security challenges: the rapid expansion of perimeter-less enterprise networks, the proliferation of connected device types, the increased sophistication of cyberattacks, and the shift to zero trust.

Learn More

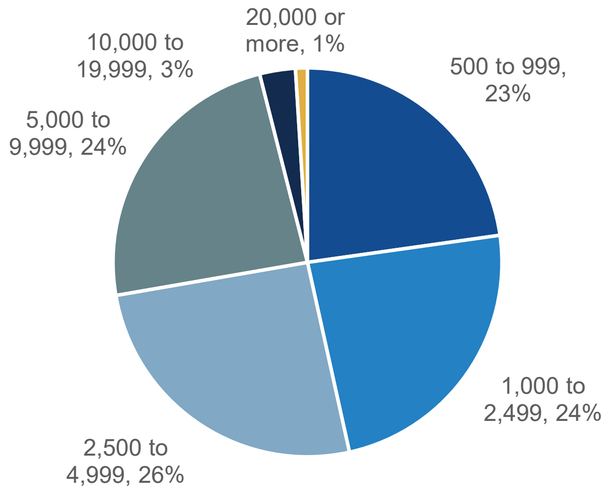
© 2023 TechTarget, Inc. All Rights Reserved.

Research Methodology and Demographics

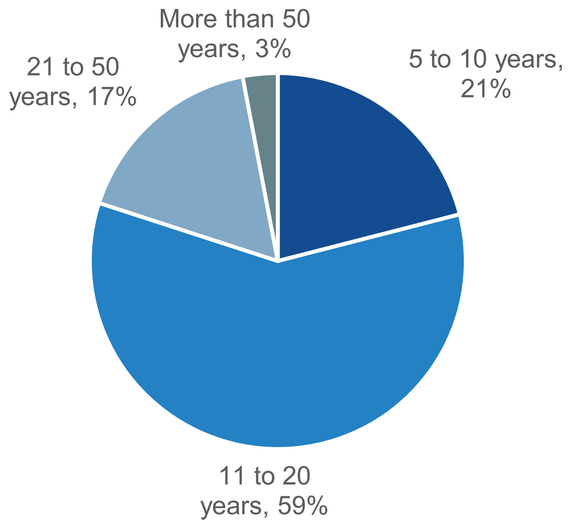
To gather data for this report, TechTarget's Enterprise Strategy Group conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America between September 26, 2023 and October 11, 2023. To qualify for this survey, respondents were required to be involved with technology and processes supporting zero trust. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 379 IT and cybersecurity professionals.

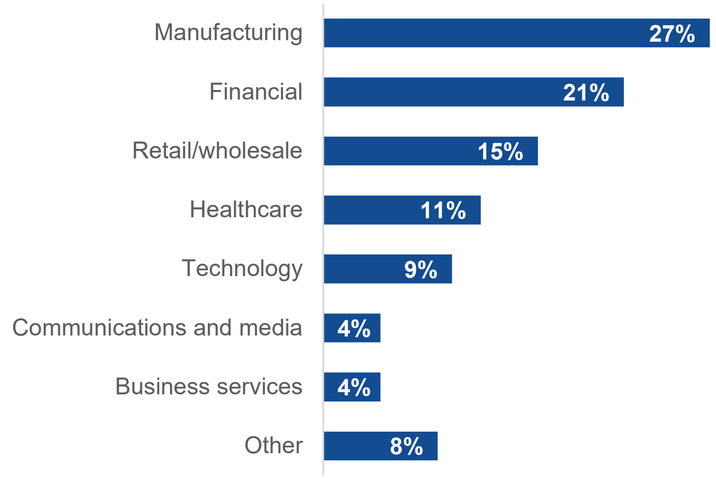
RESPONDENTS BY NUMBER OF EMPLOYEES.



RESPONDENTS BY AGE OF COMPANY.



RESPONDENTS BY INDUSTRY.



© 2023 TechTarget, Inc. All Rights Reserved.

BACK TO CONTENTS

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

© 2023 TechTarget, Inc. All Rights Reserved.