RESEARCH HIGHLIGHTS

The State of Zero-trust Security Strategies

John Grady, Senior Analyst

FEBRUARY 2021

CONTENTS

Research Objectives

Zero-trust approaches are arguably more relevant than ever due to the increasingly distributed nature of the modern enterprise. Whether implementing least-privilege tenets for user access or securing the connections to and between the disparate aspects of today's hybrid multi-cloud deployments, zero trust can provide a framework to secure even the most complex environments. The sudden shift to work-from-home models has only highlighted the importance of a zero-trust approach. Yet for many organizations, confusion remains as to exactly what a zero-trust initiative should entail, where to begin, and how best to overcome the organizational obstacles that result from such a cross-functional undertaking.

In order to gain insight into these trends, ESG surveyed 421 IT and cybersecurity professionals at organizations in North America (US and Canada) personally responsible for driving zero-trust security strategies and evaluating, purchasing, and managing security technology products and services in support of these initiatives.

THIS STUDY SOUGHT TO:

Understand the trigger points that are influencing zero-trust initiatives and how decision makers are prioritizing and timing purchasing decisions.

Gain insights into the planning, purchasing, and implementation dynamics across different stakeholders within IT and the lines of business.

Examine the results zero-trust strategies have delivered with regards to anticipated outcomes such as improving security, simplifying compliance, and reducing costs.

Determine the extent to which specific technologies and products are being deployed to support zero-trust strategies.

Research Highlights

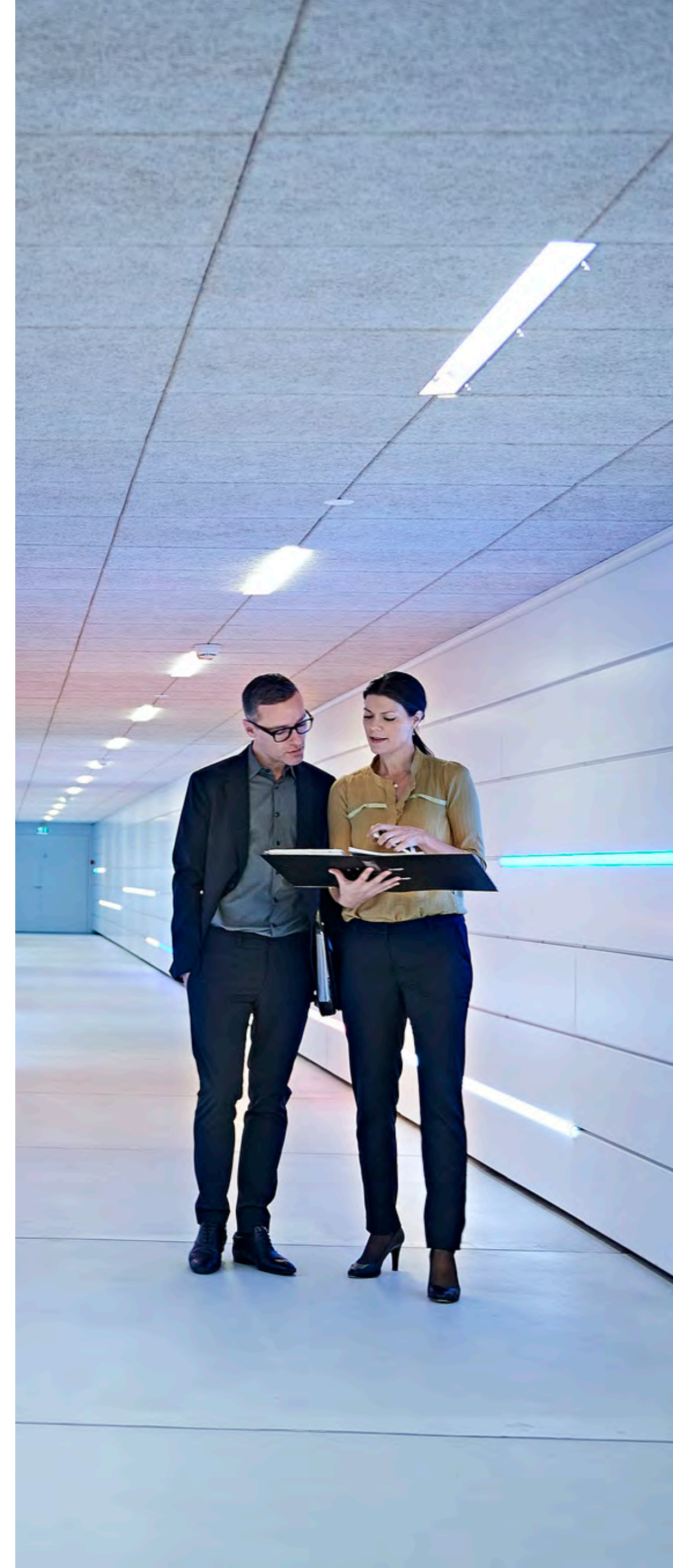**The definitions and drivers of zero trust vary, but many organizations claim multiple security and business benefits.**
Nearly half of organizations rate their zero-trust initiatives as very successful and claim benefits such as reduced security incidents, better SOC efficiency, fewer data breaches, and higher user satisfaction.

The pandemic validates the importance of zero trust.
Most organizations carried on with zero-trust plans even as the pandemic put other initiatives on hold. But further, those with zero-trust projects in place were less likely to see increased security team workloads as a result of the shifting focus to securing remote workers.

Formalized strategies for zero trust are common. However, most organizations begin with a specific use case and "back into" a broader zero-trust Initiative.
Nearly nine out of ten organizations have formalized zero-trust strategies. While it is common for these early movers to begin with a use-case-specific approach or inventory the tools they have in place, many plan to build a broader strategy from those starting points.

The broad range of tools required for zero trust drives interest in a platform approach.
The vast majority of organizations are using or interested in zero-trust platforms. Not surprisingly, integrations are a top consideration when adopting tools in recognition of the fact that a single vendor approach is not feasible.
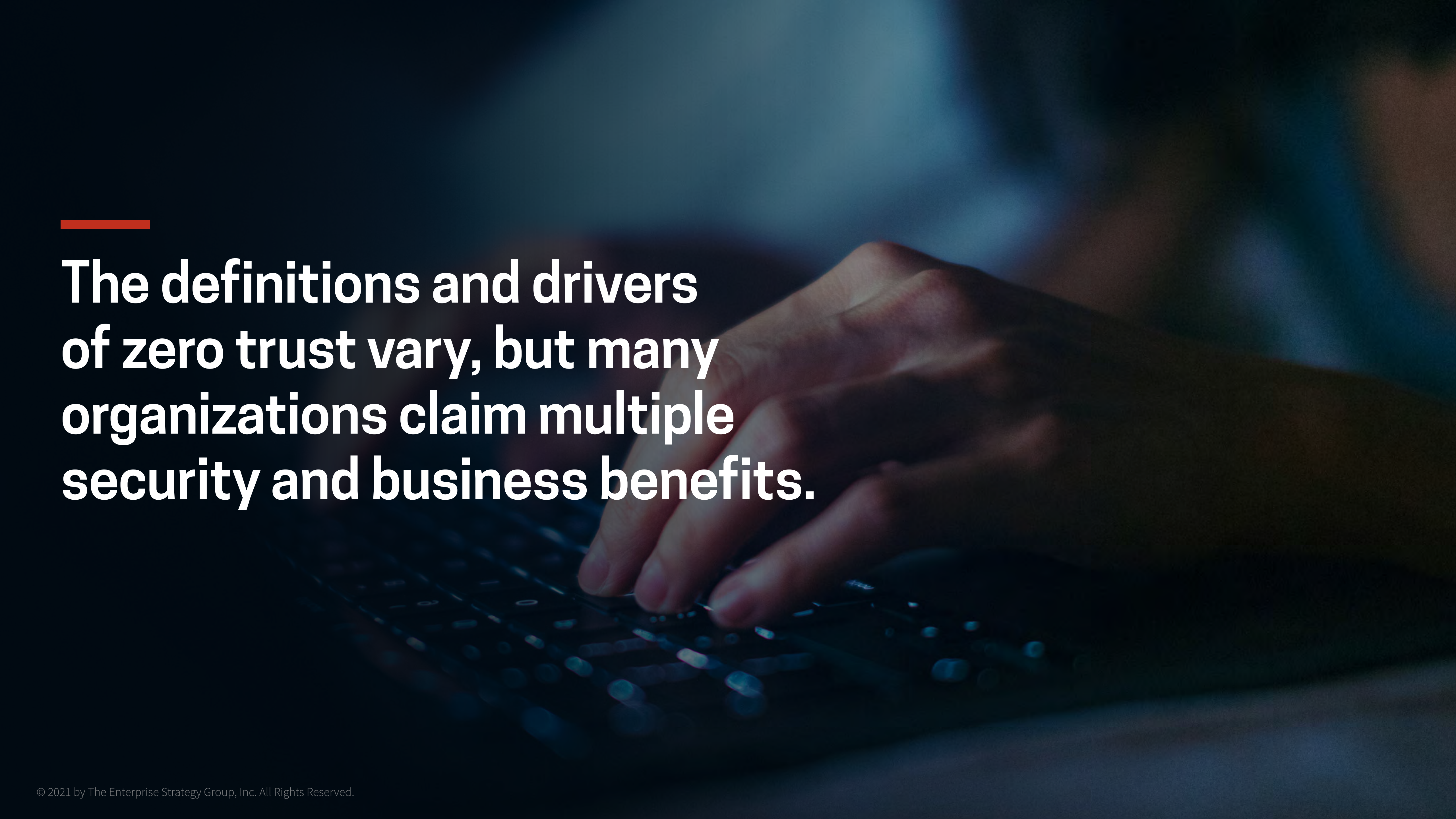
Cross-functional collaboration is critical to zero-trust success and is leading to interest in centers of excellence.
There are currently many individuals and groups involved with zero-trust strategies. And while only 12% of organizations have implemented a zero-trust center of excellence (CoE) to date, interest is very high in this approach to formalize the collaboration across the different groups involved in zero trust.

Budget for zero trust is often new, and organizations anticipate robust spending.
More than three-quarters of organizations allocate at least some new budget to zero trust, and 34% expect spending to increase significantly over the next 12-18 months.

The definitions and drivers of zero trust vary, but many organizations claim multiple security and business benefits.

Definitions of Zero Trust Vary…

Over time, zero trust has evolved to include a larger number of cybersecurity disciplines. However, even today, there is not universal agreement as to exactly what zero trust means and how it should be implemented. While a plurality of organizations think of zero trust as a strategy, 56% continue to equate it with technology—whether segmentation-centric or identity and access-focused.

" **While a plurality of organizations think of zero trust as a strategy,** 56% continue to equate it with technology"

| How organizations view zero trust.

A security strategy which assumes the network is compromised and brokers resource-specific access through a least-privileged approach supported by continuous authentication, authorization, and risk evaluation for every request — **43%**

Security technologies that granularly segment the network, data centers, and cloud infrastructure to enforce east-west traffic policy in order to limit lateral movement and prevent untrusted entities from gaining broad access to the network — **30%**

Security technologies that create an identity- and context-based logical access boundary around an application or set of applications, hiding them from public view and restricting access to a set of named entities via a trust broker — **26%**

...Leading to Divergent Zero-trust Practices

These differences in zero-trust interpretations are borne out across the principles that organizations put in place to support zero-trust initiatives. More than half of respondents strongly agree that their organizations identify and inventory all devices on the network and employ multiple factors of authentication for all users. However, other important aspects of zero trust, such as least privilege, conditional access, application-centric access, and analysis of device health and posture, are slightly less likely to be in place. The result is that, as far as zero trust has come in awareness and adoption, many organizations still have far to go in applying it pervasively across the enterprise.

Organizations employ a variety of security technologies and processes.

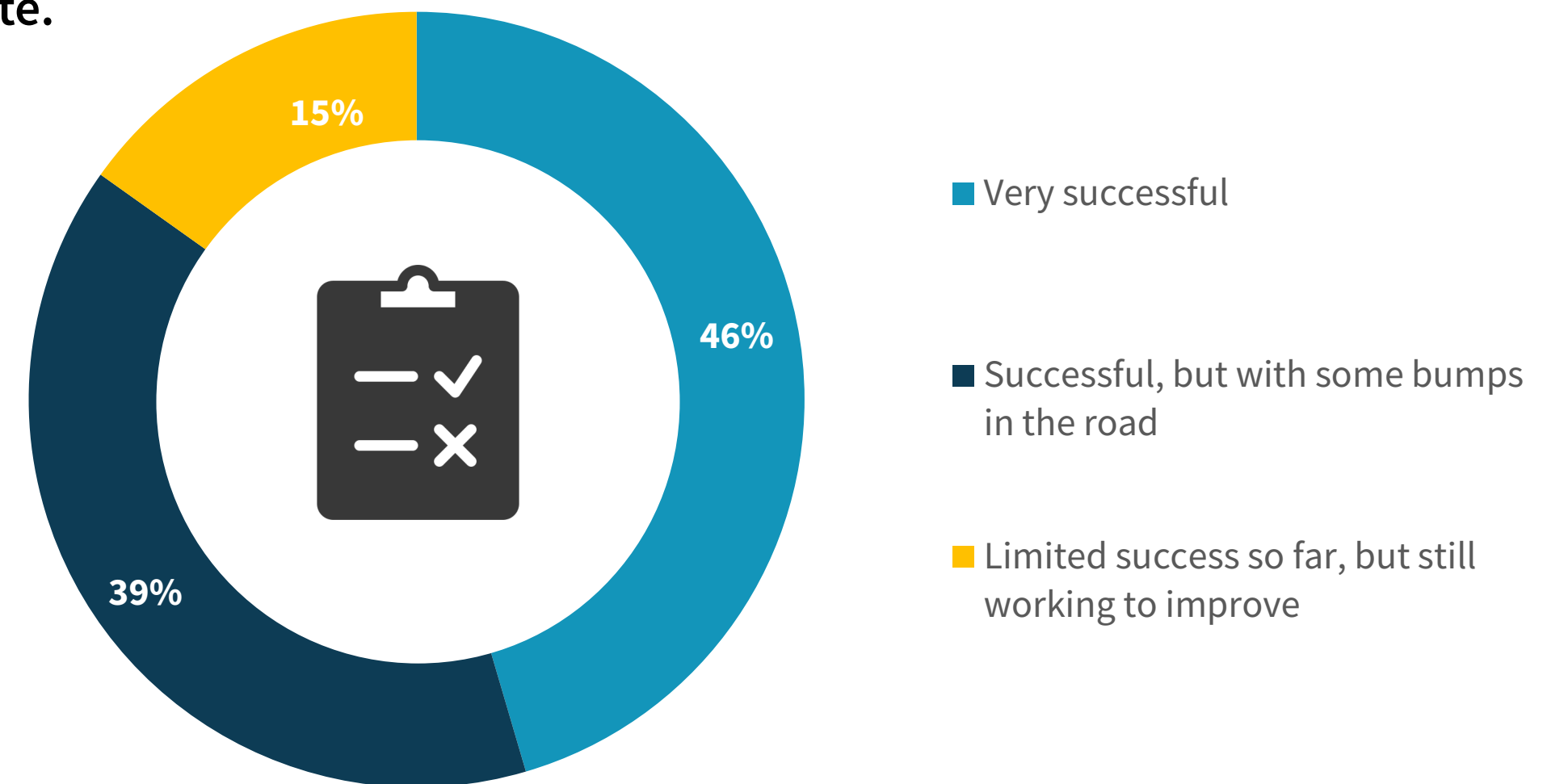|	
We identify and inventory all devices on our network	55%
We employ multiple factors of authentication for all users	50%
We use analytics to identify anomalous behavior, and require additional authentication or restrict access when questionable events occur	48%
We use data classification and security controls to understand the type and sensitivity of data users are attempting to access	48%
We use a conditional access model that weighs multiple factors before granting access	45%
We use a least-privileged access model to ensure users have only the minimum level of access required to do their job	45%
We use an application-centric model for remote user access rather than allowing users onto the open internal network	45%
We check device health and posture before allowing connections to occur	44%
Our network is adequately segmented	42%
We use microsegmentation in our on-premises data center environments	39%
We use microsegmentation in our cloud environments	37%

Regardless of the Reasons for Adopting Zero Trust, Most Report Success

There are a variety of reasons for launching a zero-trust initiative. Many organizations take a tactical view and see zero trust as an avenue towards reducing security incidents, preventing data breaches, or providing secure access to remote users. On the other end of the spectrum, enabling broader business initiatives, such as digital transformation and cloud adoption, drive zero-trust projects as well. However, most organizations look to zero trust as a means of modernizing their cybersecurity program. The tenets of zero trust are especially applicable to distributed environments and, with the acceleration of cloud adoption and remote work, it makes sense that organizations view zero trust as a way to optimize security to better address these dynamics. Regardless of why organizations begin to implement zero trust, most report at least some level of success. Zero trust should be a journey and issues can arise, but the fact that nearly half of respondents believe their initiatives have been very successful is a reassuring proof point for those considering the approach.

Top drivers of zero-trust strategies.

Driver	%
Modernizing cybersecurity program	51%
Reducing the number of security incidents	43%
Enabling secure remote access for employees and/or third parties	41%
Supporting digital transformation	35%
Accelerating cloud adoption	34%
Simplifying compliance	31%
Preventing data exfiltration	30%
Reducing/optimizing costs	29%
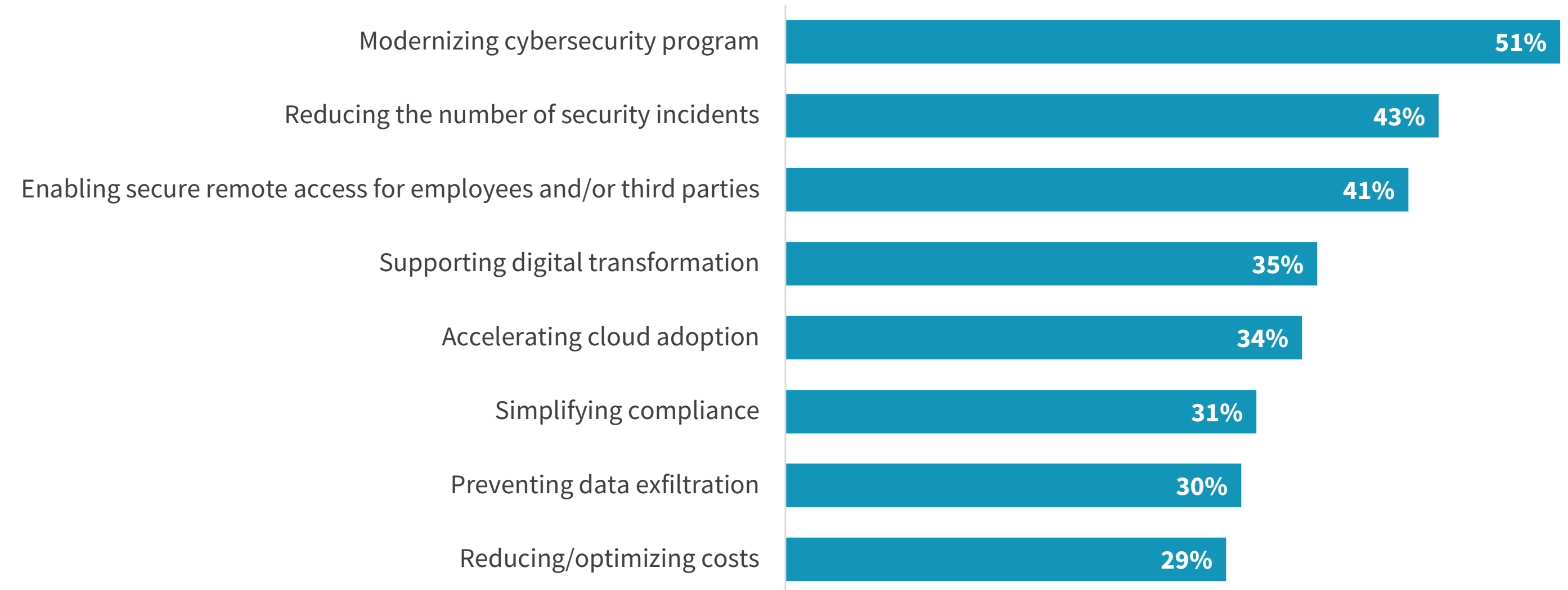
Zero-trust success to date.

- Very successful — 46%
- Successful, but with some bumps in the road — 39%
- Limited success so far, but still working to improve — 15%

" Organizations that have implemented zero trust, whether pervasively or for a specific use case, cite numerous security and business benefits resulting from the project."

| Zero-trust outcomes.

Zero trust has reduced the number of cyber incidents — **43%**

Zero trust has improved the efficiency of our SOC — **43%**

Zero trust has simplified our compliance efforts — **41%**

Zero trust has reduced the number of data breaches — **41%**

Zero trust has helped our organization become more adaptive — **38%**

Zero trust has helped our organization become more agile — **37%**

Zero trust has increased our employees' productivity — **36%**

Zero trust has increased our employees' user satisfaction — **34%**

Zero trust has reduced our organizations' security costs — **31%**

Zero Trust Improves Security and Helps the Business

Those that have yet to begin to implement zero trust in their organizations often have negative perceptions of the initiative. Technology and organizational complexity, expense, and poor user experience are all concerns prior to starting a zero-trust project. However, the reality is quite the opposite. Organizations that have implemented zero trust, whether pervasively or for a specific use case, cite numerous security and business benefits resulting from the project. As opposed to increasing complexity, organizations report better SOC efficiency and streamlined compliance efforts. Rather than being expensive to implement, zero trust can reduce security costs. And instead of adversely impacting the user experience, many report that employees are more productive and have higher user satisfaction.
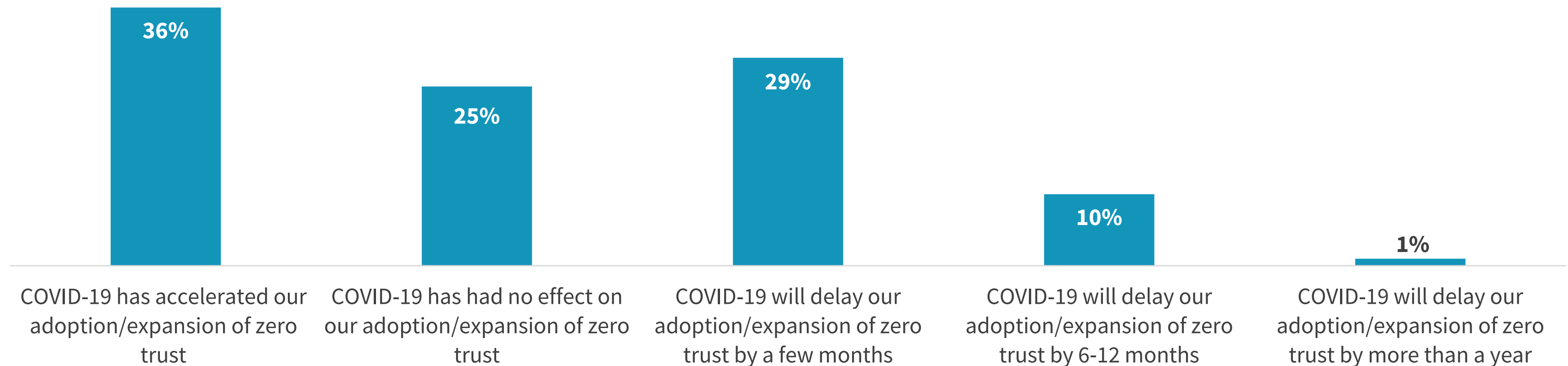
The pandemic validates the importance of zero trust.

COVID-19 Has Had A Minimal Negative Impact on Zero-trust Timing

Given the suddenness with which security organizations were forced to pivot to supporting a work-from-home model in early 2020, it would be fair to expect a majority to have paused their zero-trust projects to focus on the more pressing needs of the business. Yet while some did report that this occurred, more than one-third actually accelerated their zero-trust rollouts due to the pandemic. An additional 25% reported no impact, pointing to the strategic importance of zero trust, especially with regards to supporting work-from-home initiatives. With the emphasis zero trust places on a location-agnostic approach to establishing trust and providing secure access, it makes sense that many organizations would continue to prioritize these initiatives.

" More than one-third actually accelerated their zero-trust rollouts due to the pandemic."

Impact of COVID-19 on zero-trust initiatives.

36%	25%	29%	10%	1%
COVID-19 has accelerated our adoption/expansion of zero trust	COVID-19 has had no effect on our adoption/expansion of zero trust	COVID-19 will delay our adoption/expansion of zero trust by a few months	COVID-19 will delay our adoption/expansion of zero trust by 6-12 months	COVID-19 will delay our adoption/expansion of zero trust by more than a year

Percentage of Remote Employees Has Tripled

Percentage of total employees that are remote users.

PRIOR TO COVID-19	FALL 2020
19%	**61%**
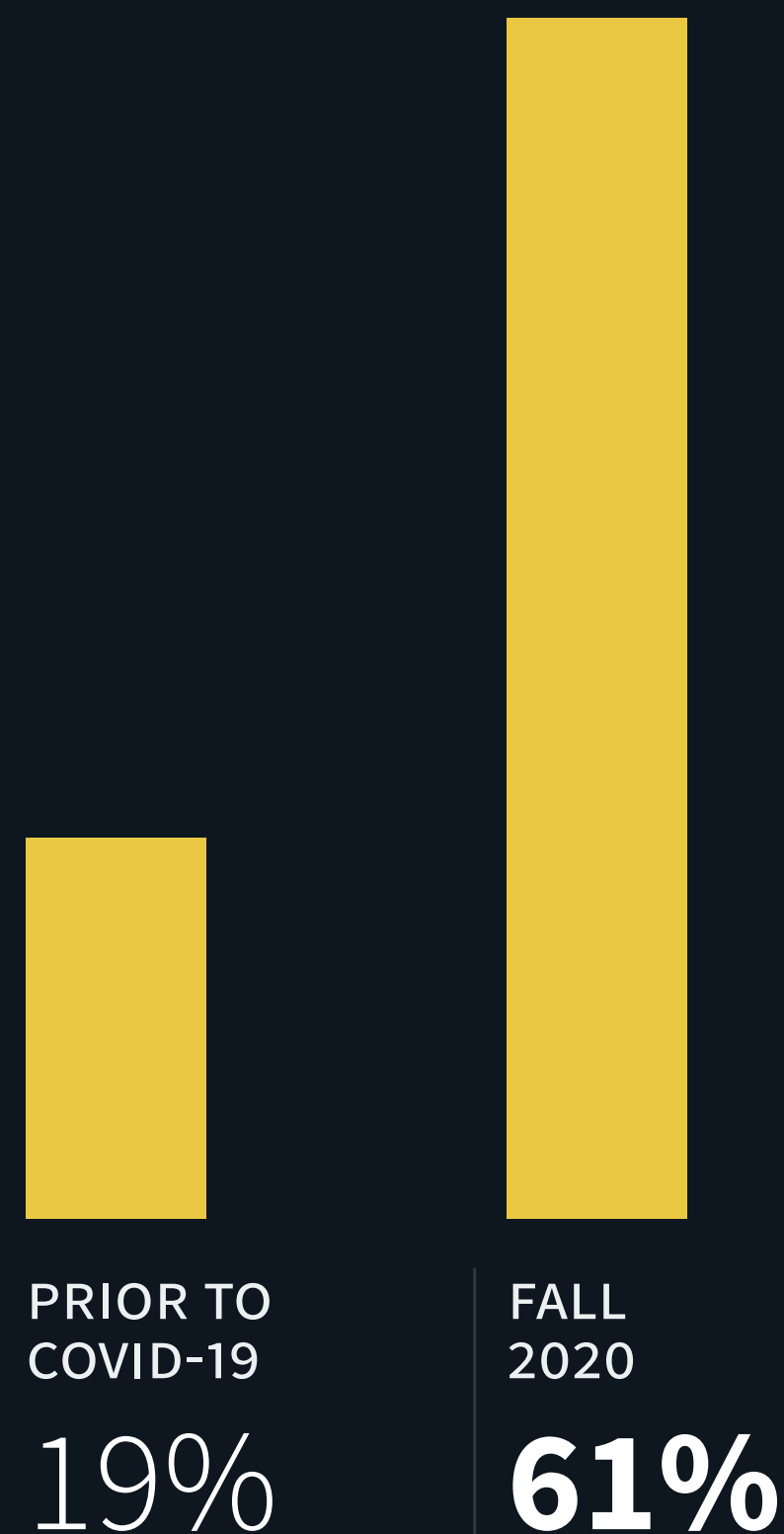
The Impact of Zero Trust on Securing Remote Employees

The logical follow-on question with regards to zero trust and work-from-home initiatives then becomes: Did organizations with these initiatives in place fare better than those that did not? Our research results reveal that they did. Specifically, those respondents at organizations with zero-trust initiatives in place were much more likely to report that the transition to a work-from-home model was very smooth. Conversely, 43% of those yet to begin a zero-trust project reported a moderate increase in their IT/security teams' workloads. With zero trust typically incorporating a least-privilege access model, multi-factor authentication, and modern remote access tools, organizations that had these initiatives in place were on average, much better prepared to pivot to work from home.

Zero-trust organizations had smoother work-from-home transitions.
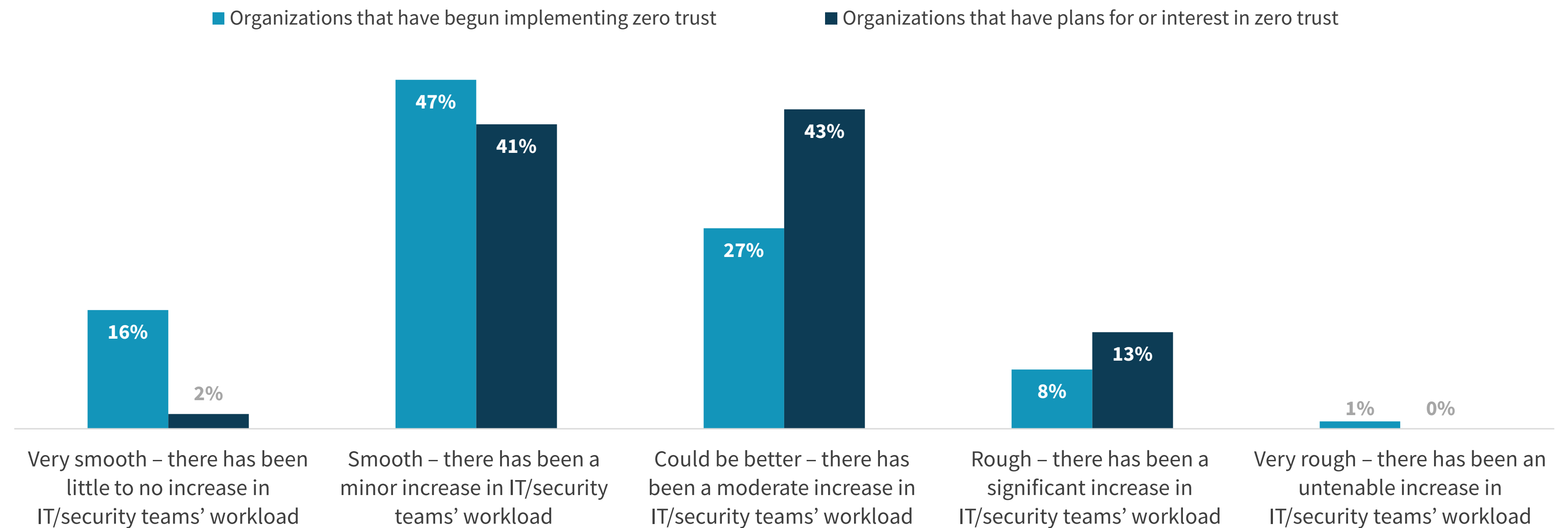
■ Organizations that have begun implementing zero trust   ■ Organizations that have plans for or interest in zero trust

	Very smooth – there has been little to no increase in IT/security teams' workload	Smooth – there has been a minor increase in IT/security teams' workload	Could be better – there has been a moderate increase in IT/security teams' workload	Rough – there has been a significant increase in IT/security teams' workload	Very rough – there has been an untenable increase in IT/security teams' workload
Begun implementing	16%	47%	27%	8%	1%
Plans/interest	2%	41%	43%	13%	0%

Formalized strategies for zero trust are common. However, most organizations begin with a specific use case and "back into" a broader zero-trust initiative.

Formalized Strategies Are Important But Often Not the Starting Point

Nearly all respondents at organizations that have begun to implement zero trust say they have a formalized, documented strategy that guid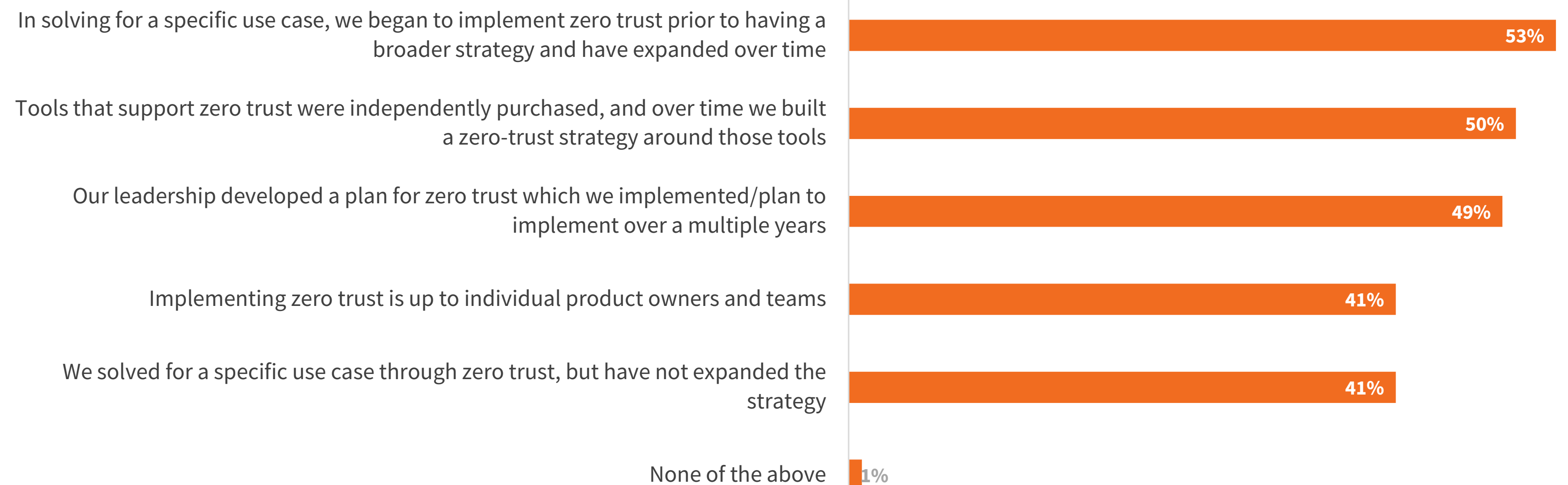es their cybersecurity program, at least some of the time. However, this does not mean that such a strategy started the initiative. Rather, many indicate that zero trust began with a specific use case and/or that a strategy was built around tools already in place in the environment. So, while critical to longer term success with zero trust, a broad, formalized strategy is not required to begin.

Approach to zero-trust.

We have a formalized, documented strategy for zero trust that guides our cybersecurity program most of the time — **43%**

We have a formalized, documented strategy for zero trust that guides our cybersecurity program some of the time — **45%**

We do not currently have a formalized strategy for zero trust, but it is in development — **9%**

We do not have a formalized strategy for zero trust, but have implemented multiple zero-trust tools — **3%**

We do not have a formalized strategy for zero trust, but have implemented one zero-trust tool — **1%**

Zero-trust experience.

In solving for a specific use case, we began to implement zero trust prior to having a broader strategy and have expanded over time — **53%**

Tools that support zero trust were independently purchased, and over time we built a zero-trust strategy around those tools — **50%**

Our leadership developed a plan for zero trust which we implemented/plan to implement over a multiple years — **49%**

Implementing zero trust is up to individual product owners and teams — **41%**

We solved for a specific use case through zero trust, but have not expanded the strategy — **41%**

None of the above — **1%**

" **Nearly two-thirds of those respondents that have had a zero-trust strategy in place** for at least two years report that it has been implemented across their organization. **"**

| Extent of zero-trust strategy implementations.

■ Zero trust in place for less than two years   ■ Zero trust in place for two years or more

43%   62%

57%   38%

We've implemented or begun to implement zero trust across the organization

We've implemented or begun to implement zero trust for specific use cases

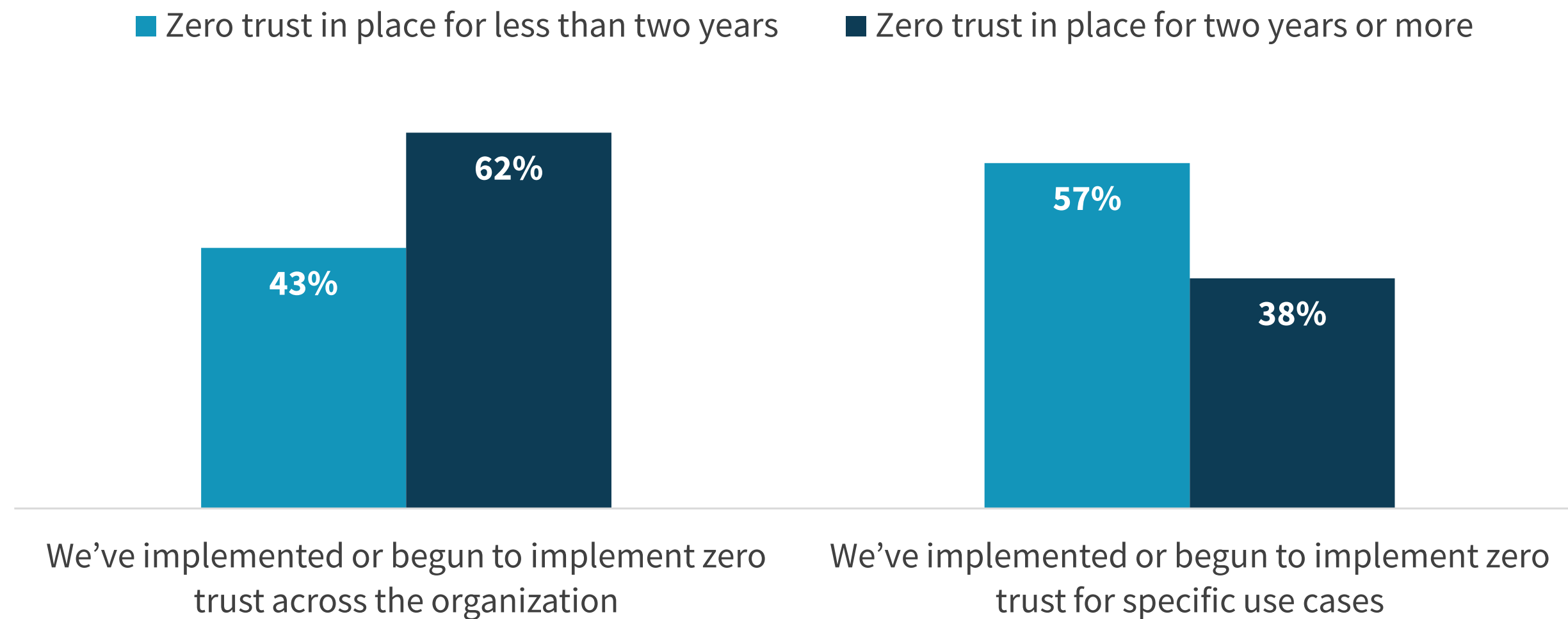## Moving From Specific Use Cases to a Broader Strategy Is Not Always Dependent on Length of Time Zero Trust Has Been in Place

Nearly two-thirds of those respondents that have had a zero-trust strategy in place for at least two years report that it has been implemented across their organization. That is not to say that all organizations over time move to a broader, more enterprise-wide implementation. Many do, but some continue to focus on specific aspects of zero trust or apply zero trust to specific use cases even after multiple years. The breadth of technologies required, the number of teams with input into strategy creation and decision making, and potential complexity as the initiative is broadened all contribute to some organizations deciding to maintain a more focused approach to zero trust.

Process and Technology Improvements Are a Key Focus Moving Forward

Even those organizations citing success with zero trust recognize the need to continually improve and optimize their approach. The top area organizations expect to focus their attention on is improving collaboration across the cross-functional teams involved with zero trust. This is an ongoing challenge across all of security, so with the broad teams required to successfully implement zero trust, it is no surprise that improving collaboration would be a top focus. More tactically, authentication, secure access, and analytics all play a major role in securing the remote workforce and top the list from a technology perspective.

" **The top area organizations expect to focus their attention on** is improving collaboration across the cross-functional teams involved with zero trust. **"**
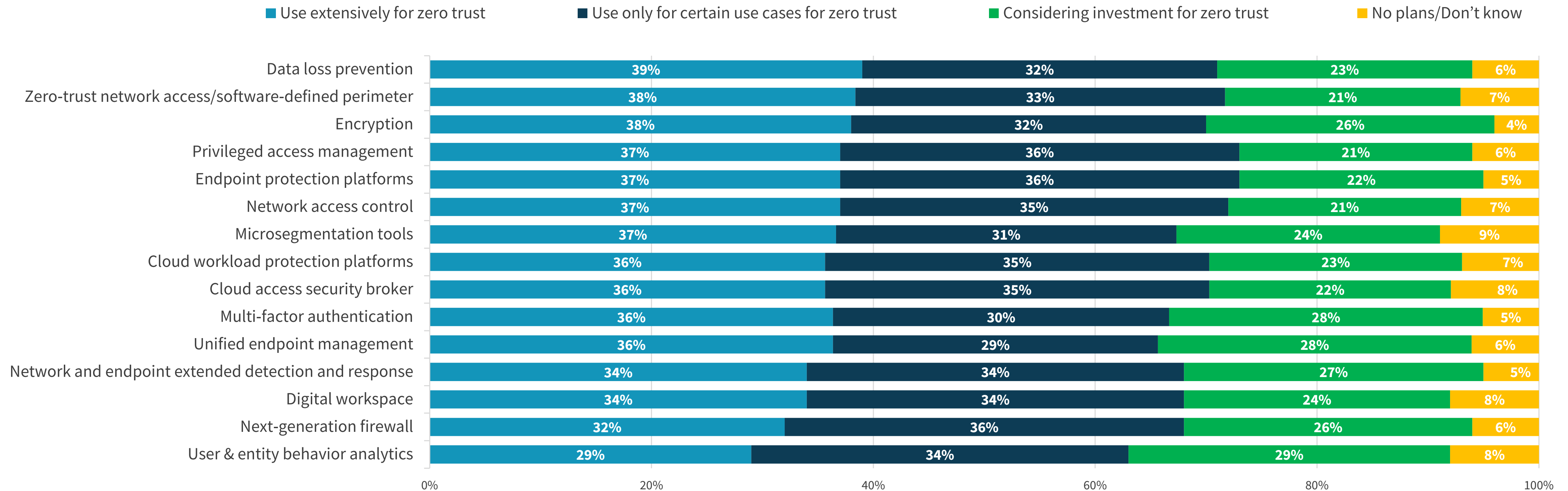
| **Approach to zero-trust.**

Improve the collaboration across security operations, IT operations, and lines of business	46%
Implement stronger authentication controls	43%
Invest in tools to modernize secure remote access	40%
Enhance analytics, detection, and response capabilities	40%
Work with professional services firms to build or refine our zero-trust strategy	38%
Work with professional services firms to implement zero-trust tools	38%
Incorporate more data-centric controls	36%
Incorporate more automation	33%
Hire more personnel	28%

The broad range of tools required for zero trust drives interest in a platform approach.

Clear Agreement That Zero Trust Requires Many Tools

Zero trust can be a significant undertaking, crossing multiple security disciplines spanning the technology stack, including the network, data, identity, endpoints, and operations and analytics. Unfortunately, there is no "right" answer as to where to begin. Deciding on a starting point must be based on the organization's initial goals, existing capabilities, and ultimate strategy. While one organization prioritizing the prevention of data breaches may lean more heavily on data security controls, another securing remote users may invest in zero-trust network access solutions.
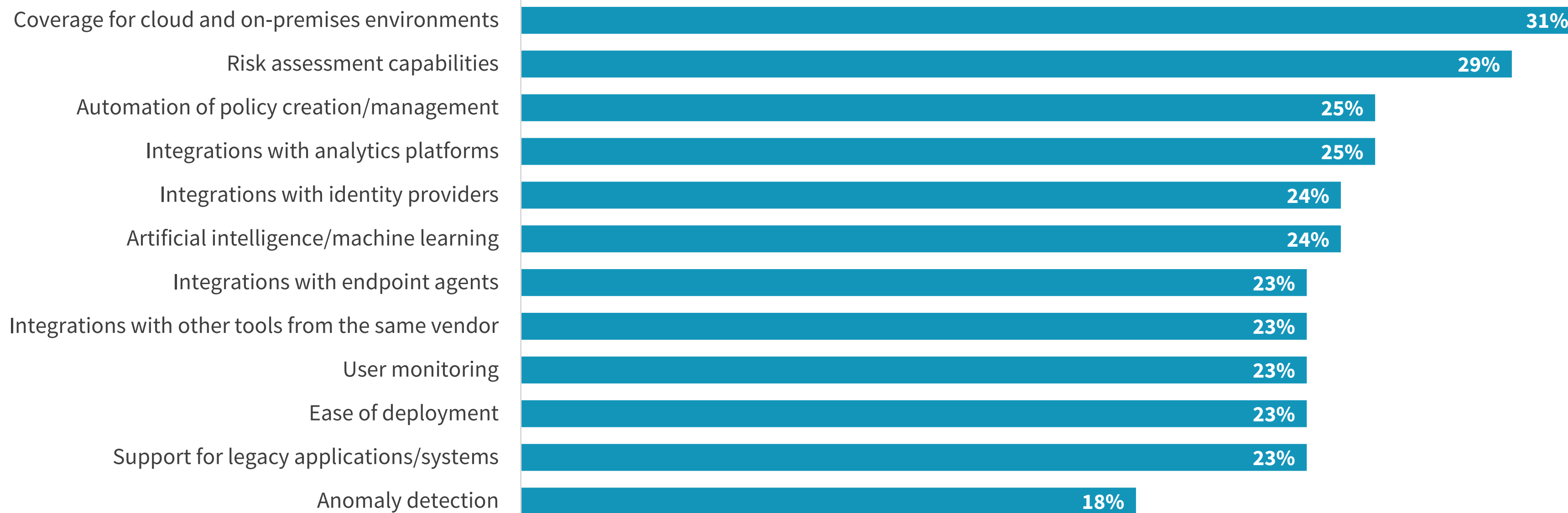
| Extent of technologies used to support zero-trust strategies.

	■ Use extensively for zero trust	■ Use only for certain use cases for zero trust	■ Considering investment for zero trust	■ No plans/Don't know
Data loss prevention	39%	32%	23%	6%
Zero-trust network access/software-defined perimeter	38%	33%	21%	7%
Encryption	38%	32%	26%	4%
Privileged access management	37%	36%	21%	6%
Endpoint protection platforms	37%	36%	22%	5%
Network access control	37%	35%	21%	7%
Microsegmentation tools	37%	31%	24%	9%
Cloud workload protection platforms	36%	35%	23%	7%
Cloud access security broker	36%	35%	22%	8%
Multi-factor authentication	36%	30%	28%	5%
Unified endpoint management	36%	29%	28%	6%
Network and endpoint extended detection and response	34%	34%	27%	5%
Digital workspace	34%	34%	24%	8%
Next-generation firewall	32%	36%	26%	6%
User & entity behavior analytics	29%	34%	29%	8%

Users Expect a Broad Range of Capabilities, Paving the Way for a Platform Approach

The shift to platforms is prevalent across many parts of the cybersecurity industry. SASE, XDR, and WAAP are all examples of the trend towards consolidation. While zero trust is in many ways much broader than those examples, the interest in a platform-based approach is very strong. But there is recognition that it will be difficult for any one vendor to offer a comprehensive platform. Integrations, specifically with analytics, identity, and endpoint tools, are key attributes respondents look for in zero-trust tools. Further, a platform must be able to provide consistent coverage across both cloud and on-premises environments to alleviate the operational inefficiencies many organizations struggle with when using siloed tools, and incorporate risk assessment capabilities to monitor activity and understand changes in an entity's posture (and inherent trustworthiness) over time.

Most important zero-trust attributes.

Attribute	Percentage
Coverage for cloud and on-premises environments	31%
Risk assessment capabilities	29%
Automation of policy creation/management	25%
Integrations with analytics platforms	25%
Integrations with identity providers	24%
Artificial intelligence/machine learning	24%
Integrations with endpoint agents	23%
Integrations with other tools from the same vendor	23%
User monitoring	23%
Ease of deployment	23%
Support for legacy applications/systems	23%
Anomaly detection	18%

Approach to Zero-trust Tools

37%

We are currently using a platform approach to support our zero-trust strategy

28%

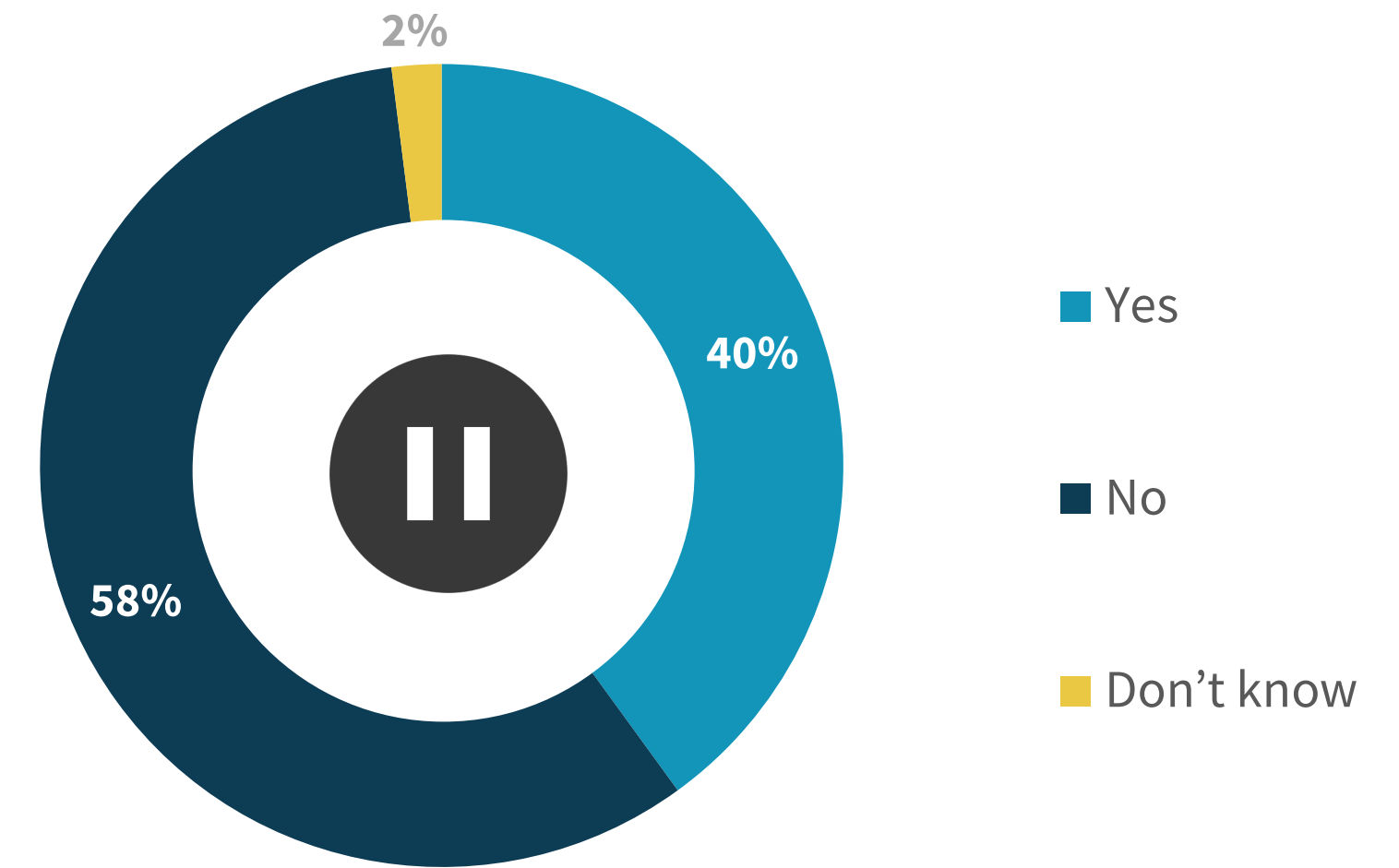We will consider a platform approach to support our zero-trust strategy over the next 12-24 months

Back to Contents

Cross-functional collaboration is critical to zero-trust success and is leading to interest in centers of excellence.
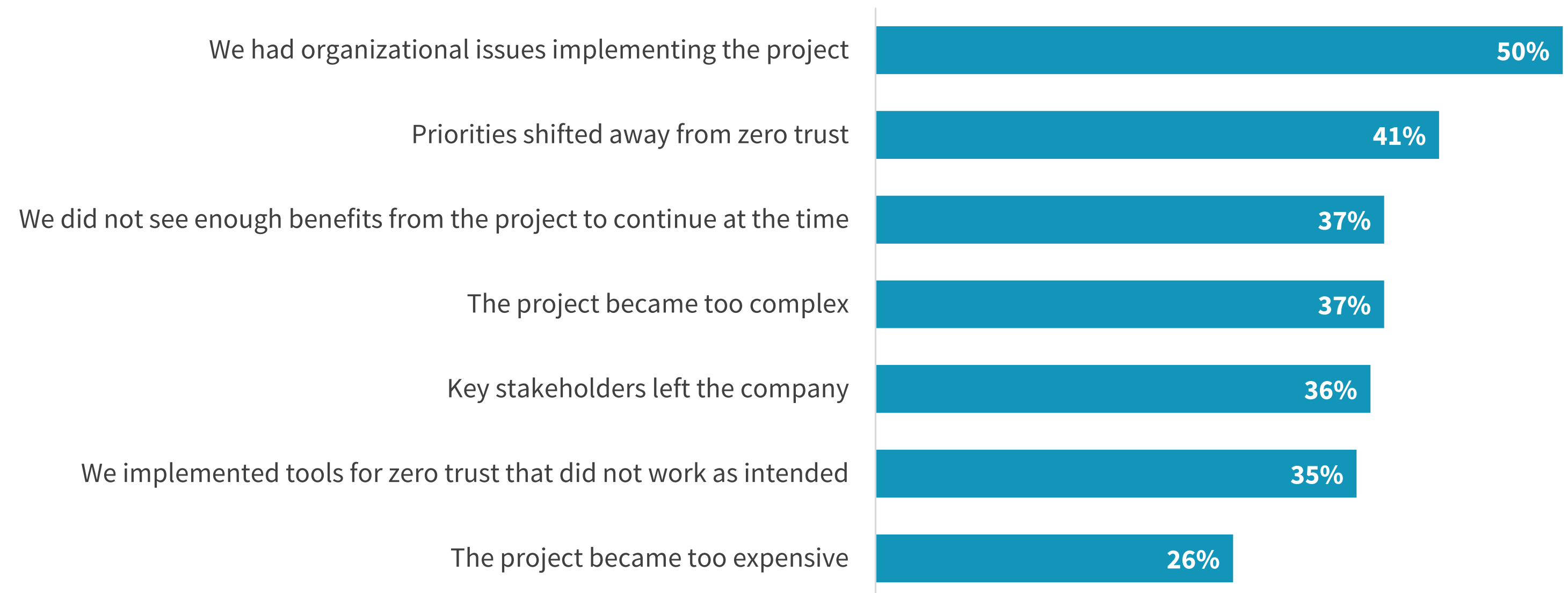
False Starts Are Common, Often for Organizational Reasons

It is not uncommon for organizations to struggle with zero trust at some point during their journey. In fact, 40% of respondents report that their organization paused or abandoned a project at some point in the past. However, it is important to note that all of those reporting that projects were paused or abandoned were companies with current zero-trust implementations or interest in zero-trust projects. While there are many reasons, half of our respondents cited the difficulties in navigating organizational complexity. An additional 36% indicated that key stakeholders had left the company, pointing to the fact that as much as zero trust is a team sport, it also needs a champion to succeed.
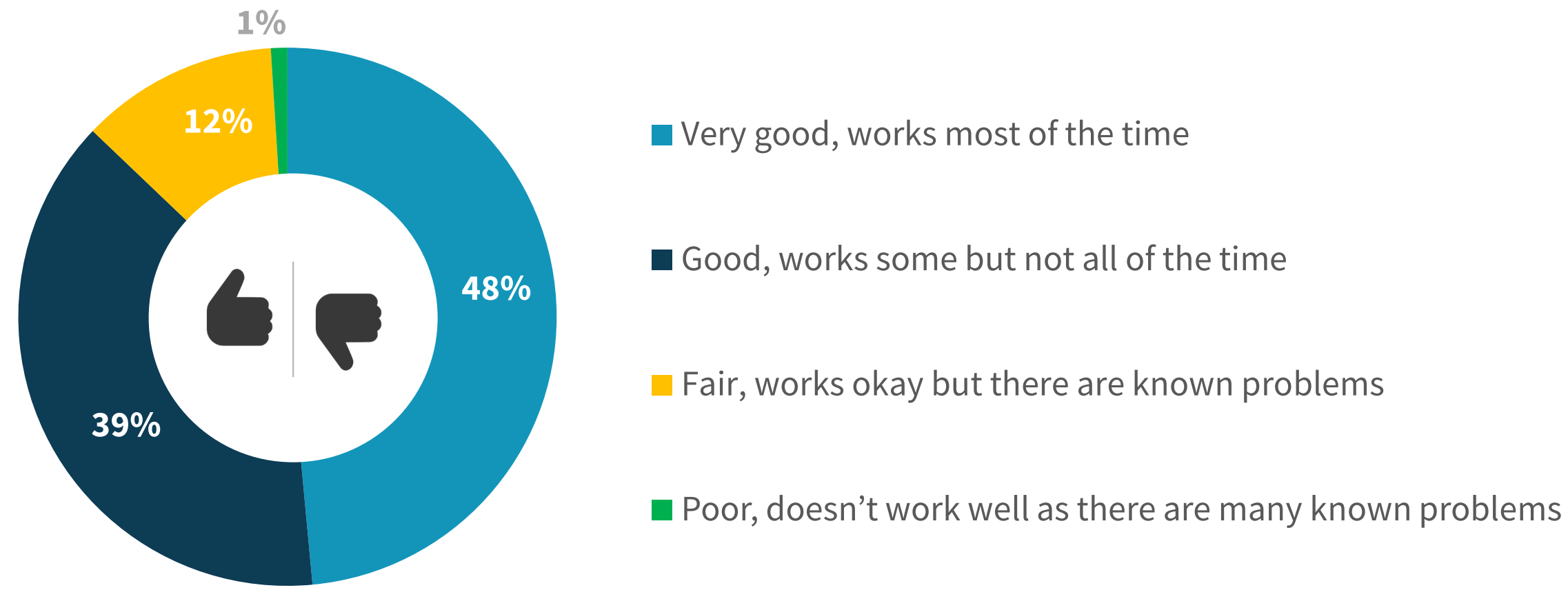
| Have organizations paused or abandoned a zero-trust project?

2%

40%

58%

■ Yes

■ No

■ Don't know

| Reasons zero-trust projects were paused or abandoned.

We had organizational issues implementing the project	50%
Priorities shifted away from zero trust	41%
We did not see enough benefits from the project to continue at the time	37%
The project became too complex	37%
Key stakeholders left the company	36%
We implemented tools for zero trust that did not work as intended	35%
The project became too expensive	26%

Day-to-day zero-trust collaboration effectiveness.

1%

12%

48%

39%

- Very good, works most of the time
- Good, works some but not all of the time
- Fair, works okay but there are known problems
- Poor, doesn't work well as there are many known problems

Organizational challenges related to zero trust.

Communication issues related to collaborative tasks	32%
Security teams are slow to incorporate feedback/recommendations from non-security teams	32%
Lack of clarity about areas of responsibility	29%
Non-security teams move too quickly without input from security teams	29%
Different groups are measured and compensated on conflicting goals	29%
Security team does not keep non-security teams apprised of new developments	28%
Issues related to the chain of command	26%
Non-security teams do not keep security teams apprised of new developments	25%
Not enough top-level leadership supporting the initiative	20%
We have not experienced any challenges/have no concerns	11%

Zero-trust Collaboration Is Fairly Strong But Issues Do Exist

While many organizations report some level of success with the cross-functional collaboration across the different groups responsible for the strategy, technical evaluation, and decision making related to zero trust, challenges certainly remain. As with other areas of IT and security, communication is a key problem area, both with regards to optimizing workflows related to collaborative tasks and keeping the different teams involved well informed and up to speed. To be clear, no one team is to blame. In fact, most put equal weight on both the security teams and non-security teams with regards to not keeping the other informed of new developments. Additionally, the well-established perceptions of security teams as groups that act methodically and slow the business down and the lines of business as organizations that move too quickly and without regards for security still exist, even with the context of zero trust.
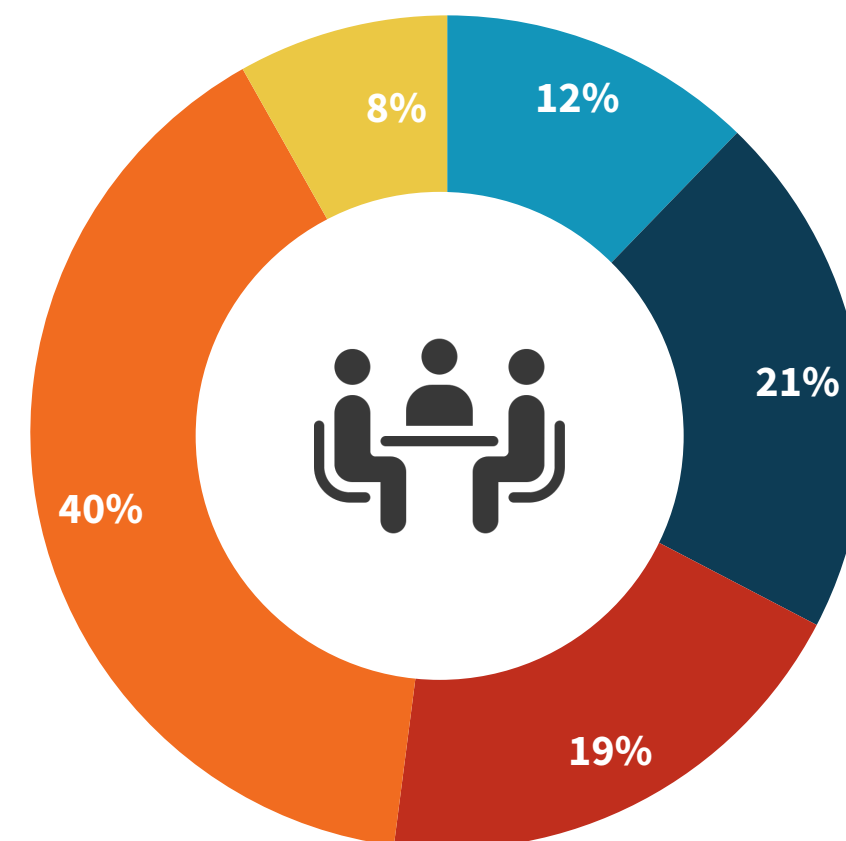
There Is Early Interest in a Center-of-excellence Model to Formalize the Cross-functional Collaboration Required for Zero-trust Success

When asked about the individuals and groups involved with zero-trust initiatives, respondents had varied answers, though the majority did indicate that some combination of senior IT and security management, along with IT operations, have been participants. Because of the range of teams and people involved with zero trust, there is early movement towards, and significant interest in, centers of excellence (CoE) to support the cross-functional collaboration required for a successful implementation. While only 12% of organizations report that their organization has already implemented a zero-trust CoE, an additional 20% are actively working towards implementing one. In fact, fewer than one in ten respondents indicated that their organizations have no plans for or interest in zero trust.

Personas involved with zero-trust initiatives.

Persona	%
Senior IT management	64%
Senior security management	56%
IT operations	53%
Security operations	39%
Data protection officer	35%
Security architect	33%
DevOps/application development	31%
Risk/legal/compliance	29%
Cloud architect	28%
Zero-trust center of excellence	7%
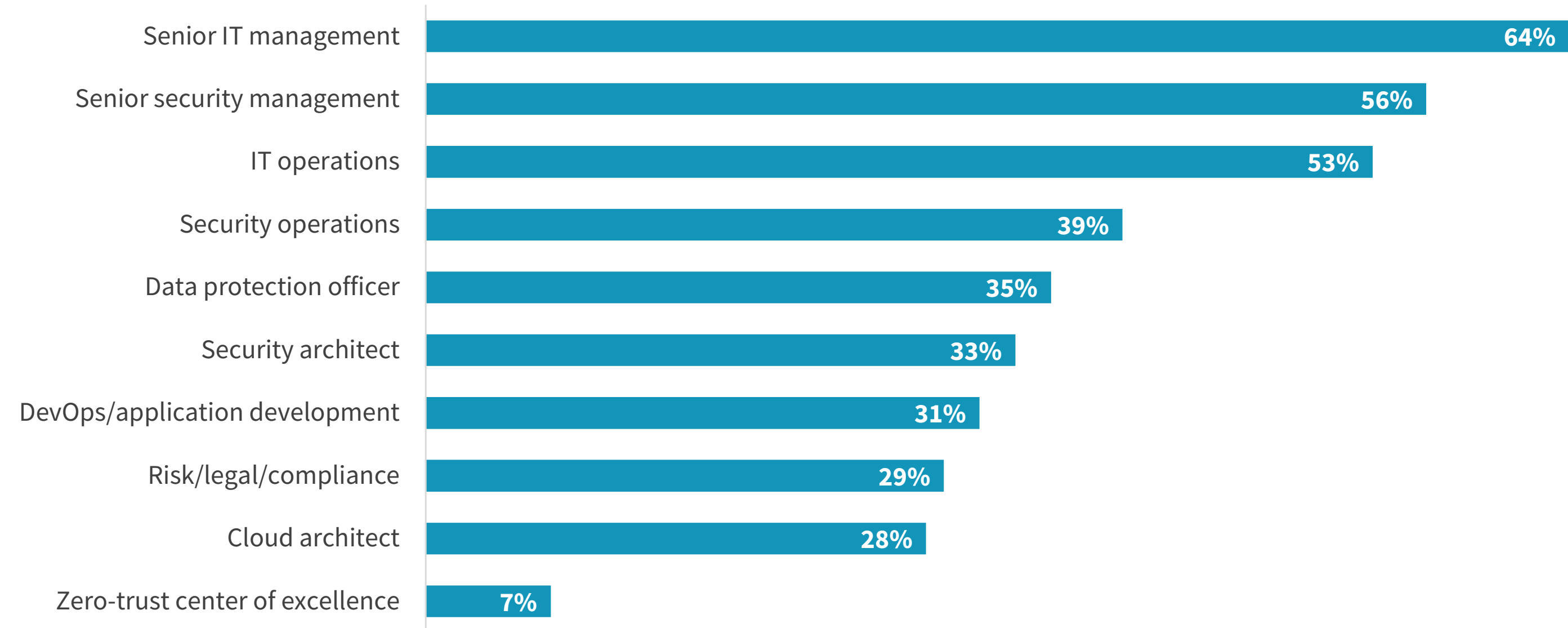
Interest in zero-trust centers of excellence.

- 12% ■ My organization has implemented a zero-trust center of excellence
- 21% ■ My organization is actively working to implement a zero-trust center of excellence
- 19% ■ My organization plans to implement a zero-trust center of excellence
- 40% ■ My organization is interested in implementing a zero-trust center of excellence
- 8% ■ My organization has no plans for or interest in implementing a zero-trust center of excellence

# Budget for zero trust is often new, and organizations anticipate robust spending.

# Budget Models Differ, but Zero-trust Funding is Typically Net-new

Not surprisingly, given the prevalence of formalized zero-trust strategies, many organizations have established dedicated zero-trust budgets with which to fund these initiatives. There is a split with regards to whether this represents a dedicated program budget or a line-item budget within other program budgets such as network, identity, or endpoint. However, the trend towards discrete zero-trust spending shows the strategic importance organizations are placing on these projects. Further, it is largely new budget that is funding zero trust. Nearly a third of respondents say their zero-trust budget is fully net-new, and an additional 44% report it is a mix of net-new and reallocated funding.

76%
report net-new
zero-trust funding

**Sources of
zero-trust funding**

35%

48%
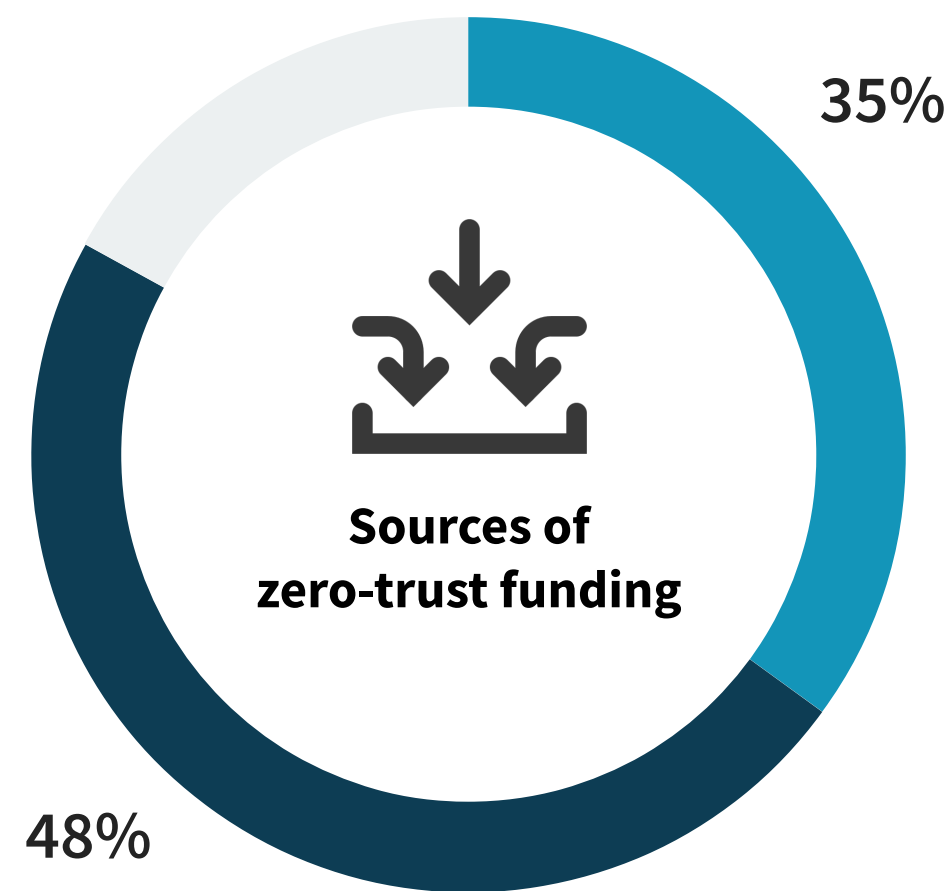
■ A dedicated zero-trust program budget

■ Discrete zero-trust budget within other
security program budgets
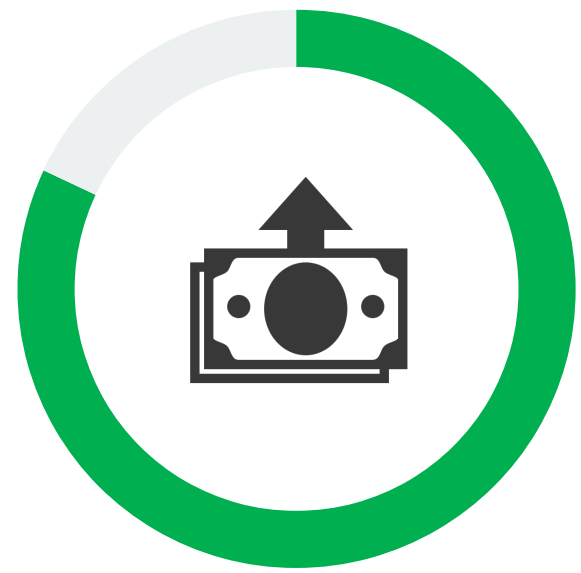
82%

of organizations will increase spending on zero trust over the next 12-18 months

| Security controls expected to benefit from increased zero-trust spending.

Zero-trust network access/software-defined perimeter	43%
Cloud access security broker	41%
Multi-factor authentication	36%
Network access control	34%
Digital workspace/virtual desktop infrastructure	33%
Endpoint protection platforms	33%
Data loss prevention	32%
Identity and access management	31%
User and entity behavior analytics	28%
Encryption	28%
Next-generation firewall	28%
Remote browser isolation	27%
Privileged access management	26%
Continuous monitoring for anomalous activity	26%
Unified endpoint management	26%
Microsegmentation tools	25%

Robust Spending On Zero Trust Is Anticipated

While the pandemic certainly impacted the IT spending plans of many organizations, it was not always a negative development. Many organizations saw the pandemic as an opportunity to increase spending in areas that increased business agility and resiliency and that would help them be more successful in the long term, especially in the face of socioeconomic uncertainty. Zero trust would seem to fall into this category, especially considering the agility and adaptability benefits organizations have seen from zero-trust initiatives. The vast majority of organizations anticipate increased spending on technologies and services supporting zero trust. ZTNA, CASB, MFA, and NAC are among the areas where the most organizations expect to increase spending. NAC may seem like an outlier on the surface; however, as employees return to office settings and apply zero-trust principles to IoT environments, NAC is a critical component of the strategy.

zscaler™

Zscaler enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a multitenant, distributed cloud security platform that protects thousands of customers from cyberattacks and data loss. Learn more at zscaler. com or follow us on Twitter @zscaler.

LEARN MORE

About ESG

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

Research Methodology

To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between December 8, 2020 and December 22, 2020. To qualify for this survey, respondents were required to be IT and cybersecurity professionals personally responsible for driving zero-trust security strategies and evaluating, purchasing, and managing security technology products and services in support of these initiatives. 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 421 IT and cybersecurity professionals.

Totals in figures and tables throughout this eBook may not add up to 100% due to rounding.
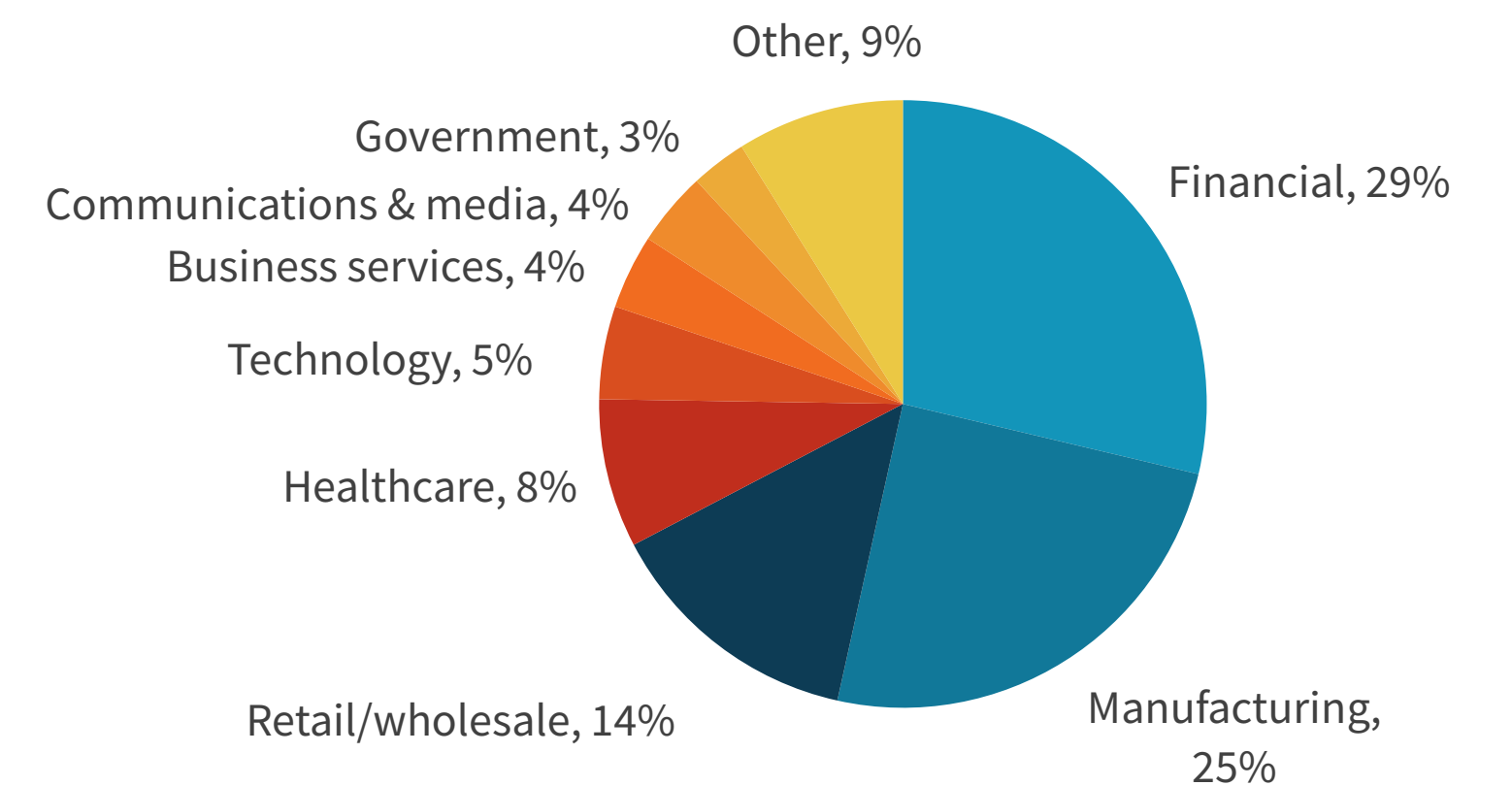
RESPONDENTS BY NUMBER OF EMPLOYEES

- 500 to 999, 15%
- 1,000 to 2,499, 24%
- 2,500 to 4,999, 32%
- 5,000 to 9,999, 18%
- 10,000 to 19,999, 7%
- 20,000 or more, 5%
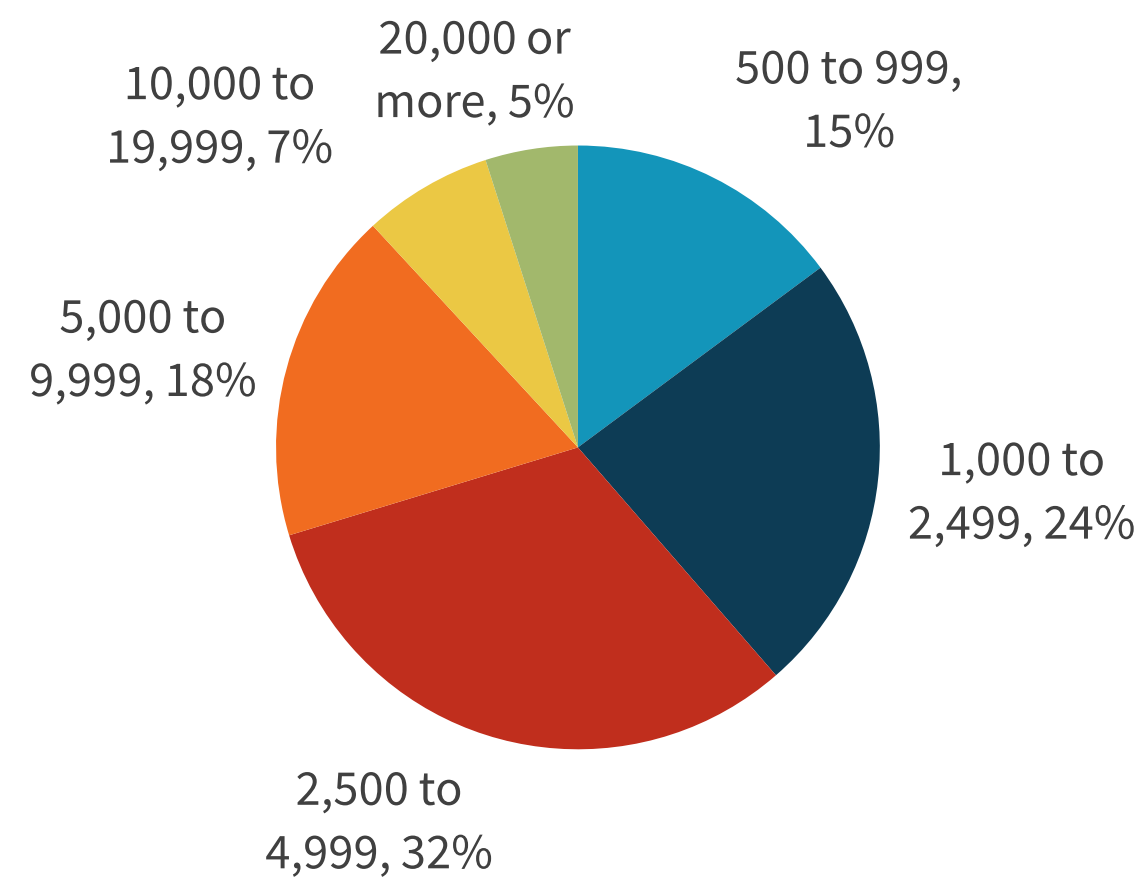
RESPONDENTS BY AGE OF COMPANY

- 1 to 5 years, 6%
- 6 to 10 years, 26%
- 11 to 20 years, 39%
- 21 to 50 years, 19%
- More than 50 years, 11%
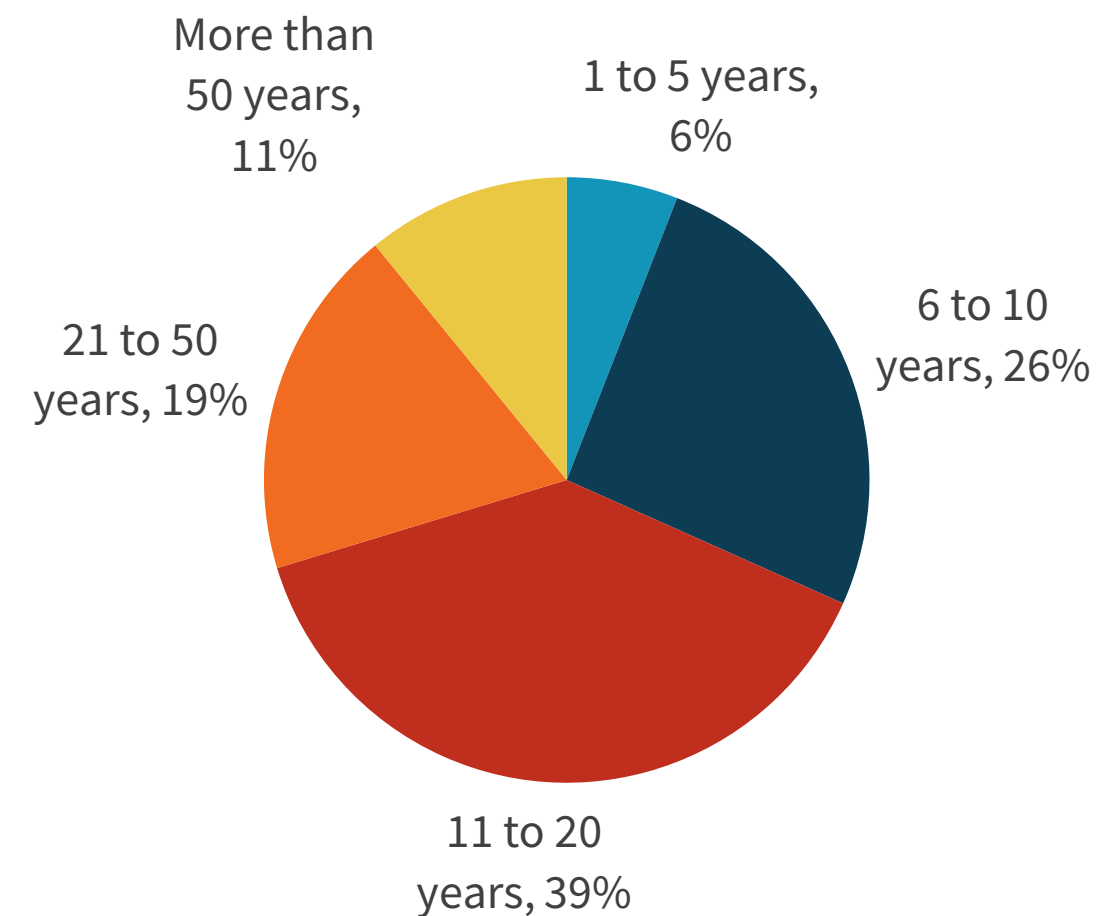
RESPONDENTS BY INDUSTRY

- Financial, 29%
- Manufacturing, 25%
- Retail/wholesale, 14%
- Healthcare, 8%
- Technology, 5%
- Business services, 4%
- Communications & media, 4%
- Government, 3%
- Other, 9%

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.
© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.