



Enterprise Strategy Group | Getting to the bigger truth.™

RESEARCH HIGHLIGHTS

# The State of Zero-trust Security Strategies

John Grady, Senior Analyst

---

FEBRUARY 2021





CONTENTS

Research Objectives 3

Research Highlights 4

The definitions and drivers of zero trust vary, but many organizations claim multiple security and business benefits. 5

The pandemic validates the importance of zero trust. 10

Formalized strategies for zero trust are common. However, most organizations begin with a specific use case and “back into” a broader zero-trust initiative. 13

The broad range of tools required for zero trust drives interest in a platform approach. 17

Cross-functional collaboration is critical to zero-trust success and is leading to interest in centers of excellence. 20

Budget for zero trust is often new, and organizations anticipate robust spending. 24





## 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:



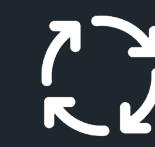
**Understand the trigger points** that are influencing zero-trust initiatives and how decision makers are prioritizing and timing purchasing decisions.



**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.



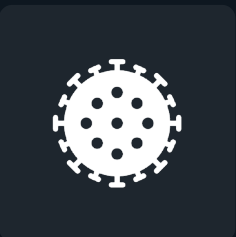
**Determine the extent** to which specific technologies and products are being deployed to support zero-trust strategies.



# 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.

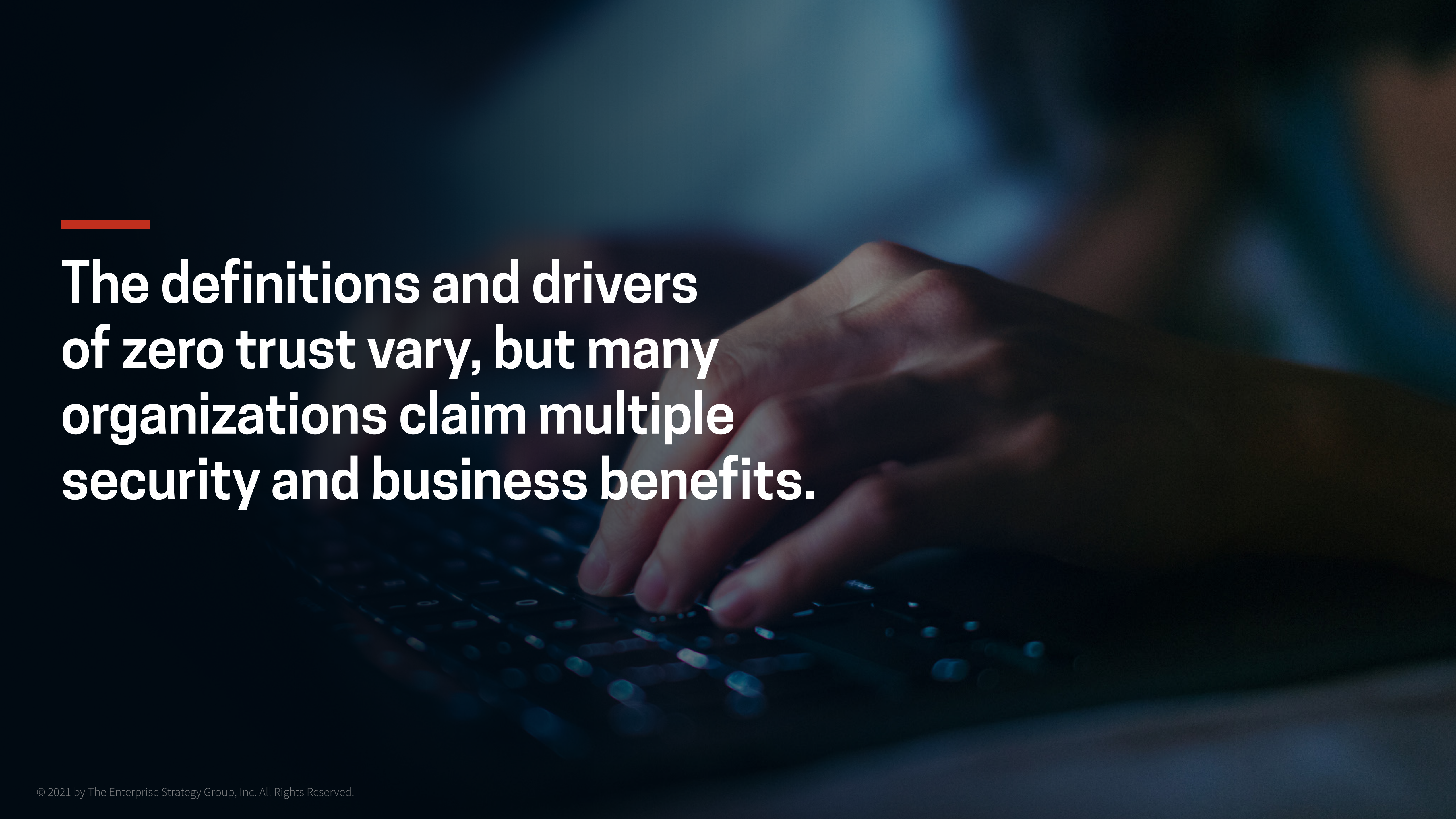


**Cross-functional collaboration is critical to zero-trust success and is leading to interest in centers of excellence.**  
There are currently many individuals and groups involved with zero-trust strategies. And while only 12% of organizations have implemented a zero-trust center of excellence (CoE) 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.



A close-up, low-angle shot of a person's hand typing on a laptop keyboard. The scene is dimly lit, with a strong blue light source creating a cool, technological atmosphere. The hand is positioned in the center-right of the frame, with fingers pressing down on the keys. The keyboard itself is dark, and the keys are illuminated by the ambient blue light. The background is out of focus, showing more of the laptop and possibly the user's face in shadow.

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

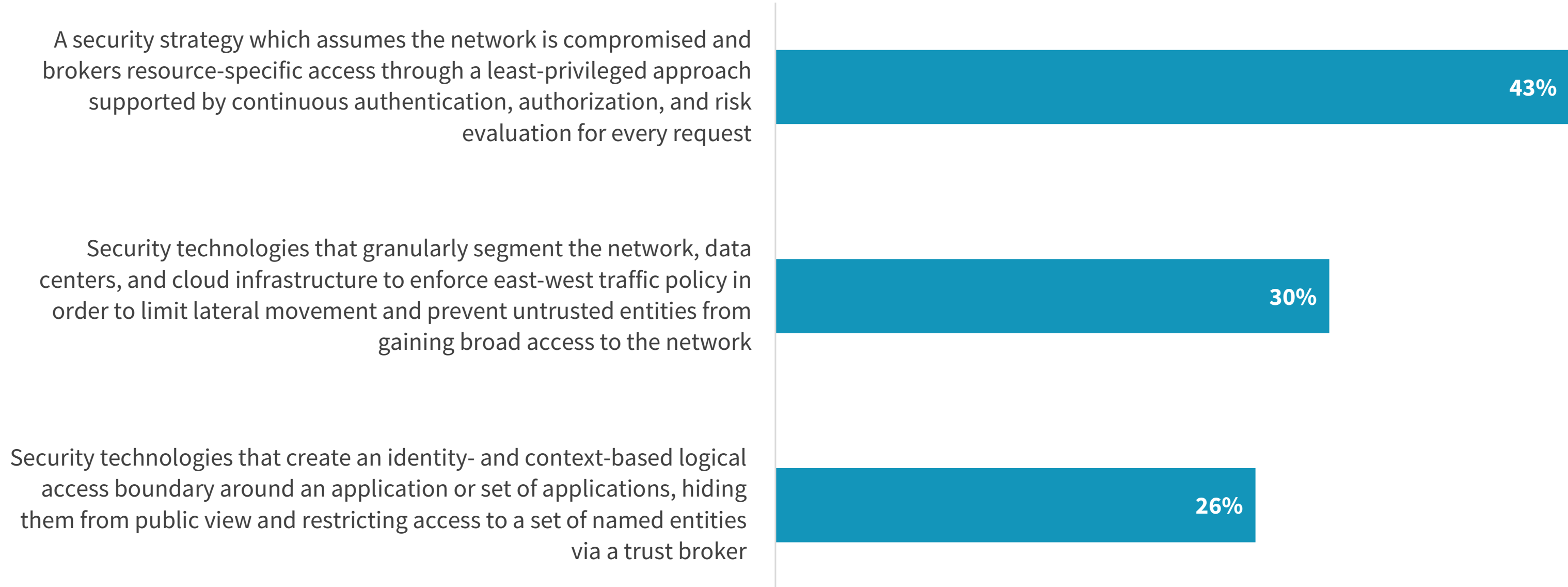


Definitions of Zero Trust Vary...

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”

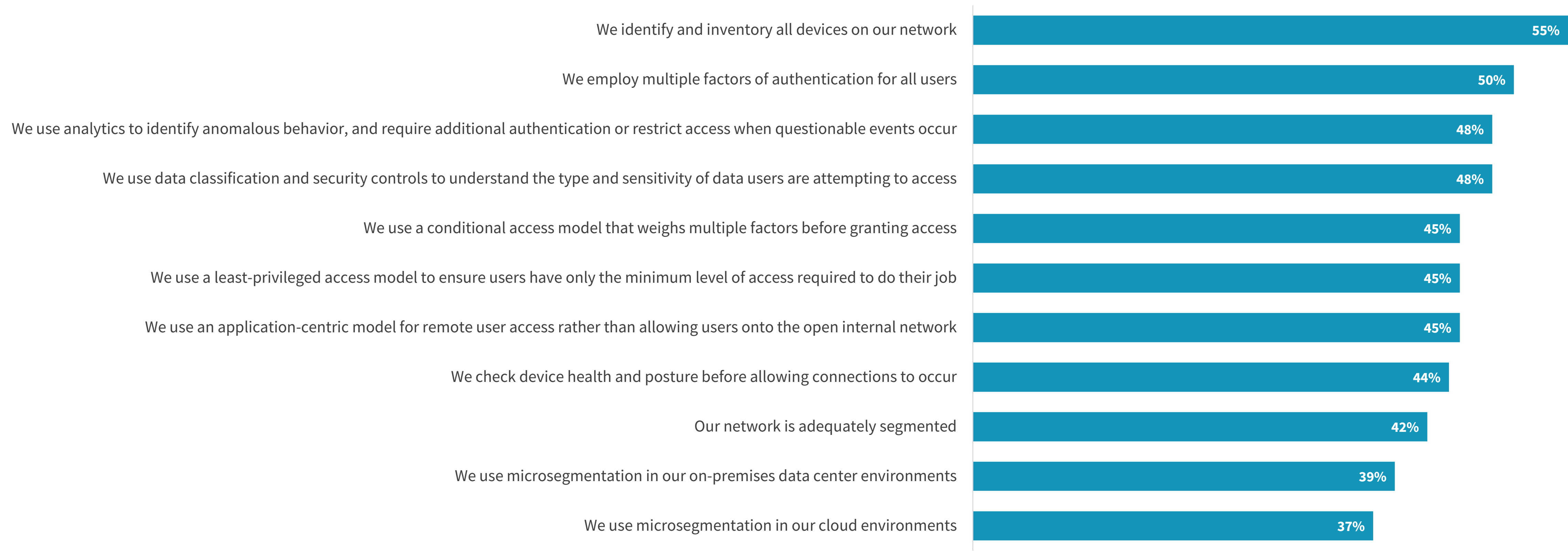
How organizations view zero trust.



## ...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.

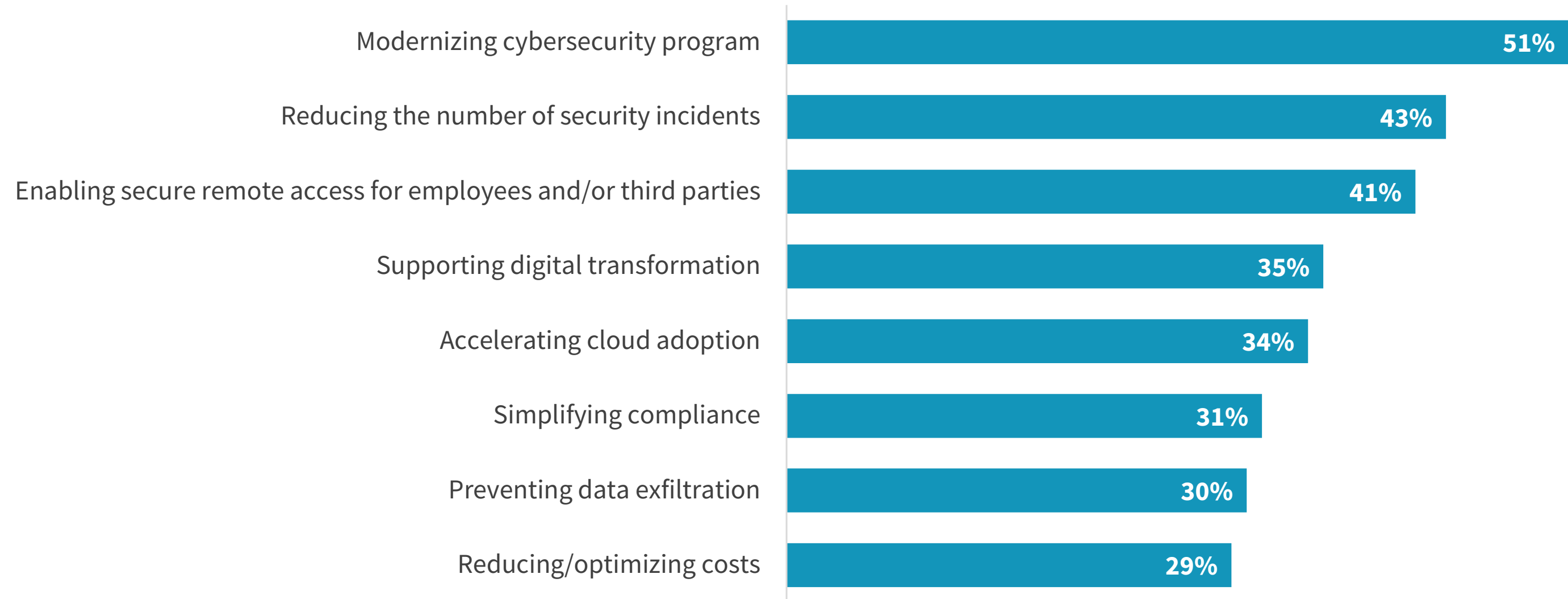
### | Organizations employ a variety of security technologies and processes.



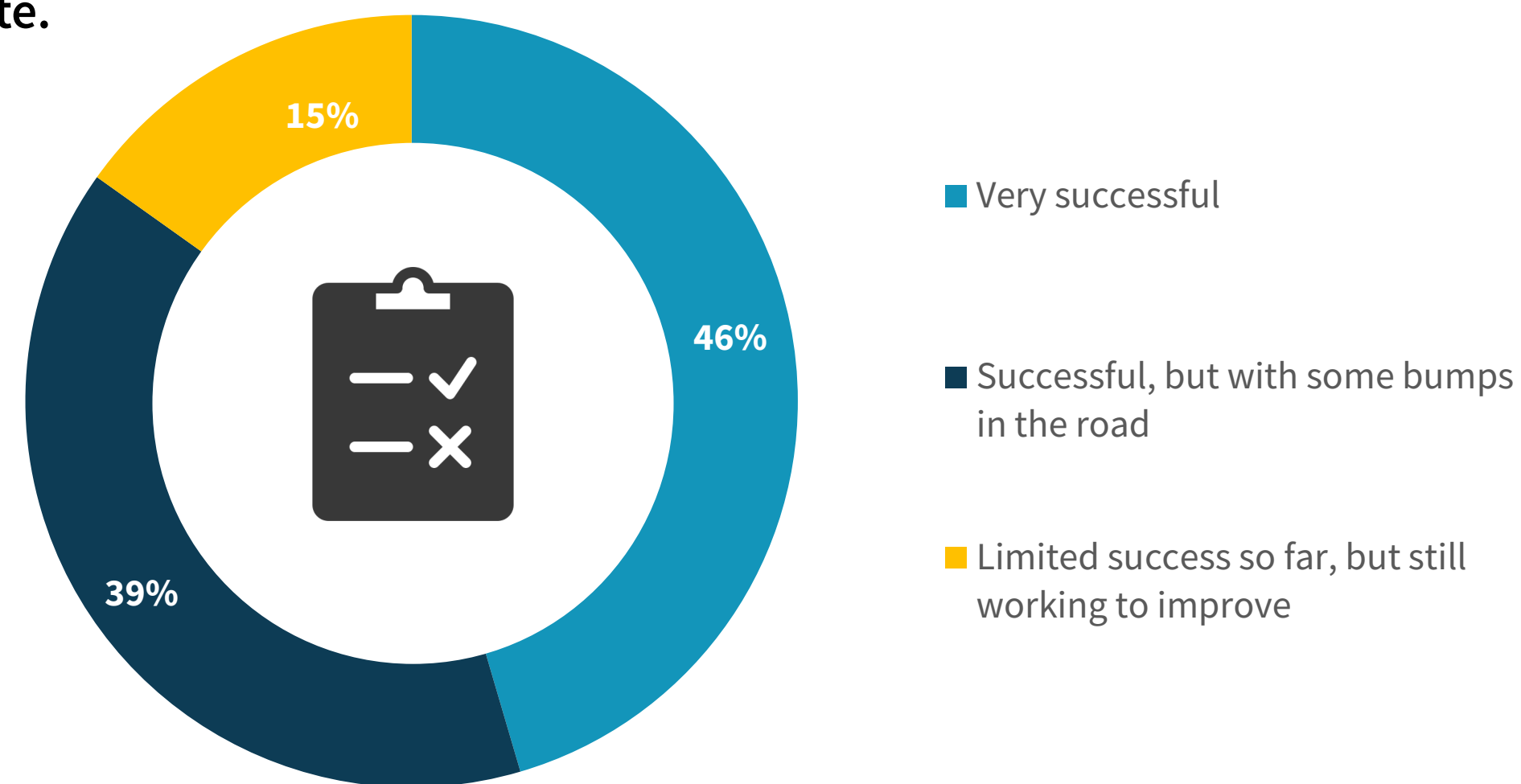
## Regardless of the Reasons for Adopting Zero Trust, Most Report Success

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.



### Zero-trust success to date.





“ **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 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.



A man with dark skin and curly hair, wearing a beige blazer over a yellow shirt, is seated at a desk, focused on his work. He is typing on a laptop. On the desk, there is a white mug with a wood-grain pattern and a black watch on his left wrist. The background shows a blurred office environment with large windows and greenery outside.

**The pandemic validates the  
importance of zero trust.**

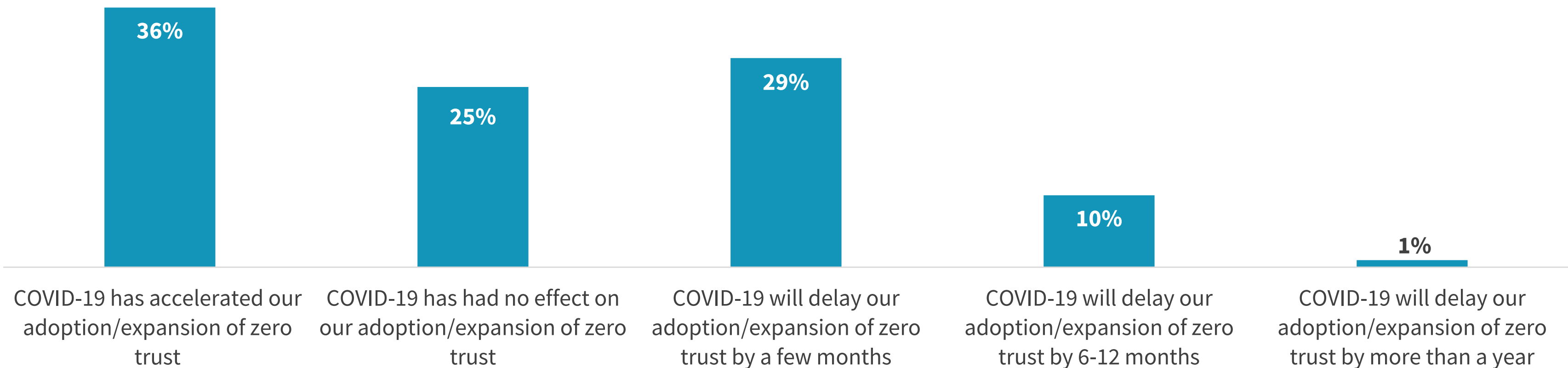


## COVID-19 Has Had A Minimal Negative Impact on Zero-trust Timing

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.”

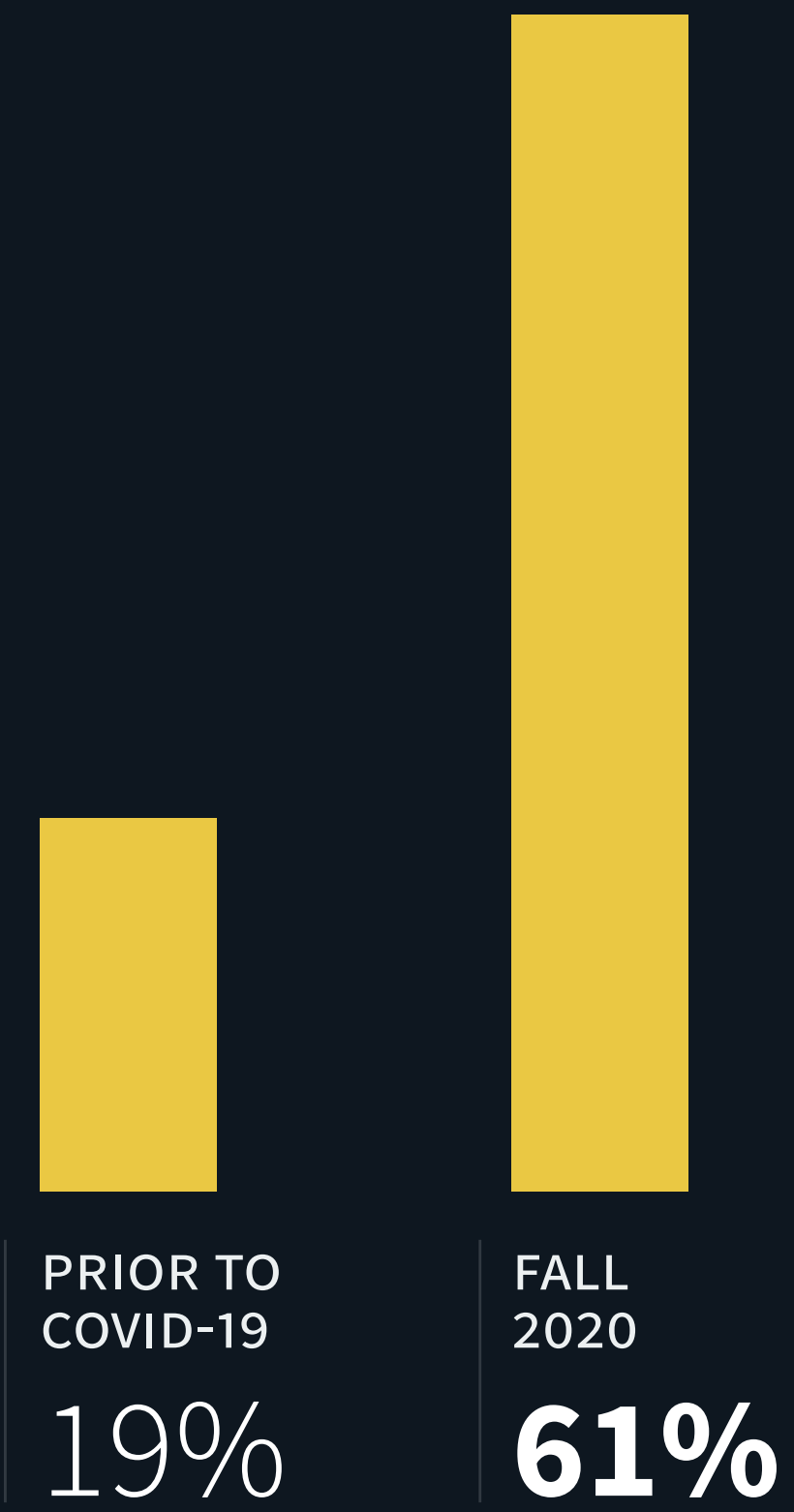
Impact of COVID-19 on zero-trust initiatives.





## Percentage of Remote Employees Has Tripled

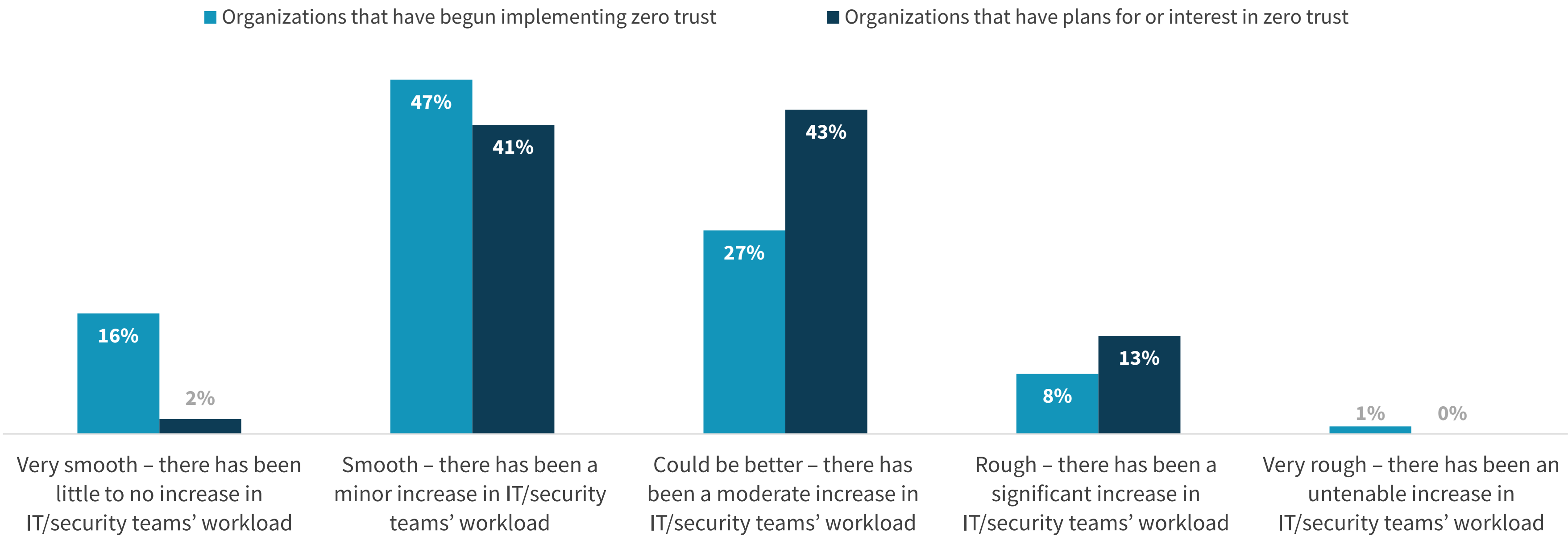
Percentage of total employees that are remote users.




## 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.







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



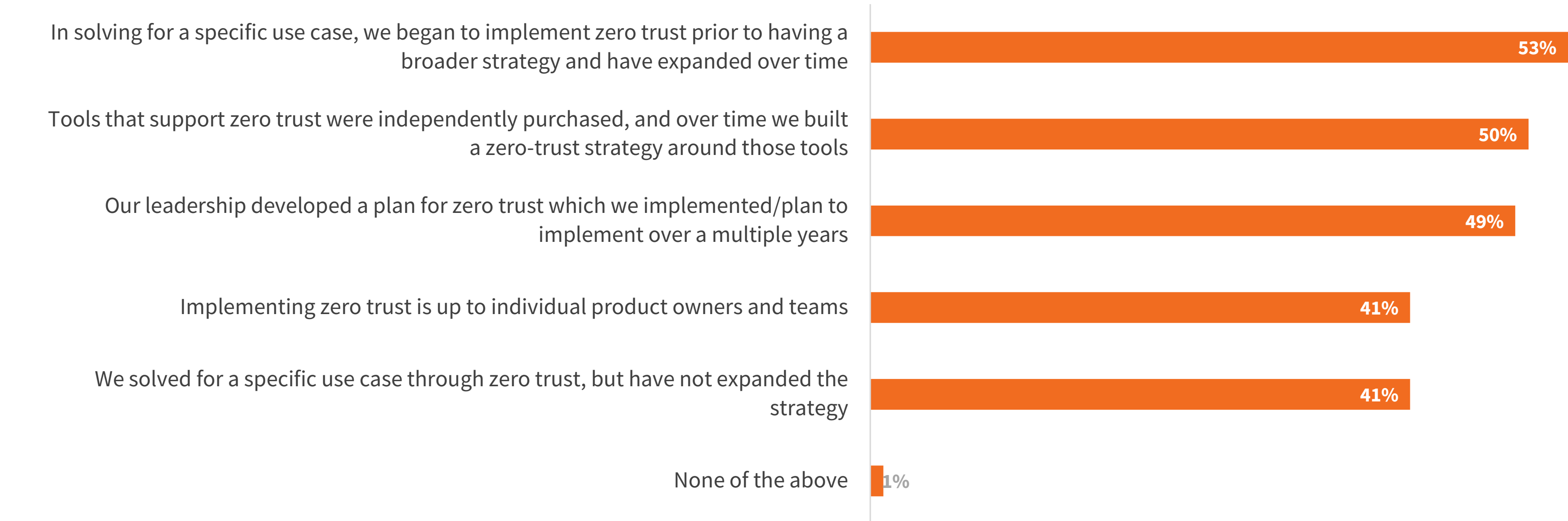
## Formalized Strategies Are Important But Often Not the Starting Point

Nearly all respondents at organizations that have begun to implement zero trust say they have a formalized, documented strategy that guides 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.



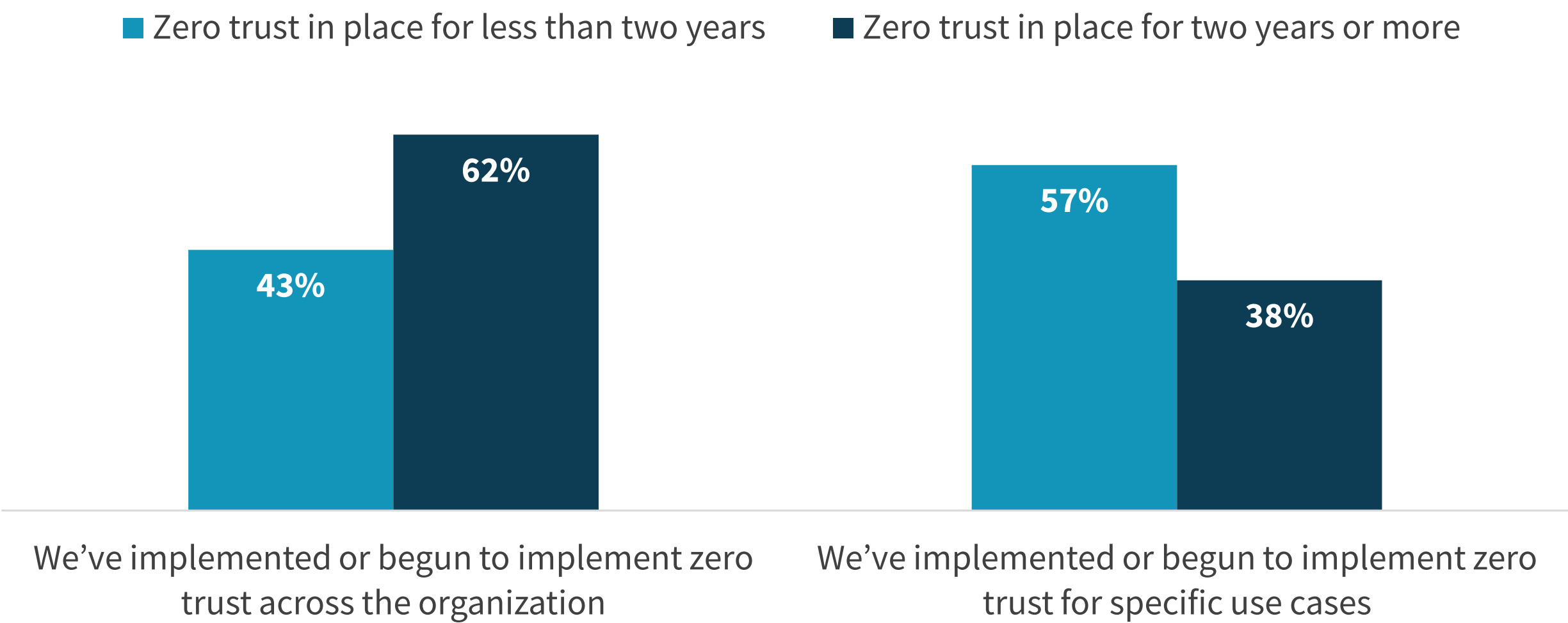
### Zero-trust experience.





“ **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.**



**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.





A woman with dark hair tied back, wearing glasses and a dark top, is shown in profile, looking at a computer screen. She is holding her glasses with her right hand. The background is dark, with the glow of the computer screen and other monitors visible. The text is overlaid on the left side of the image.

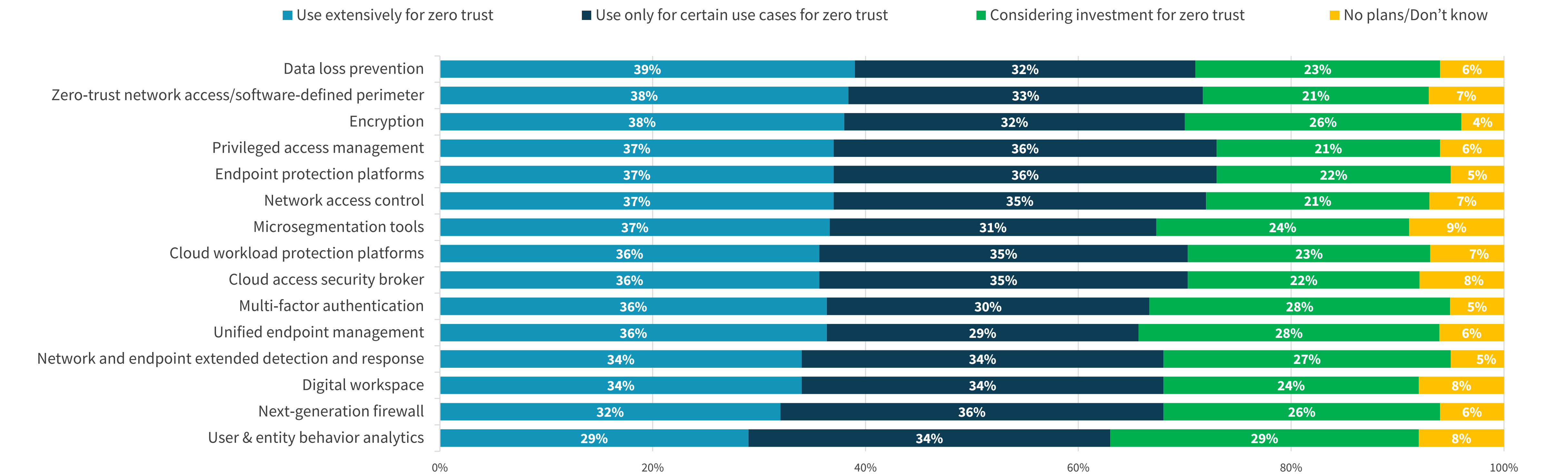
**The broad range of  
tools required for zero  
trust drives interest in a  
platform approach.**



## 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.

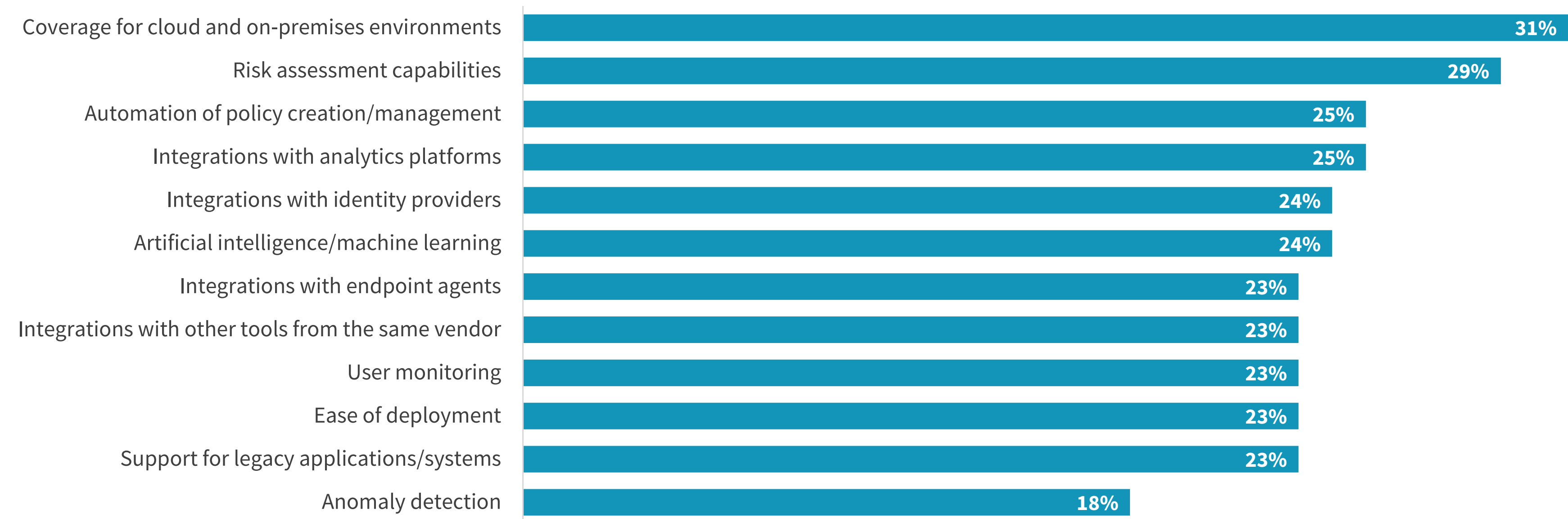




## Users Expect a Broad Range of Capabilities, Paving the Way for a Platform Approach

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.



## 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





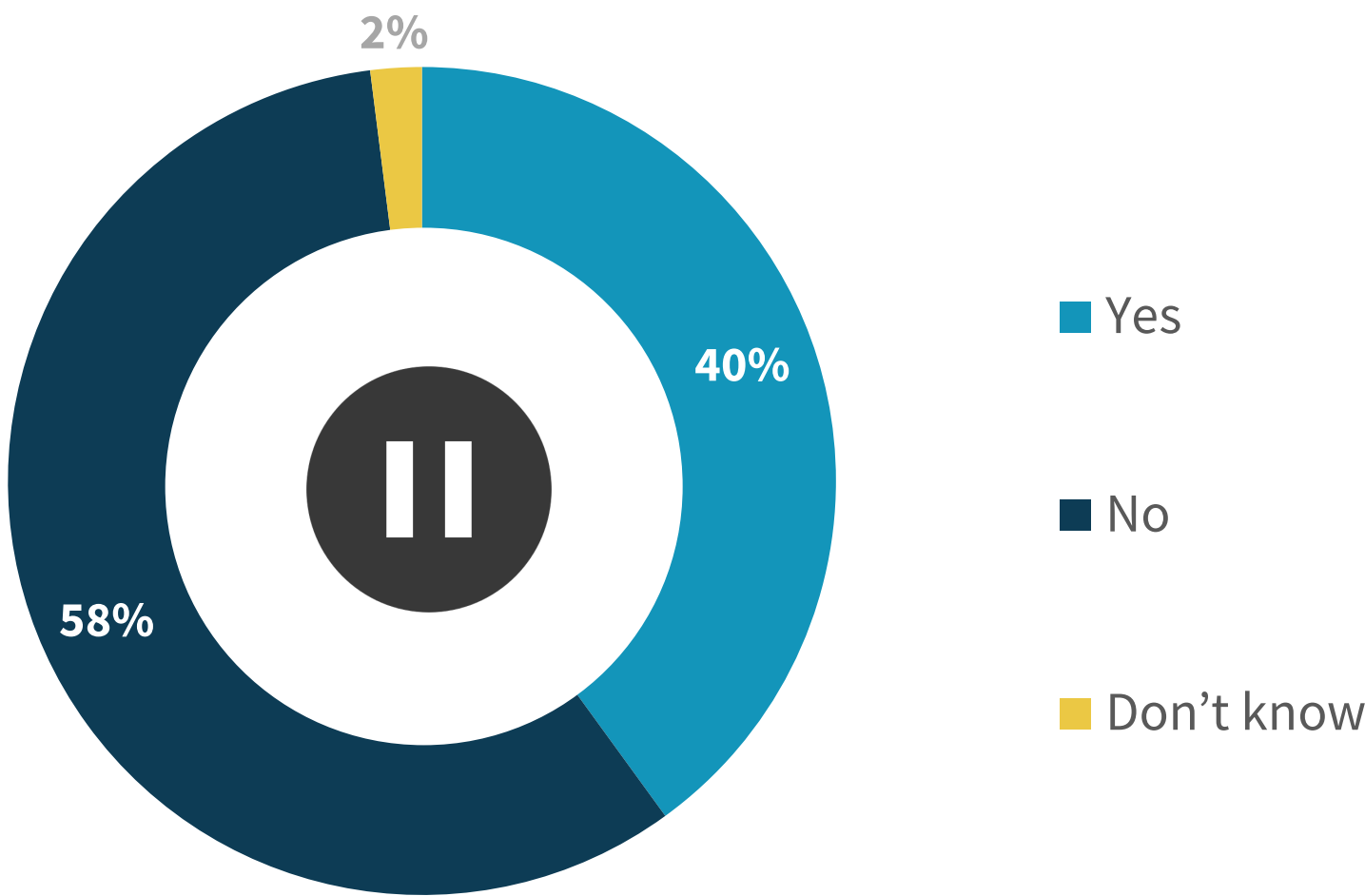
**Cross-functional collaboration  
is critical to zero-trust success  
and is leading to interest in  
centers of excellence.**



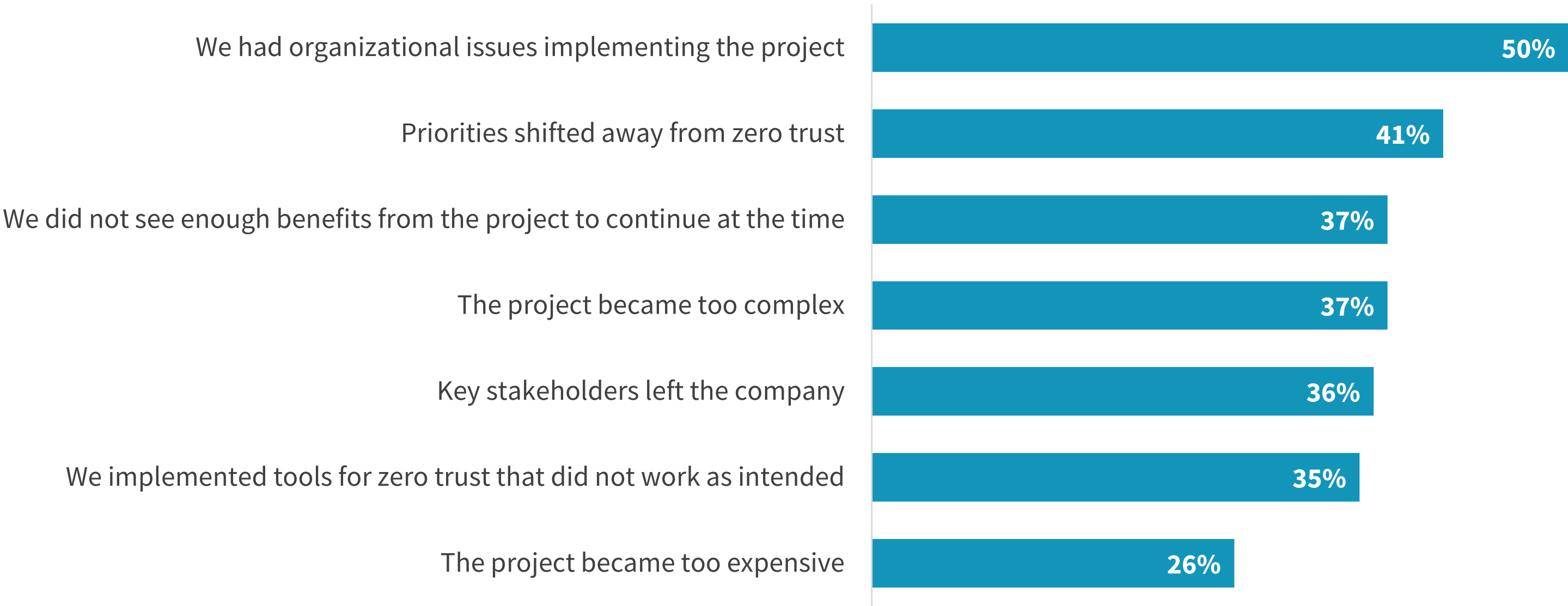
## False Starts Are Common, Often for Organizational Reasons

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?

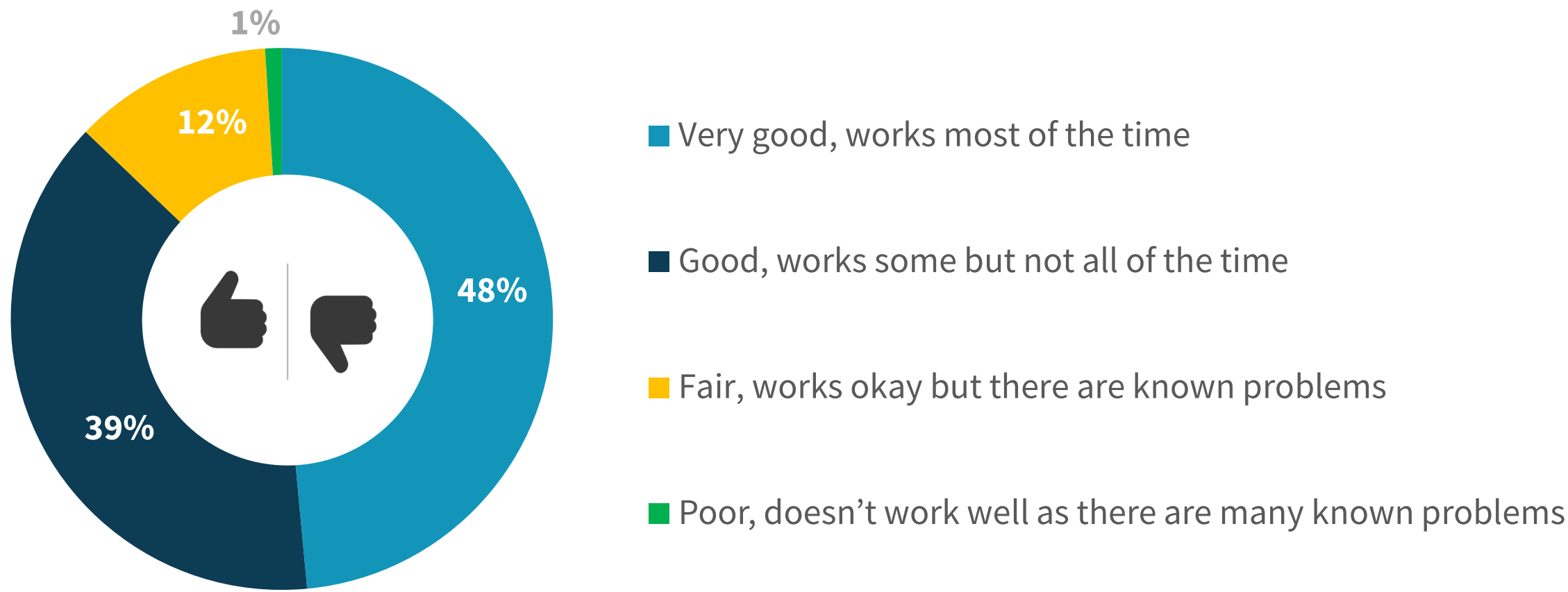


Reasons zero-trust projects were paused or abandoned.





Day-to-day zero-trust collaboration effectiveness.



Organizational challenges related to zero trust.



Zero-trust Collaboration Is Fairly Strong But Issues Do Exist

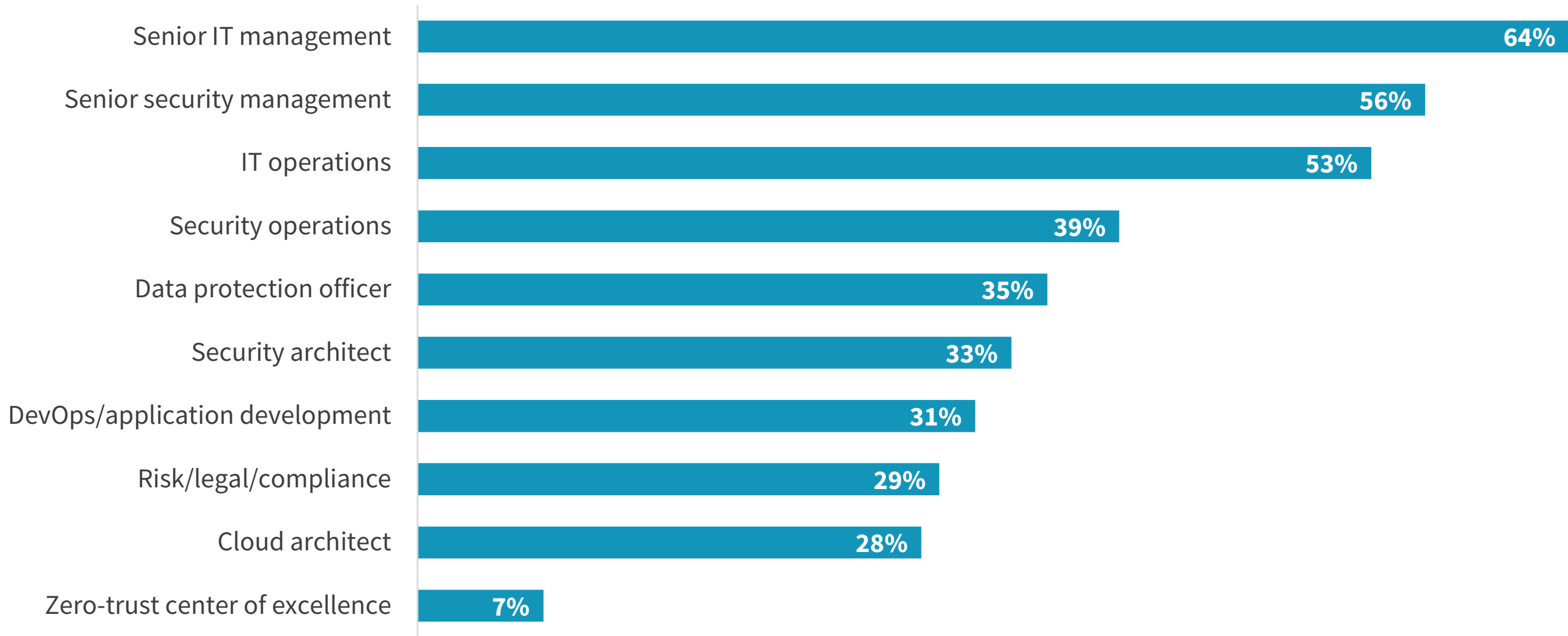
While many organizations report some level of success with the cross-functional collaboration across the different groups responsible for the strategy, technical evaluation, and decision making related to zero trust, challenges certainly remain. As with other areas of IT and security, communication is 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.



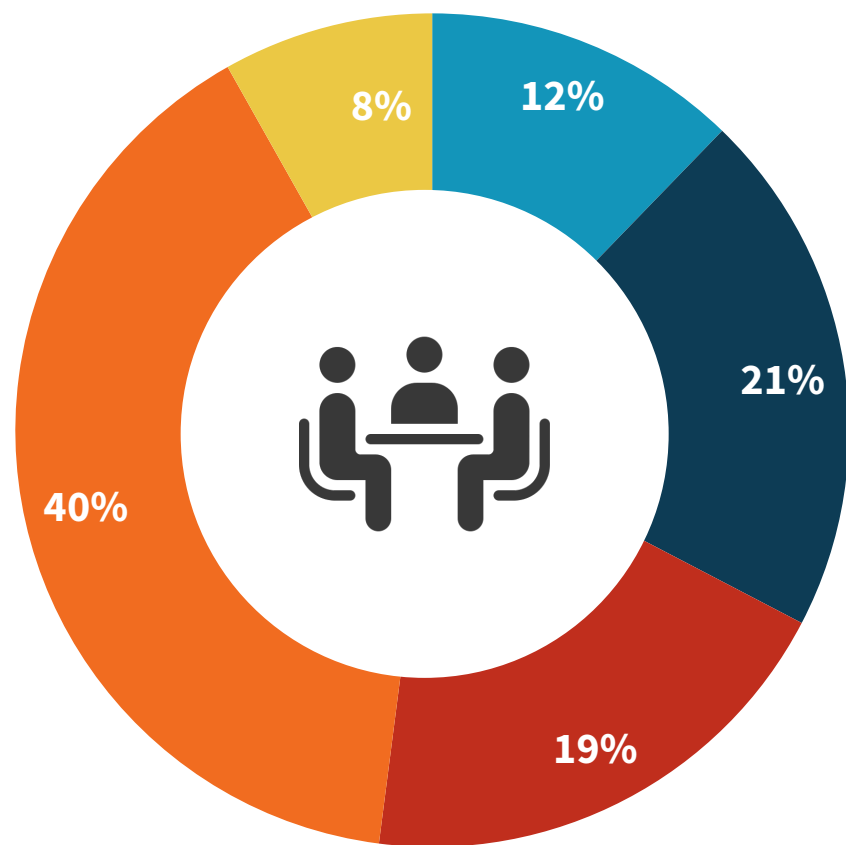
## There Is Early Interest in a Center-of-excellence Model to Formalize the Cross-functional Collaboration Required for Zero-trust Success

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.




### Interest in zero-trust centers of excellence.



- My organization has implemented a zero-trust center of excellence
- My organization is actively working to implement a zero-trust center of excellence
- My organization plans to implement a zero-trust center of excellence
- My organization is interested in implementing a zero-trust center of excellence
- 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.**

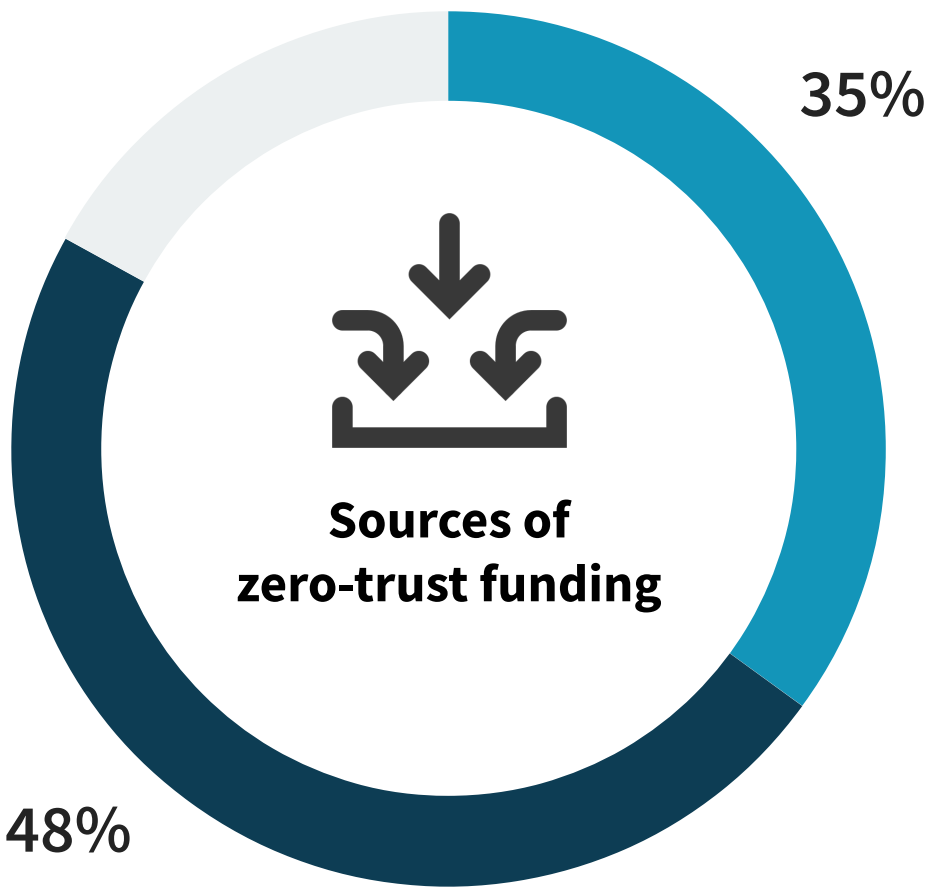


Budget Models Differ,  
but Zero-trust Funding is  
Typically Net-new

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.

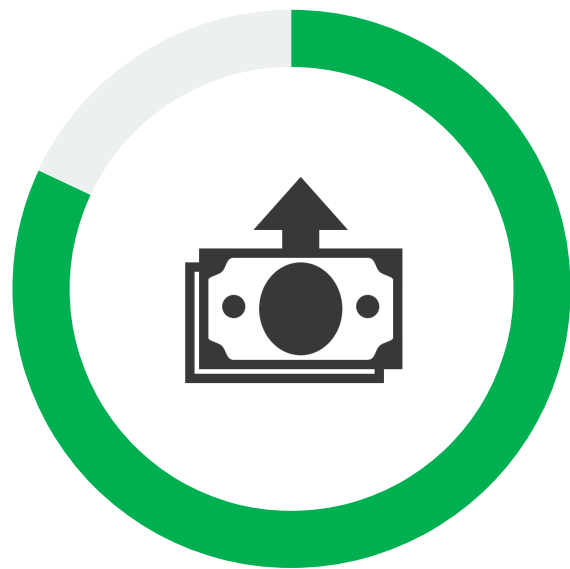


76%  
report net-new  
zero-trust funding



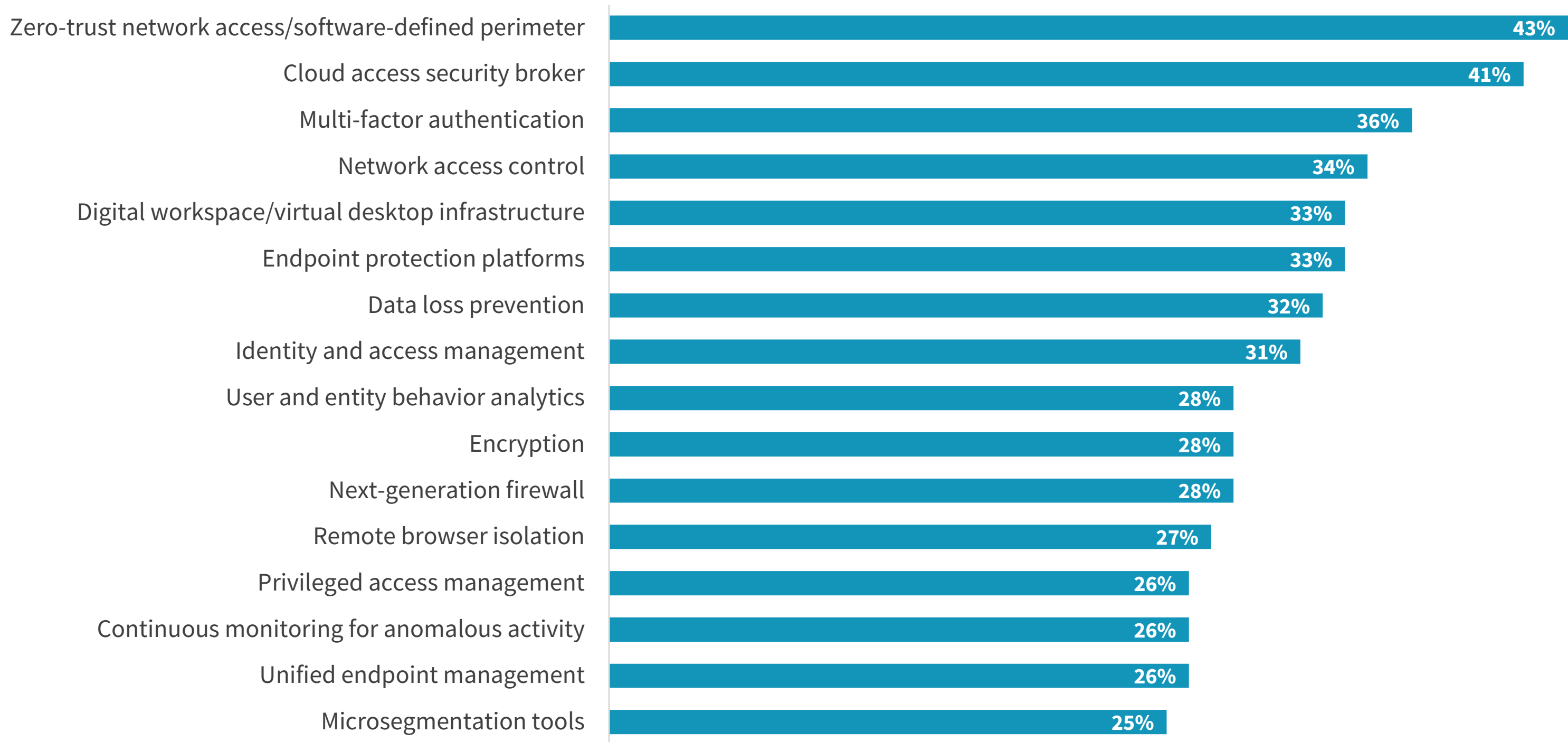
- A dedicated zero-trust program budget
- Discrete zero-trust budget within other security program budgets





**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.**



**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.





Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint’s humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

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.





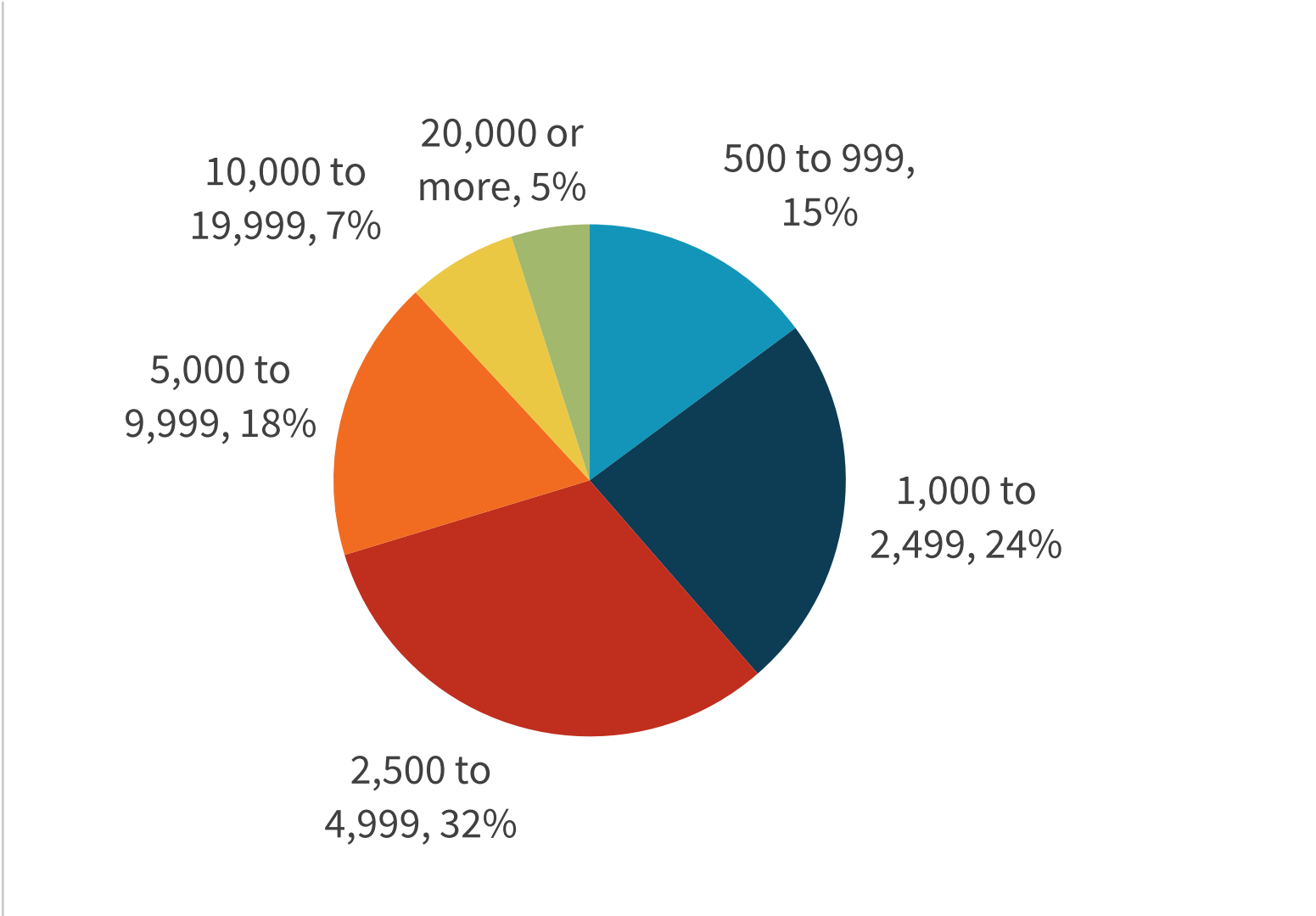
## Research Methodology

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.

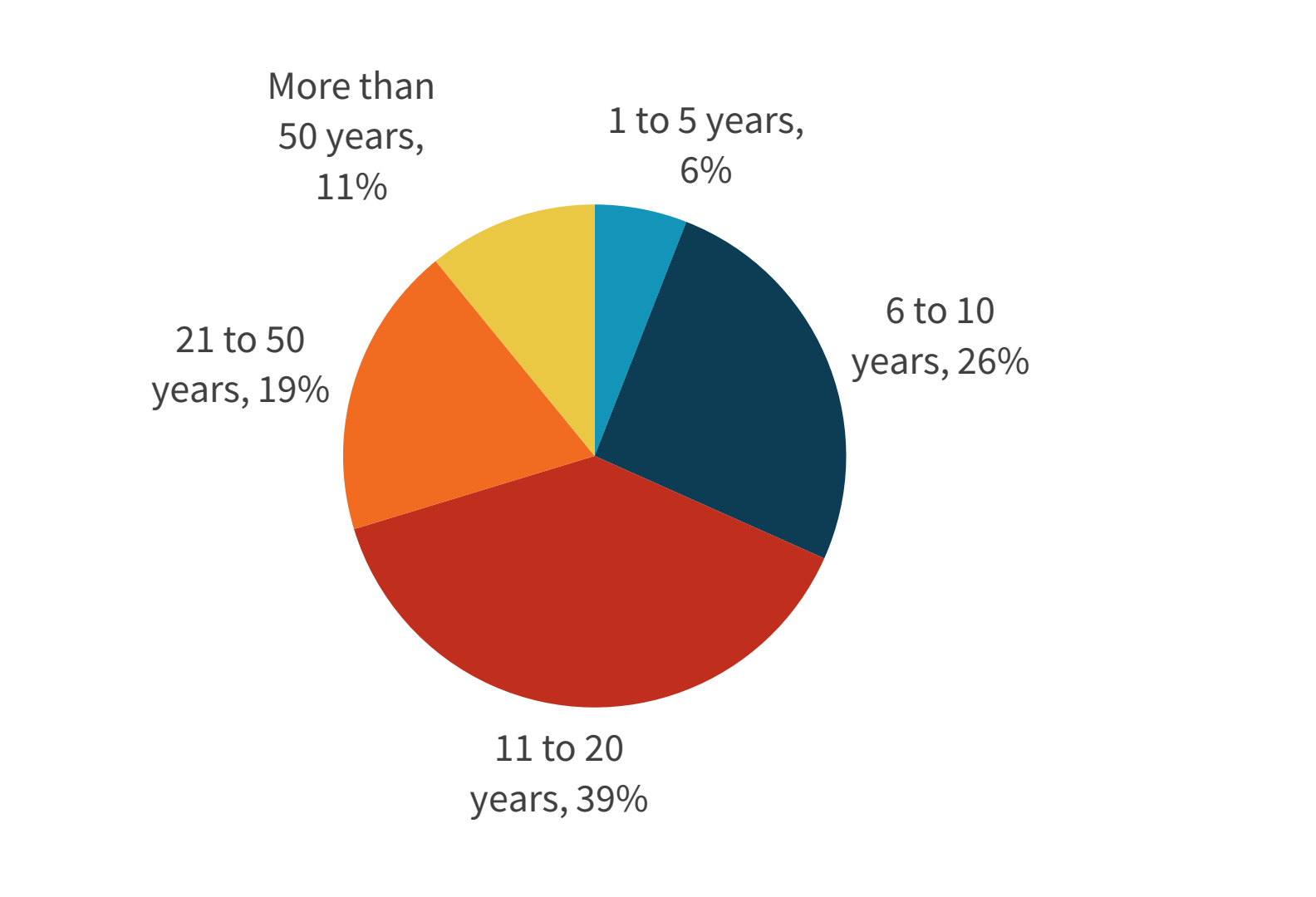
After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 421 IT and cybersecurity professionals.

Totals in figures and tables throughout this eBook may not add up to 100% due to rounding.

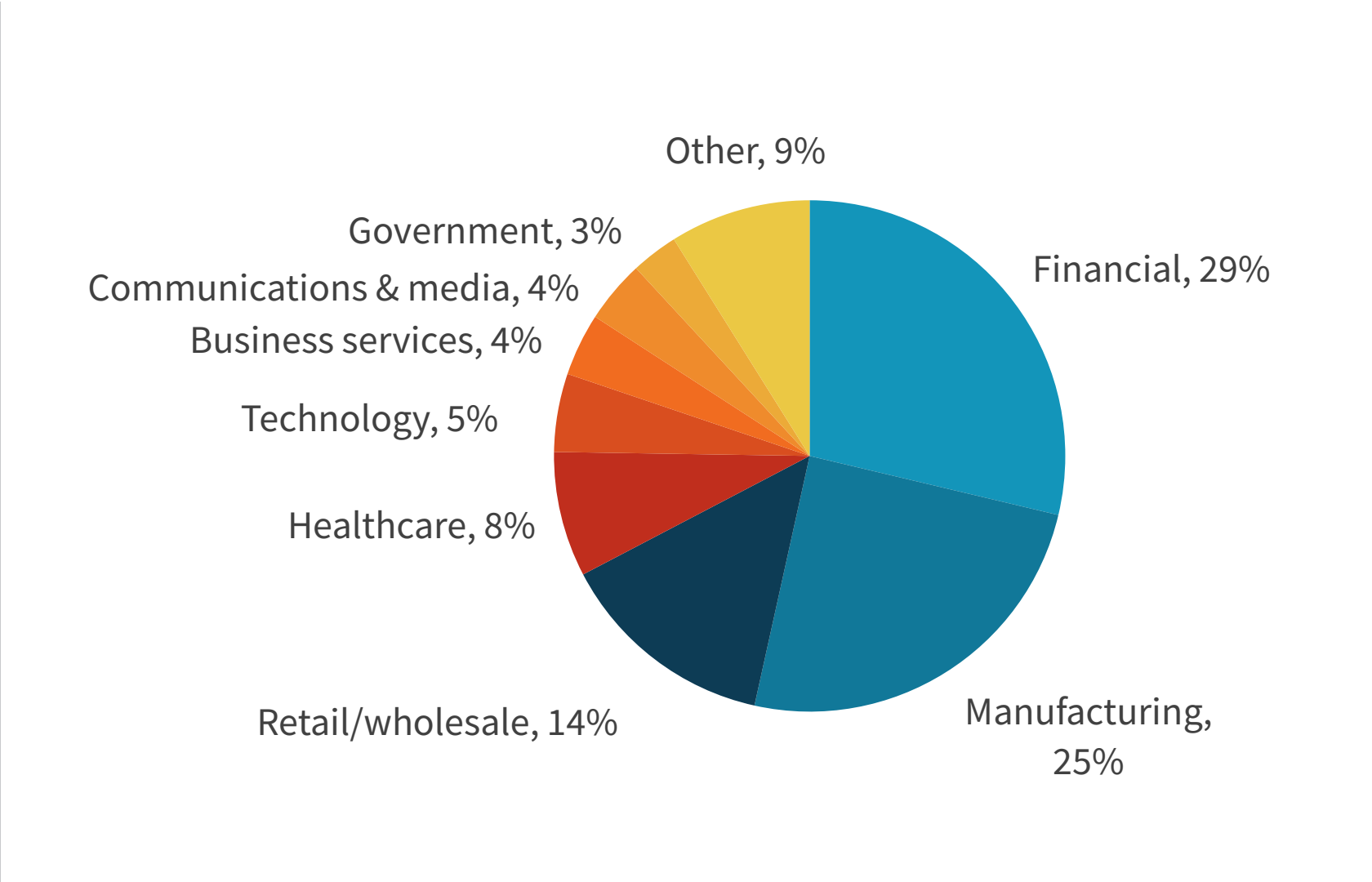
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF COMPANY



RESPONDENTS BY INDUSTRY





All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, 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 The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.



**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.