CSO Microsoft Security

SPONSORED CONTENT

Zero Trust security: **Lessons from early adopters**

Table of Contents

Introduction

The past two years of disruption have shaken up traditional IT and security models. As a result, Zero Trust security has quickly evolved from being an interesting concept to a foundation of modern enterprise security.

New research from Foundry finds that 52% of organizations are piloting or have deployed Zero Trust architecture, and another 15% are researching Zero Trust models. These adopters report numerous benefits from their deployments, including improved protection of customer data, reduction in complexity, and the delivery of secure, reliable access to corporate resources.

This e-book will explore the results of the Foundry research, which underscores the importance of a Zero Trust strategy for helping CISOs protect their organizations against a multitude of risks from numerous attack vectors. It also includes guidance on how to implement Zero Trust for those beginning their journey.

About the survey

Foundry surveyed US businesses in February and March 2022 to explore the current state of Zero Trust adoption. Respondents were required to be an IT manager or above at a company with 500+ employees and have a role in the purchase of cybersecurity products and services.

There were 250 total respondents for the 23-question survey.

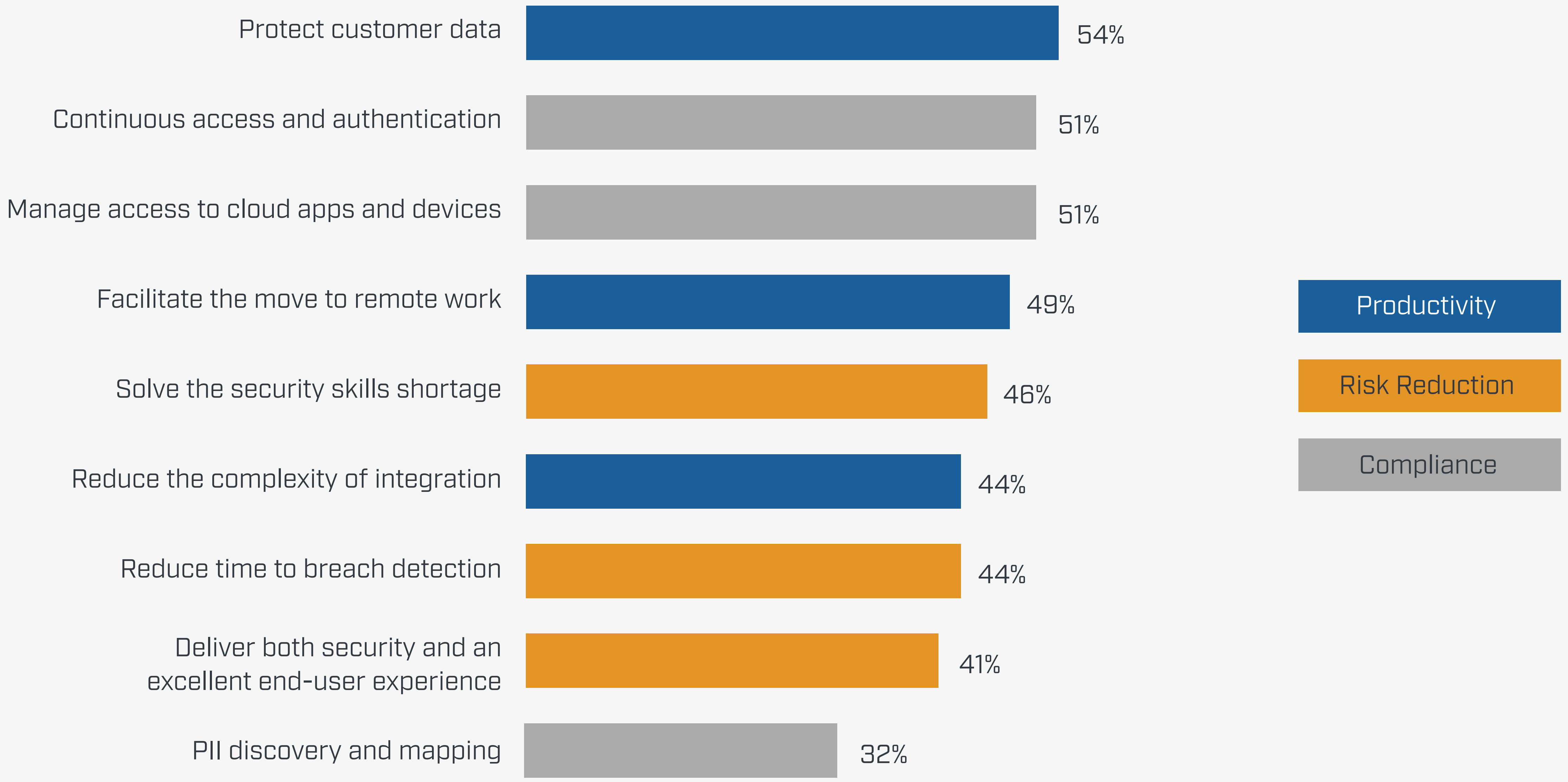
Zero Trust is here and it’s delivering value

It’s clear from the survey results, along with in-depth interviews with IT and security executives, that Zero Trust is top of mind at most organizations. And those that have deployed different Zero Trust components are already seeing the benefits.

Most respondents who have implemented Zero Trust (87%) say the architecture is delivering at or above their original objectives for implementation, adoption, and integration.

“[Zero Trust] has become a standard operating procedure for us. I can’t see us ever going back to the way we were before,” says an IT director for a global retailer. (Respondents were granted anonymity in exchange for talking freely about their security plans.)

Benefits captured since implementing Zero Trust



12% of respondents said they were achieving *all* of these benefits

Source: Zero Trust Adoption Survey, March 2022, Foundry. Base: 250

Some 44% of respondents also reported Zero Trust reduced the complexity inherent in implementing an integrated security architecture. “Since you’re dealing and working with a framework, it does make things less complicated,” says the CISO for a call center company with 3,500 employees.

A VP and CISO for a financial services firm with 17,000 employees says the multifactor authentication his company implemented as part of Zero Trust has been a hit with employees. “It has driven employee satisfaction up, actually, because now they don’t have to get on their company-provided machine and use a VPN client; they can get to resources from anywhere,” he says.

The concept of least privilege access has likewise paid dividends, the CISO notes. “We’ve had fewer catastrophic errors by system administrators because of the implementation of that privilege access system,” he says. “They get their privileges for specific things and specific timeframes, which means they’re less likely to make a mistake.”

Given the increased prevalence of phishing and other cyberattacks, the director of IT at the retail company sums up the benefits of Zero Trust this way: “If we didn’t have these types of tools, we would probably be in a bad situation and paying someone in bitcoin right now.”

CSO Microsoft Security

Drivers of Zero Trust deployment

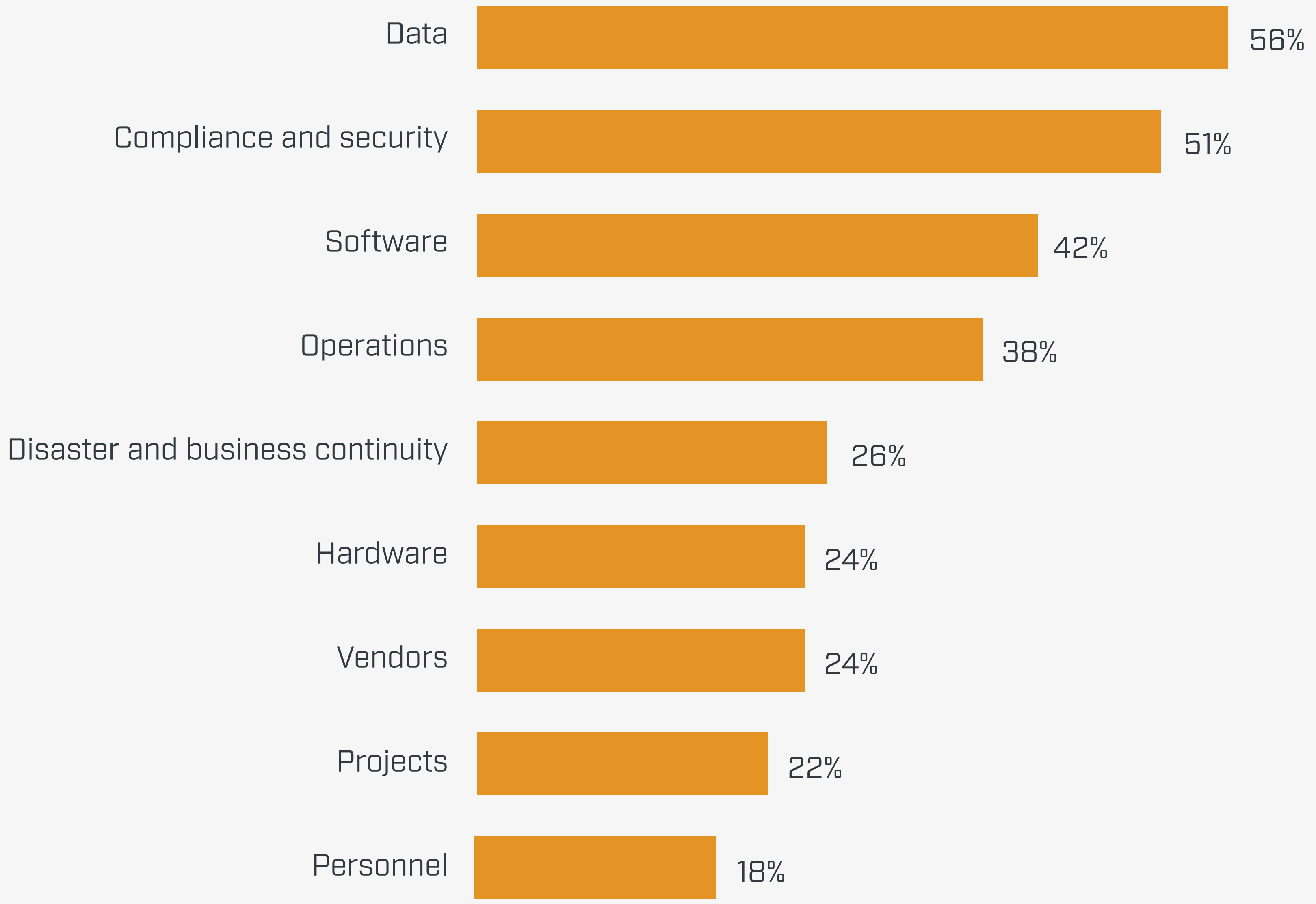
A confluence of events is driving companies to at least consider a Zero Trust architecture. At the top of the list is the need to manage risks to a multitude of resources against numerous threats. Survey respondents attributed a years' worth of security incidents to a number of causes, led by security vulnerabilities from third-party individuals or organizations. Other causes included:

- Unexpected business risks
- Misconfiguration of services or systems
- Malicious, intentional insider attacks
- Non-malicious user error, including phishing victims
- Compromised identities
- Unpatched software
- Stolen credentials

These incidents pose a variety of risks, led by data.

For many organizations, the sudden shift to remote work prompted by the pandemic accelerated adoption plans for Zero Trust, as traditional perimeter-based security models became obsolete. Many organizations had already been headed in that direction as they moved more applications and IT infrastructure to the cloud, but the pandemic provided an extra jolt.

Top categories at risk from cybersecurity threats



Source: Zero Trust Adoption Survey, March 2022, Foundry. Base: 250

For example, the CISO for a medical technology company with 1,700 employees says the cloud and the pandemic were drivers for his adopting Zero Trust, which now provides a secure foundation for whatever workplace model lies ahead.

“The business drivers were the fact that we’re a cloud-based company and needed to be able to secure our environment,” he says. “We also had to provide a capable remote workforce during the pandemic. [Zero Trust] has allowed us to dramatically reduce our real estate footprint, and we’re likely going to remain at least a 60% virtual remote company.”

No shortage of threats

Compliance needs have also provided an impetus for more robust security models. “Regulators are watching us, and they expect us to continue to improve our security framework,” says the SVP of global information security for a financial services company with 290,000 employees.

Some organizations have proactively taken steps toward Zero Trust to avoid a high-profile breach putting them in the spotlight for the wrong reasons. “It was about being proactive and trying to stay out of the news,” says the CIO at a higher-ed institution with 3,500 employees. “There are some real horror stories of other local institutions of about our size that were down for a long time.”

Others have already experienced a serious cybersecurity incident, prompting them to quickly revisit their security strategy. After an insurance company with 6,000 employees suffered a ransomware attack that shut down the corporate network for two weeks, the mandate to adopt Zero Trust came directly from the CEO. “We turbocharged the implementation,” says the firm’s VP of IT development. “It was definitely best practices in the beginning, and then it really accelerated heavily after our ransomware attack.”

A cloud-based catalyst

The VP and CISO for a major financial services company says his team recognized the need for a new security architecture several years ago, as it began adopting more cloud-based resources and users became more mobile.

“We realized the traditional castle-and-moat security architecture that we had relied on in the past was not going to protect us from attackers going forward,” he says.

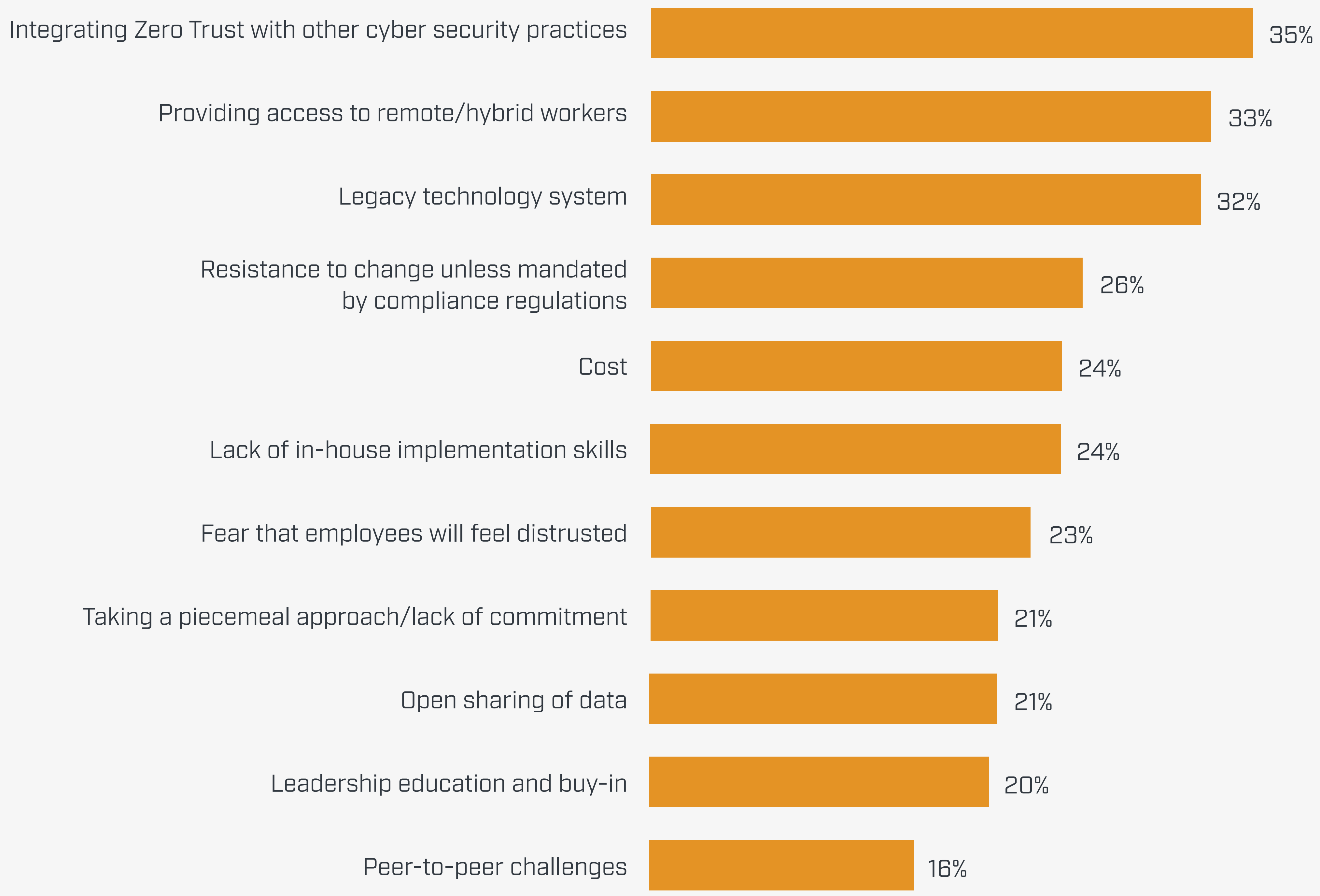
That reality became abundantly clear in early 2020, when the company discovered that sometime in the prior year an attacker had penetrated its perimeter and moved laterally within the environment without detection. “We needed a new architecture where we could protect and authenticate the use of those resources wherever they happen to reside, and Zero Trust is an architecture that’s designed to do that.”

Hurdles to Zero Trust adoption

For many organizations, Zero Trust represents a fundamental shift in security structure, process, and mindset—which explains some of the barriers they must overcome before adopting it.

“There were so many different silos we started hitting within the organization,” noted the call center CISO, explaining that server, network, and database teams each had its own contingent of web servers and tools. “That bogged us down because everybody had a different idea of where to go and how to do it.”

What’s holding back Zero Trust adoption?



Source: Zero Trust Adoption Survey, March 2022, Foundry. Base: 250

Unearthing such issues can actually be a positive side effect of Zero Trust, according to Anthony Mocny, senior product marketing manager for Zero Trust at Microsoft. “As an architecture, Zero Trust is designed to break down silos of security teams that live within technology pillars and help teams work together cohesively,” he says. “It may mean a cultural change as well, in terms of the way teams work together.”

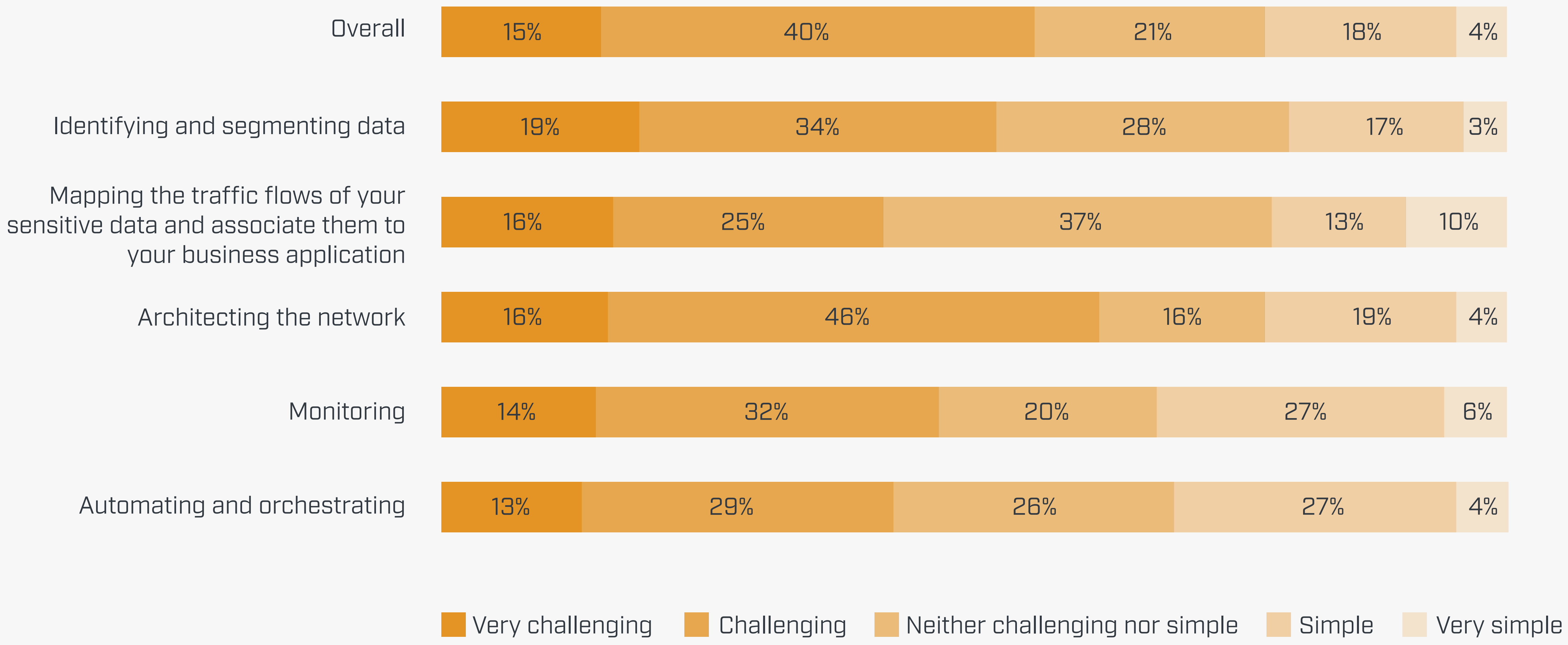
For the financial services VP/CISO, legacy applications were a hurdle to overcome on the road to Zero Trust. “They have to be retrofitted with modern authentication technology,” he says. “Depending on how old they are, that may not be a very easy thing to do.”

CSO Microsoft Security

Deployment challenges

Once companies embark on a Zero Trust journey, a variety of implementation challenges can also surface. More than half of survey respondents (56%) acknowledged that implementing Zero Trust was challenging or very challenging. Specifically:

How challenging is Zero Trust implementation?



Source: Zero Trust Adoption Survey, March 2022, Foundry. Base: 168

Challenges around segmentation and micro-segmentation came up frequently in the in-depth interviews.

“You’re segmenting your network down to the individual host,” says the financial services VP/CISO. “It’s like putting up a little firewall between every single host on the internal network so you can see all the traffic and control it right down to the individual machine. That has huge security benefits, but it’s super hard to implement because now you have to essentially manage tens of thousands of firewalls.”

Mapping traffic flows can be another multi-month process. For the CTO of a publishing and media company with 5,000 employees, after defining the critical data, application, and network services they needed to protect, “we mapped transaction flows along the network and tried to understand them as groups of information,” he says. “[We then] segmented portions of that information and how it actually transverses the network, even down to single packets of information.” At that point the company applied Zero Trust policies to each type of traffic flow. “We also built on new capabilities to monitor and maintain our network.”

Despite the challenges, many respondents believe Zero Trust ultimately simplifies day-to-day operations. With traditional technologies, “it takes days to make changes; you have to push them out across all the hardware and software components, and we’re using a lot of resources for that,” says the financial services SVP for global information security. “When we look at Zero Trust, it really minimizes the architectural complexity in the long run and reduces the number of employees we need to do the same type of work.”

Best practices for implementing Zero Trust

As more companies implement a Zero Trust architecture, they are developing roadmaps and best practices for others to follow. Here are five considerations when planning a deployment.

Don’t take on too much to start

Mapping out a Zero Trust strategy can be daunting if you view it only in the broad context of having to revise policies and protections across networks, data, applications, identities, endpoints, and infrastructure. “In the beginning it was just looking at this huge mountain to climb and we questioned if we were really going to do it,” says the higher-ed CIO. “You just have to take it one step at a time.”

The CIO and their team eventually adopted a “follow the money” approach, prioritizing the segmentation of finance and payroll applications on a separate network.

Identifying the most critical assets to protect is a sound approach, according to Mocny. “Be mindful of the reason you’re implementing Zero Trust in the first place,” he says.

When in doubt, start with multifactor

When prioritizing the security stack, many CISOs and security vendors recommend focusing initially on authentication and other identity-based protections. “If you don’t have a starting place in mind, multifactor authentication is a good place to look,” says Mocny. Microsoft estimates that multifactor authentication can prevent more than 90% of identity-based attacks.

The financial services VP/CISO agrees. “Authentication is a foundational element of implementing Zero Trust architecture. None of the other components work if you can’t validate the identity of the end user, so we started there.”

Next, the financial services VP/CISO tackled the networking component, which provided immediate benefits for supporting remote workers. The team left micro-segmentation until later in the journey because it’s not readily visible to the business at large. “When you’re done with it, you’re significantly more secure, but nobody knows the difference,” he says.

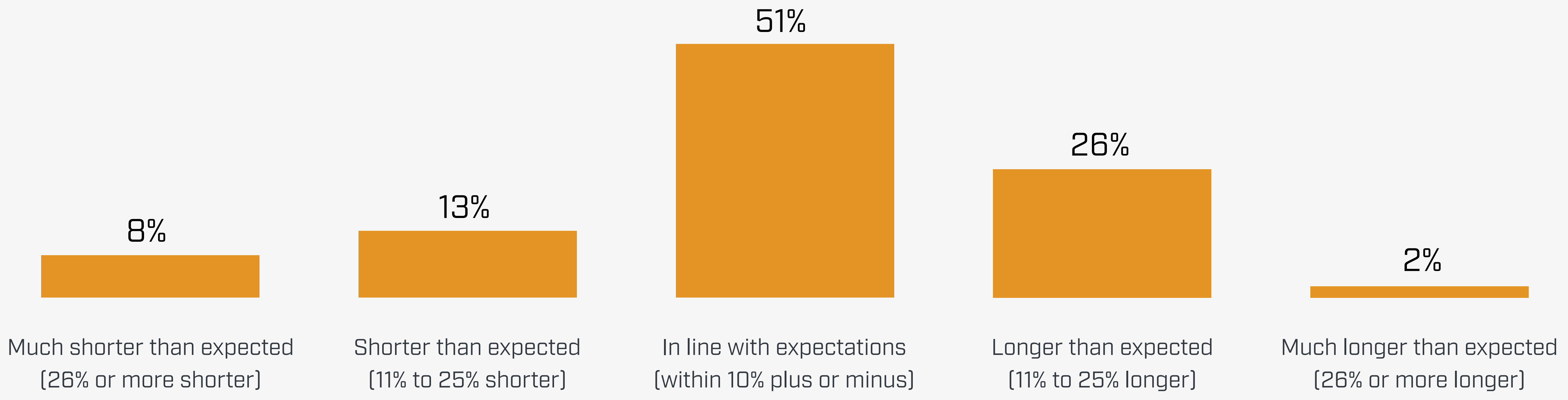
Be realistic about timelines

It's important that CISOs set realistic expectations about Zero Trust deployments. "Implementing a Zero Trust architecture is a program and not a project," says the financial services VP/CISO. "This was a huge change. Doing it right involves numerous projects, and it likely lasts for years; there's no quick and easy implementation of Zero Trust architecture."

His fellow financial SVP agrees. "I don't think we'll ever be done because there is always new technology coming out, there's always new malware coming out, there's always new threats coming out," he says.

The majority of survey respondents (72%) say their deployment timelines were either on track or proceeding ahead of plan, with the remainder saying implementation was taking longer than expected.

Is Zero Trust meeting your timeline objectives?



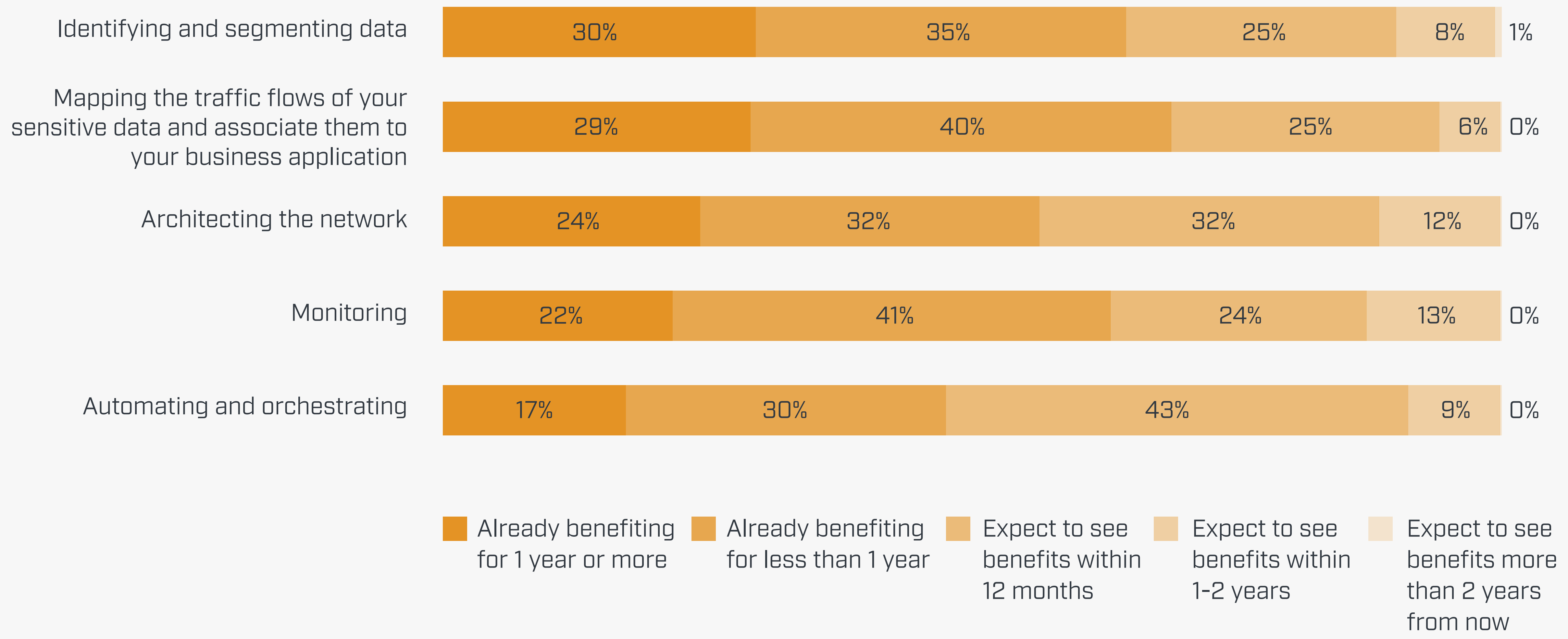
Source: Zero Trust Adoption Survey, March 2022, Foundry. Base: 168

Measure as you go

While a Zero Trust deployment is ongoing, CISOs can and should create milestones along the way to measure progress. It’s a good sign that around two-thirds of survey respondents say they were capturing benefits from most aspects of their projects within a year, and about another quarter or more expect to within 12 months, across key activities including identifying and segmenting data, mapping traffic flows, and architecting the network.

“Zero Trust is a journey because of the continuous evaluation you need to defend against the changing nature of attacks,” says Mocny. “Always be on the lookout for improvements.”

Timeline for capturing Zero Trust benefits



Source: Zero Trust Adoption Survey, March 2022, Foundry. Base: 103

Focus on people, not just technology

The broad reach of a Zero Trust security model impacts every employee, including the IT and security teams tasked with deploying it. That's why, as with any large technology project, it's important to make sure deployments are in sync with new processes and change management practices to ensure a smooth and successful rollout.

"In addition to a technology change, there's also a cultural change," says Mocny. "If you have multiple teams addressing security—including network architects or identity experts—you also need to change the way those teams work together. You need to break down silos to ensure technology all works together cohesively."

Eliminating silos involves getting teams across all of those disciplines closely involved in piloting and proof of concept (POC) projects. An IT systems director with a telecommunications company of approximately 2,000 employees learned that lesson after struggling with several single points of failure during deployment, including services that could not authenticate and were suddenly "untrusted," which rendered them as well as some systems unavailable.

"Deploying one service can have a domino effect and bring down others," he says. Going forward, "we are being much more careful—more POC time, more reviews, and more architectural reviews with subject matter experts before deploying."

Zero Trust ROI

A 2021 commissioned **Forrester Consulting Total Economic Impact™ study** quantifies cost savings and business benefits of Microsoft Zero Trust solutions. Based on the five enterprises Forrester interviewed, a composite organization realized a three-year return on investment of 92% by implementing a Zero Trust architecture with Microsoft.

This composite organization also saved an average of $20 per employee per month by obviating the need for security tools that became redundant under Zero Trust, including endpoint management, antivirus, and antimalware solutions.

CSO Microsoft Security

Where are you on the path to Zero Trust?

As the survey indicates, the benefits of a Zero Trust security model clearly outweigh some of the deployment challenges CISOs and their security teams are facing. Meeting these challenges with a well thought out plan can help your organization quickly improve protections, reduce risk, and begin delivering value across the business.

To evaluate your organization's Zero Trust maturity level and see more practical deployment resources, take Microsoft's **Zero Trust maturity model assessment**.