Enterprise
Strategy Group™
by TechTarget

Simplifying Zero Trust for AWS With Okta and Palo Alto Networks

John Grady | Principal Analyst

ENTERPRISE STRATEGY GROUP

AUGUST 2024

This Enterprise Strategy Group eBook was commissioned by Amazon Web Services, Okta, and Palo Alto Networks and is distributed under license from TechTarget, Inc.

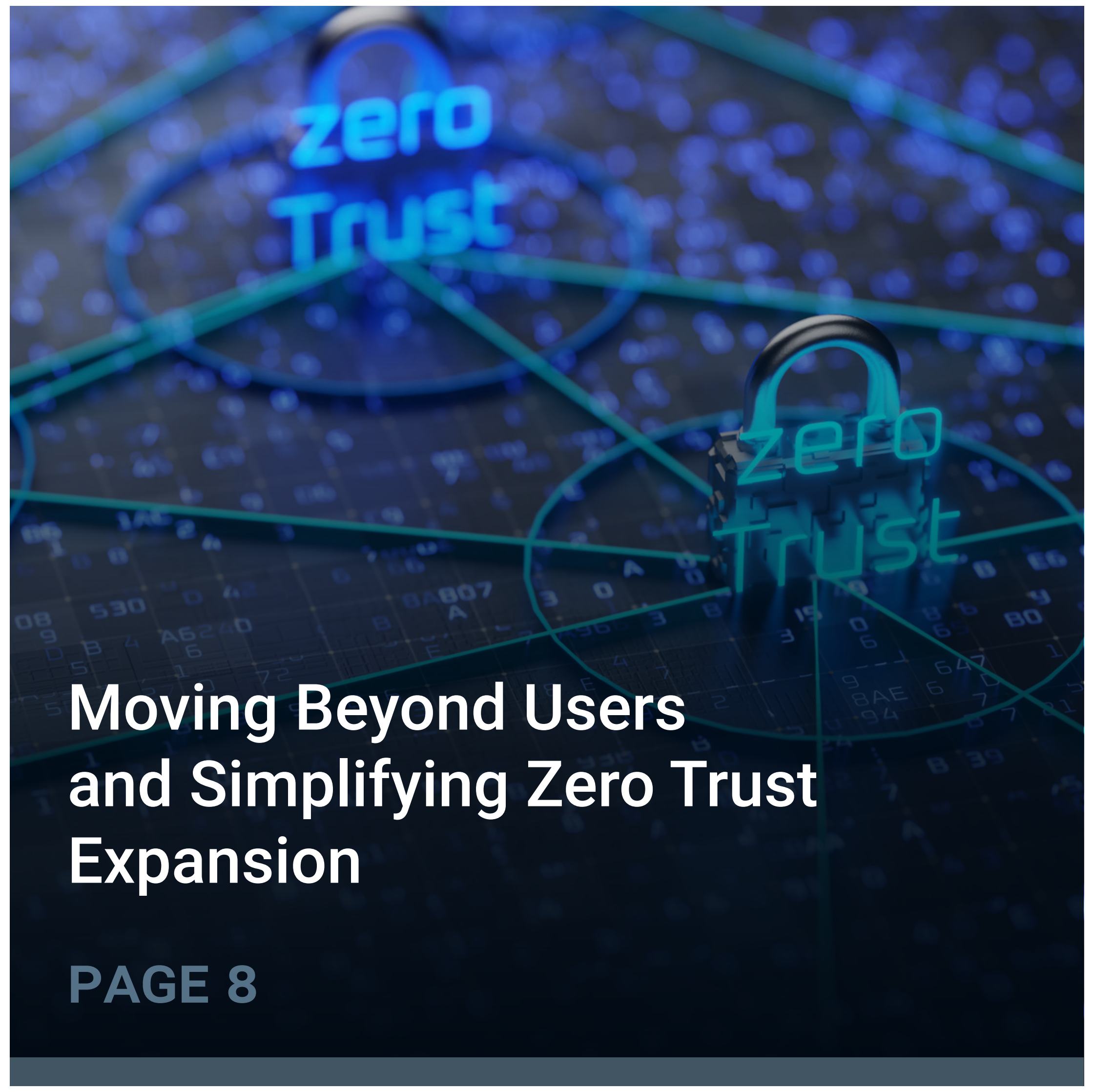
> "Zero Trust strategies **are more important than ever**."

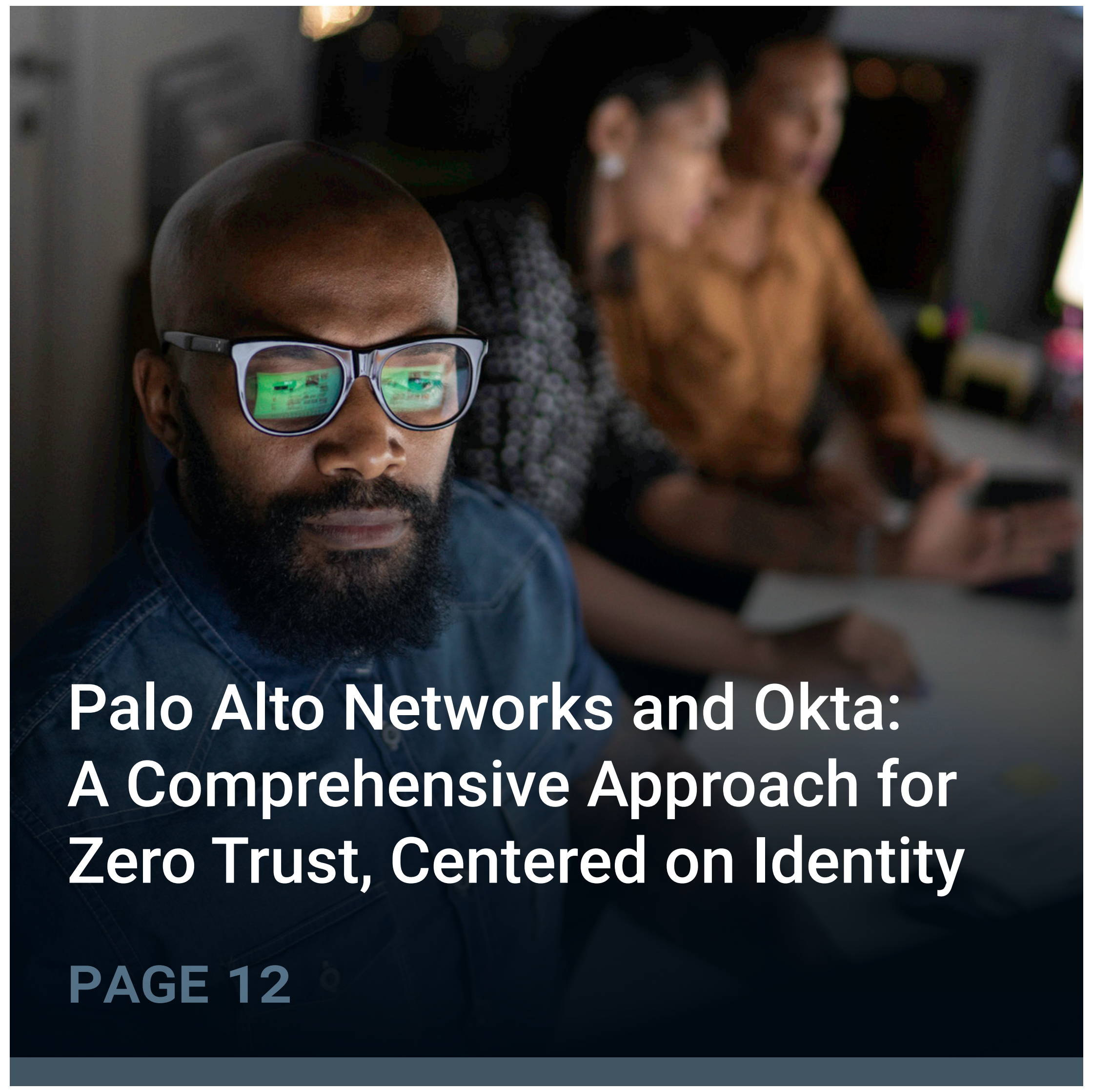
John Grady | Principal Analyst
ENTERPRISE STRATEGY GROUP

Introduction

Zero Trust strategies are more important than ever as organizations contend with the intersection of distributed users and resources with increasingly sophisticated attacks. While there is common agreement on this point, the breadth of Zero Trust leads many to focus on particular use cases or tenets of the strategy. The difficulty of integrating tools to consistently apply policies across the environment exacerbates this issue. Palo Alto Networks and Okta have partnered with Amazon Web Services (AWS) to provide customers with deep technical integrations to help them apply least-privilege access and continuous authentication with less complexity. This ensures a smaller attack surface and more confidence to accelerate cloud migration.

CONTENTS





Organizations Approach Zero Trust for Different Reasons and in Different Ways
PAGE 3

Moving Beyond Users and Simplifying Zero Trust Expansion
PAGE 8

Palo Alto Networks and Okta: A Comprehensive Approach for Zero Trust, Centered on Identity
PAGE 12

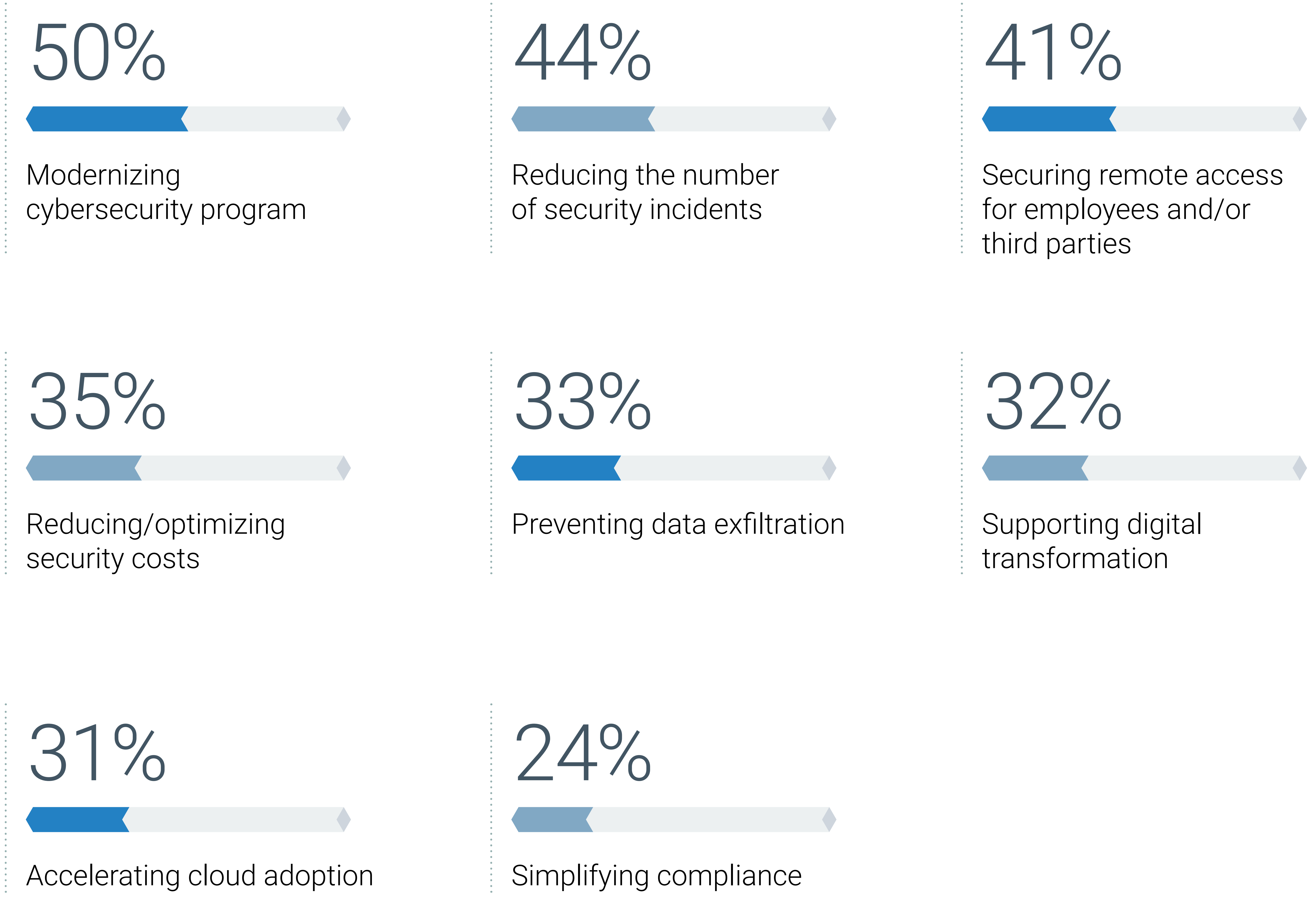
Organizations Approach Zero Trust for Different Reasons and in Different Ways

Organizations Turn to Zero Trust for Both Strategic and Tactical Reasons

Organizations turn to Zero Trust for a variety of reasons. Research from TechTarget's Enterprise Strategy Group has found organizations point to both strategic and tactical drivers for Zero Trust adoption. On the tactical side, improving security effectiveness is a main driver, with 44% adopting Zero Trust to reduce the number of incidents they must respond to and 33% doing so to prevent data exfiltration (see Figure 1).[1] Similarly, improving secure remote access (41%) has also become a common forcing function as organizations contend with hybrid work models that render traditional location-based and static security models ineffective.

From a strategic perspective, some organizations look to Zero Trust to support digital transformation (32%) or accelerate cloud adoption (31%). Yet the most common reason given for interest in Zero Trust is overall security program modernization, cited by 50% of respondents. Traditional, perimeter-based security approaches that enforce policy based on location and IP address result in users and resources being granted excessive trust based simply on where they are. As enterprise IT environments have fundamentally changed, with users accessing resources from outside of corporate locations and workloads increasingly residing in cloud environments, the risk associated with this model has become clear. Zero Trust solves these issues by denying access by default and enforcing least-privilege access through continuous authentication, authorization, risk evaluation, and monitoring for every request.

Figure 1. Top Drivers of Zero Trust



[1] Source: Enterprise Strategy Group Research Report, *Trends in Zero Trust Strategies and Practices Remain Fragmented, but Many Are Seeing Success*, March 2024. All Enterprise Strategy Group research references are from this report.

Critical Zero Trust Practices, Especially Around Identity, Are Still Lacking

Depending on the Zero Trust use cases an organization supports, the specific practices used could vary. However, there are foundational aspects that are applicable to multiple use cases and, ideally, should be broadly implemented. Yet, perhaps due to the challenges discussed, most organizations say they have not broadly implemented some of the most critical Zero Trust practices (see Figure 2). Specifically:

ONLY **49%**

have broadly employed multiple factors of authentication for all users.

ONLY **47%**

have broadly implemented a conditional access model that assesses risk factors before granting access.

ONLY **44%**

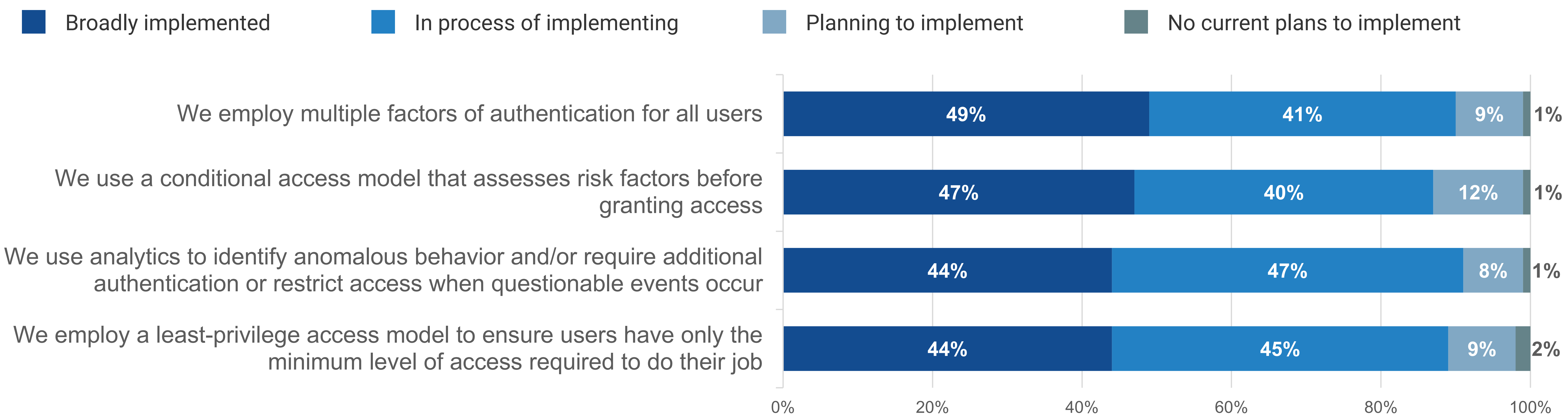
have broadly implemented analytics to identify anomalous behavior and/or require additional authentication or restrict access when questionable events occur.

ONLY **44%**

have broadly implemented a least-privilege access model to ensure users have only the minimum level of access required to do their job.

The good news is that many organizations said they are in the process of implementing across most of these areas, but help is clearly needed. One potential reason for this lack of broad adoption is the fact that, in most cases, the vendors offering identity capabilities are separate from those providing network, data, and workload security. An additional factor is that many vendors focus on specific use cases or Zero Trust pillars, requiring a lot of cross-vendor integration for broad implementation.

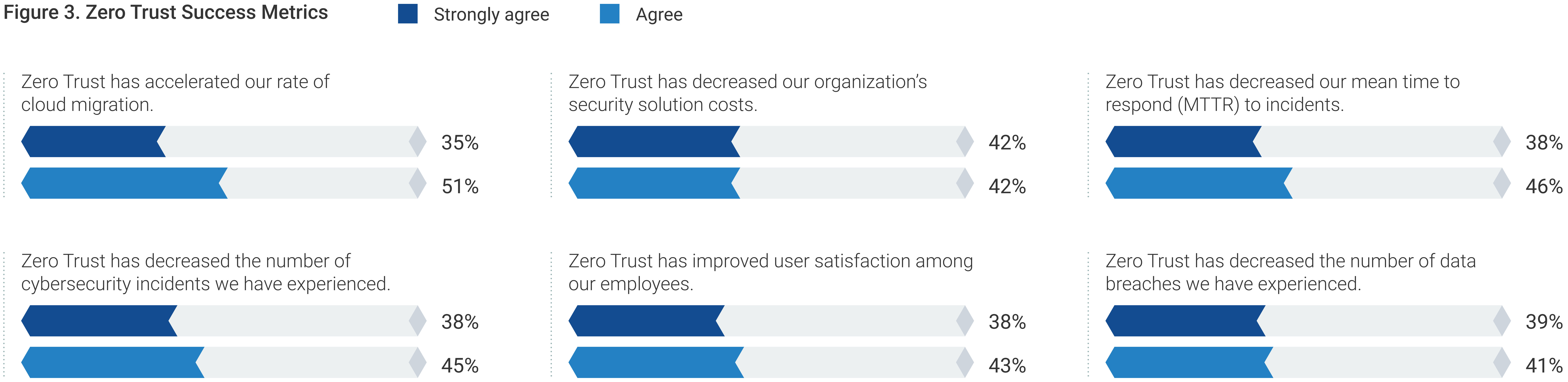
Figure 2. Progress With Zero Trust Practices



Early Adopters Are Seeing Success, but There Is Room for Improvement

The concept of Zero Trust has become fairly well known over the last few years, but adoption is far from universal. Concerns about costs, complexity, and friction can hold some organizations back from moving forward with Zero Trust initiatives. Organizations in this situation should consider the feedback from early adopters on the success they have seen. More than one-third of Enterprise Strategy Group research respondents strongly agreed that Zero Trust has helped accelerate cloud migration, decrease security costs, lower mean time to respond, reduce the number of cybersecurity incidents, improve user satisfaction, and reduce data breaches (see Figure 3). While this feedback shows great progress, it still leaves many organizations that could see more improvement in these areas over time; organizations seeing more moderate success can try to advance their Zero Trust progress by optimizing initiatives and expanding into adjacent use cases.

Figure 3. Zero Trust Success Metrics



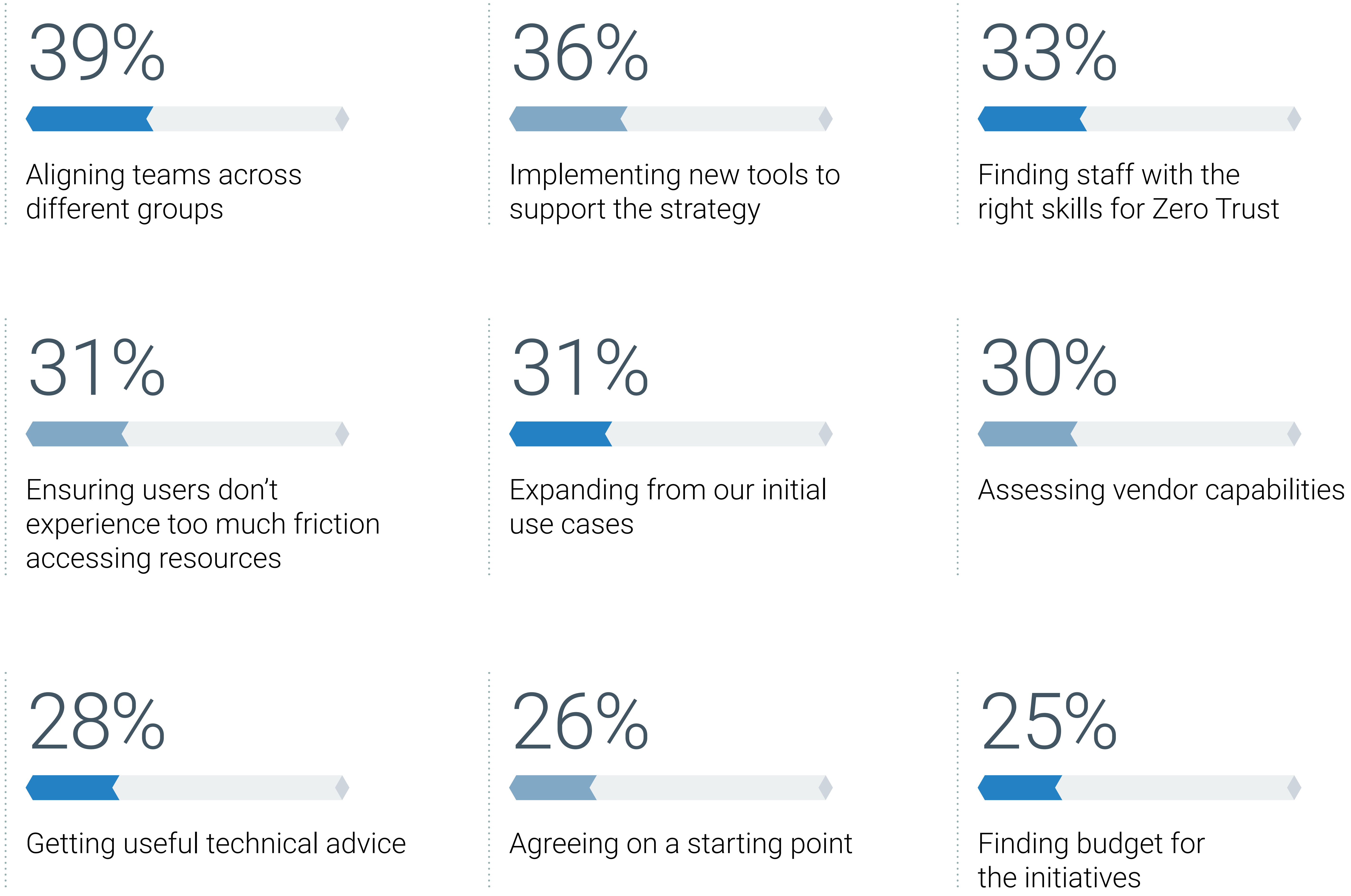
Challenges Across People, Process, and Technology Are Common With Zero Trust

There are a number of challenges across the people, processes, and technology involved in Zero Trust initiatives that can limit the success of the initiative. The most common challenge is aligning teams across different groups, cited by 39% of research respondents (see Figure 4). The cross-functional nature of Zero Trust means a variety of roles across security and IT are involved in the project. This becomes even more pronounced when it comes to the public cloud and cloud architects, cloud operations teams, and the lines of business involved. In a related finding, 33% said finding staff with the right skills for Zero Trust is a challenge.

While Zero Trust is a strategy, technology is ultimately needed to enforce the policies put in place. Sometimes existing tools can be applied for Zero Trust, but when new tools are needed to provide missing capabilities, implementation can become an issue. This was cited as a challenge by 36% of organizations. More than just implementation, integrating solutions with the existing tools and infrastructure in place can be difficult as well.

Finally, many organizations begin their Zero Trust journey by focusing on a specific use case to try to show value to the business and build momentum for the project. However, expanding from that starting point can be difficult, not only in terms of developing consensus for the next area of focus, but also in terms of expanding technologies to new use cases. This difficulty can occur when proper planning is not done at the outset or when technologies that focus on a narrow set of Zero Trust use cases are selected.

Figure 4. Top Challenges of Zero Trust Initiatives



BACK TO CONTENTS

Moving Beyond Users and Simplifying Zero Trust Expansion

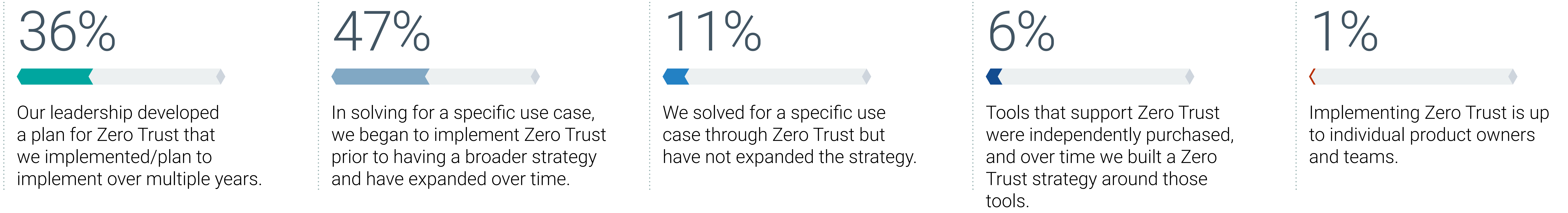
Proper Planning Pays Dividends

So, what can organizations do to achieve greater success with their Zero Trust initiatives? First and foremost, planning for the long term can help immensely. Many organizations report ad hoc adoption of Zero Trust (see Figure 5). In other words, there is not necessarily a master plan being followed that lays out the specific order in which the initiative will be applied across different parts of the environment or Zero Trust pillars. While starting with a narrow focus can help show value and build momentum, this should be done with an eye toward the future as well. There should be a balance between short-term implementation and the longer-term vision. In fact, 46% of respondents who indicated their leadership developed a plan for Zero Trust that was implemented over multiple years said the project met all the outcomes they expected. Conversely, only 16% of those who began to implement Zero Trust prior to having a broader strategy said Zero Trust met all the outcomes they expected.

Many organizations focus on users and improving secure access to corporate resources, if only because it is a strategic imperative due to changing work models. Yet Zero Trust is just as applicable to securing IoT devices, protecting cloud environments, supporting threat detection and response, and more. This means that organizations that don’t lay out a blueprint for their Zero Trust journey need to be more flexible and agile to adjust on the fly. This can either be supported or inhibited by the tools they choose to support their Zero Trust project.

> “46% of respondents who indicated their leadership developed a plan for Zero Trust that **was implemented over multiple years said the project met all the outcomes they expected.”**

Figure 5. Strategy for Zero Trust Implementation



Our leadership developed a plan for Zero Trust that we implemented/plan to implement over multiple years.

In solving for a specific use case, we began to implement Zero Trust prior to having a broader strategy and have expanded over time.

We solved for a specific use case through Zero Trust but have not expanded the strategy.

Tools that support Zero Trust were independently purchased, and over time we built a Zero Trust strategy around those tools.

Implementing Zero Trust is up to individual product owners and teams.

The Goals of Consistency and Ease of Use Highlight the Need for a Platform Approach

From a technology perspective, there are a handful of key attributes that can enable an expanding Zero Trust journey over time. Aside from strong security capabilities leveraging artificial intelligence, assessing risk, and detecting anomalies, many of the most desired attributes for tools supporting Zero Trust cited by Enterprise Strategy Group research respondents highlight the need for a simplified solution that consolidates tools and follows a platform approach.

Specifically, this solution must include the following attributes:

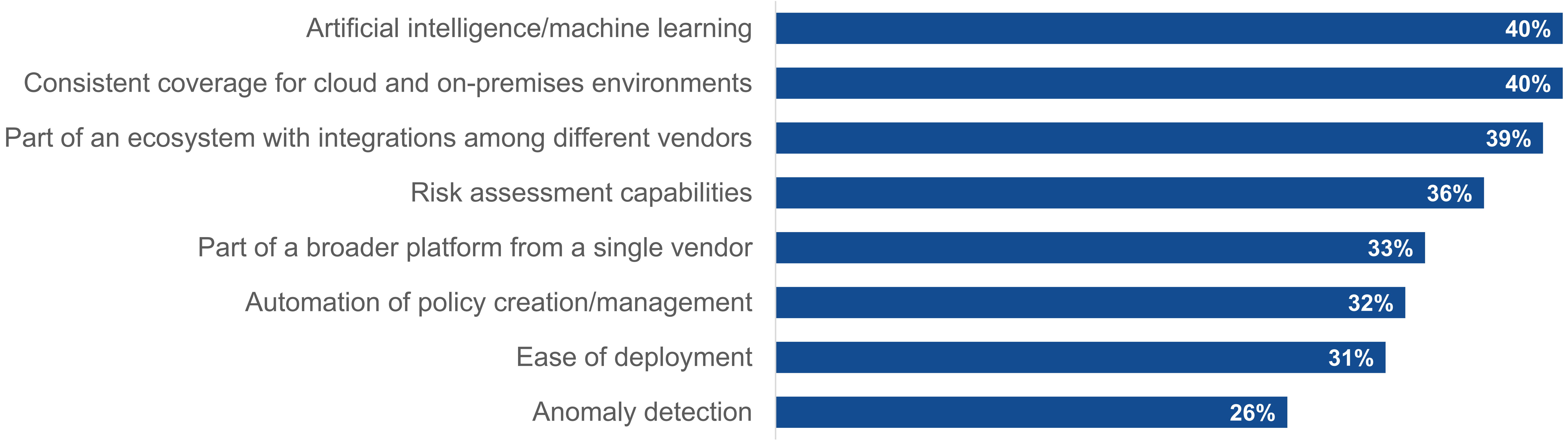
Consistent coverage across cloud and on-premises environments.

Zero Trust is predicated on removing location bias when establishing trust. As organizations look to expand from on-premises environments to the cloud, or vice versa, it is critical that there be policy and enforcement consistency to verify, authenticate, and authorize connections, regardless of where they are.

Ease of use.

Security teams remain understaffed and overworked. The quicker the tools supporting Zero Trust can be deployed, connected, configured, and put to use, the higher the likelihood of overall success. This attribute requires both ease of deployment and ease of management, with automation of policy creation and management cited as important by 32% of respondents.

Figure 6. Top Attributes for Tools Supporting Zero Trust



Platforms are well suited to support these attributes: 33% noted the importance of technologies supporting Zero Trust being part of a broader platform from a single vendor. Additionally, 39% cited the importance of technologies being part of an ecosystem, with integrations among different vendors. These are really two sides of the same coin: No vendor has tools to support every aspect of Zero Trust, but those that can address multiple aspects of it make it easier for an organization to expand over time. Ecosystems and partnerships between vendors can help fill missing gaps and ease the integration burden on security teams.

“To secure private data centers and cloud applications, organizations **must remove all implicit trust and enforce cybersecurity checks** across the entire application development lifecycle.”

Spotlighting Zero Trust in the Public Cloud

Zero Trust is often thought of in the context of users accessing applications. With applications becoming central to a variety of business processes, and with access required by many different users, this focus makes sense. However, organizations serious about a holistic Zero Trust approach must move beyond the focus on general user access and begin to think about privileged access for developers and administrators, workload-to-workload communications, and how to apply Zero Trust tenets to public cloud infrastructure such as AWS.

To secure private data centers and cloud applications, organizations must remove all implicit trust and enforce cybersecurity checks across the entire application development lifecycle. Rather than creating a role or group and broadly assigning numerous users to it, provisioning resources needs to be thought of in terms of a Zero Trust process. The ability to apply fine-grained access controls is critical to accomplishing this.

To ensure least-privilege access to applications and infrastructure, the identity and entitlements granted to the developers, DevOps team, and admins must be validated. Workloads accessing other workloads should mutually verify identity and apply least-privilege connectivity for the application. This requires microsegmentation to prevent attackers from moving laterally and helps limit the blast radius in the event of an exploitation. Finally, workloads should be continuously monitored for misconfigurations, vulnerabilities, and indicators of compromise to ensure the level of risk is properly accounted for and that policies are adjusted based on changes to this risk.

Palo Alto Networks and Okta: A Comprehensive Approach for Zero Trust, Centered on Identity

Palo Alto Networks and Okta Provide a Holistic Approach for Zero Trust on AWS

Palo Alto Networks and Okta have partnered with AWS to support customers on their Zero Trust journey and to deliver greater flexibility and ease of use across all the Zero Trust pillars identified by the Cybersecurity and Infrastructure Security Agency (CISA): identity, device, network, application, and data. Both Palo Alto Networks and Okta run on AWS infrastructure and have integrations across the AWS platform that enable customers to secure and build cloud applications—including Amazon Security Lake—which simplifies the process of pushing data from Okta and Palo Alto Networks into the lake, as well the ability to use Palo Alto Networks during investigations with data from the lake.

For all these pillars, enforcing least privilege is key and requires deep visibility into identity. Okta's multi-factor authentication (MFA), single sign-on (SSO), passwordless authentication, and Universal Directory help security teams apply granular risk-based policy, incorporate deep context, glean insights into identity-focused attacks, and ensure a seamless but secure user experience. Identity breaks down into controls pre-authentication, during authentication, and post-authentication. Pre-authentication, Okta provides capabilities to ensure that users have the right access to the applications applicable to their job function and no more—enforcing the principles of least privilege and phishing resistance with built-in provisioning and deprovisioning, auditing, and access certification features. Okta's adaptive MFA, SSO, passwordless authentication, and Universal Directory all help security teams apply granular risk-based policy, incorporate deep context, glean insights into identity-focused attacks, and ensure a seamless but secure user experience during authentication. Okta extends to post-authentication control by allowing for continuous monitoring of a user's risk across their threat surfaces—ingesting signals from partners like Palo Alto Networks—to help organizations understand and contain identity threats even when they are not directly interacting with Okta.

At the same time, Palo Alto Networks takes a modern, platform-based approach to security that makes it easier for organizations to adopt a Zero Trust approach across multiple domains (users, devices, applications, etc.). This enables organizations to create a single Zero Trust policy enforced everywhere Palo Alto Networks' enforcement points sit—Prisma Access in the cloud, virtual firewalls, hardware firewalls, etc.—helping to strengthen security and simplify operations.

Together, Okta and Palo Alto Networks help customers apply the coverage needed to achieve Zero Trust holistically across the environment, including the cloud, with fewer vendors and solutions. Specific integration points of the partnership include:

Palo Alto Networks Cloud Identity Engine (CIE) and Okta (including but not limited to lifecycle management, SSO, MFA, and passwordless authentication) strengthen and simplify authentication for more secure application access.

Palo Alto Networks Cortex and Okta Identity Threat Protection (ITP) leverage network, endpoint, and identity context during and post-authentication to detect and prevent excess risk, as well as prevent data breaches.

Palo Alto Networks Cortex and Okta log ingestion and playbook automation for streamlined operations and SOC efficiency.

Palo Alto Networks Prisma Cloud and Okta logs for ingesting data for permissions calculation in identity and access management security module to reduce risk.

BACK TO CONTENTS

Key Differentiators of the Partnership

Palo Alto Networks CIE enables consistent authentication and authorization for users, regardless of their location and the location of identity stores—on premises or in the cloud—across branches, campuses, data centers, and remote work environments. PAN-OS 11.0 introduces User Context in CIE as a single source of user information across network infrastructure to provide:

Consistent identification of users in a hybrid world by enabling redistribution of user information (User-ID, IP-Tag, User-Tag, quarantine list, and IP-port user mappings) across Palo Alto Networks' network security platform.

Centralized visibility of all user information on your network, simplifying user-based policy deployment and maintenance.

Secure segmentation of user context at cloud scale. CIE enables security administrators to keep personally identifiable information in mind by selecting the user context to be shared and the firewalls to receive the information.

> **"AWS Security Lake is an essential component for implementing a Zero Trust security architecture within a customer's environment. The integration of Palo Alto Networks, Okta, and Amazon Security Lake enables unified data storage in OCSF format, enhancing security and visibility for Zero Trust implementations while also ensuring compliance with data retention and regulatory requirements."**
>
> —Gee Rittenhouse, Vice President, Security Services at AWS

Okta's integration via Palo Alto Networks CIE simplifies adoption of MFA and passwordless authentication across Palo Alto Networks platforms. This can significantly accelerate the time to value for customers by removing operational complexity. Okta's ITP enables organizations to assess user risk post-authentication, takes in signals from third parties like Palo Alto Networks via the Shared Signals Framework (SSF), and allows for automated responses up to and including logout from Okta and downstream applications. Being able to receive threats on different platforms and have those platforms notify each other with SSF is critical to containing threats when they happen and getting a more holistic picture of real risk across your specialized security platform real estate. This, coupled with Okta's Universal Application Logout, provides a heavily layered cybersecurity defense.

BACK TO CONTENTS

Conclusion

Every organization should be researching Zero Trust and should begin to think about how it could be applied to their environment. There's no question that implementing Zero Trust is a significant project. Yet, while organizations should not try to do everything at once and are wise to identify and address critical use cases first, they should also develop at least an outline of what the project should look like in the future.

One of the keys to supporting this multipronged approach is selecting vendors that provide broad coverage across multiple use cases and Zero Trust pillars. While there are no single vendors that provide comprehensive coverage, technology partnerships can help immensely. Okta and Palo Alto Networks provide a strong example of how these types of partnerships between complementary vendors provide value to customers by simplifying integration and strengthening cybersecurity, all while improving the experience for users. Any organization that currently uses Palo Alto Networks or Okta or that is beginning to explore a Zero Trust approach would be well served to examine this partnership and how it might help them accelerate their Zero Trust journey.

okta

Okta is The World's Identity Company™. We secure Identity, so everyone is free to safely use any technology. Our customer and workforce solutions empower businesses and developers to use the power of Identity to drive security, efficiencies, and success. Learn why the world's leading brands trust Okta at okta.com.

LEARN MORE

paloalto® NETWORKS

Palo Alto Networks is the world's cybersecurity leader. Our next-gen security solutions, expert services, and industry-leading threat intelligence empower organizations across every sector to transform with confidence.

LEARN MORE

aws

Amazon Web Services (AWS) is the world's most comprehensive and broadly adopted cloud platform, offering over 200 fully featured services from data centers globally. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—trust AWS to power their infrastructure, become more agile, and lower costs.

LEARN MORE

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.

Enterprise Strategy Group™
by TechTarget

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.