JANUARY 2024

The zero-trust dilemma

Ensuring a positive user experience and getting leadership buy-in

CRA | Business Intelligence
A CRA Resource

Contents

ALSO IN THIS REPORT

Foreword

M: You don't trust anyone, do you?

007: No.

M: Then you've learned your lesson.

– Campbell, M. (2006). Casino Royale. Columbia Pictures.

Breaking the barriers to zero trust

It's been nearly two decades since Forrester analyst John Kindervag brought the concept of zero trust into the mainstream, advising organizations to "trust no one" and "verify everything."

Easier said than done, our respondents might say. While respondents almost universally regard zero trust as the right path forward, less than a third have actually implemented it in their organizations.

Many blame the high costs of implementation and the complexities of introducing zero-trust practices to existing workflows. Others say they can't get leadership buy-in and struggle to show ROI for something that defies easy explanation.

Zero trust isn't a security solution, it's a strategy. It doesn't have to mean ripping and replacing legacy IT, but sometimes it does require that. It's not supposed to disrupt the user experience, but its emphasis on authentication and least privileged access could frustrate those unaccustomed to the extra scrutiny.

"Our culture values employee empowerment and collaborative innovation," writes one respondent. "To some, zero trust is considered draconian."

In this report, we examine how organizations are facing this dilemma, and the factors that have helped some organizations make the leap where others have stalled. We hope that this research contributes to the dialogue and provides data to help organizations better understand and translate zero trust to key stakeholders.

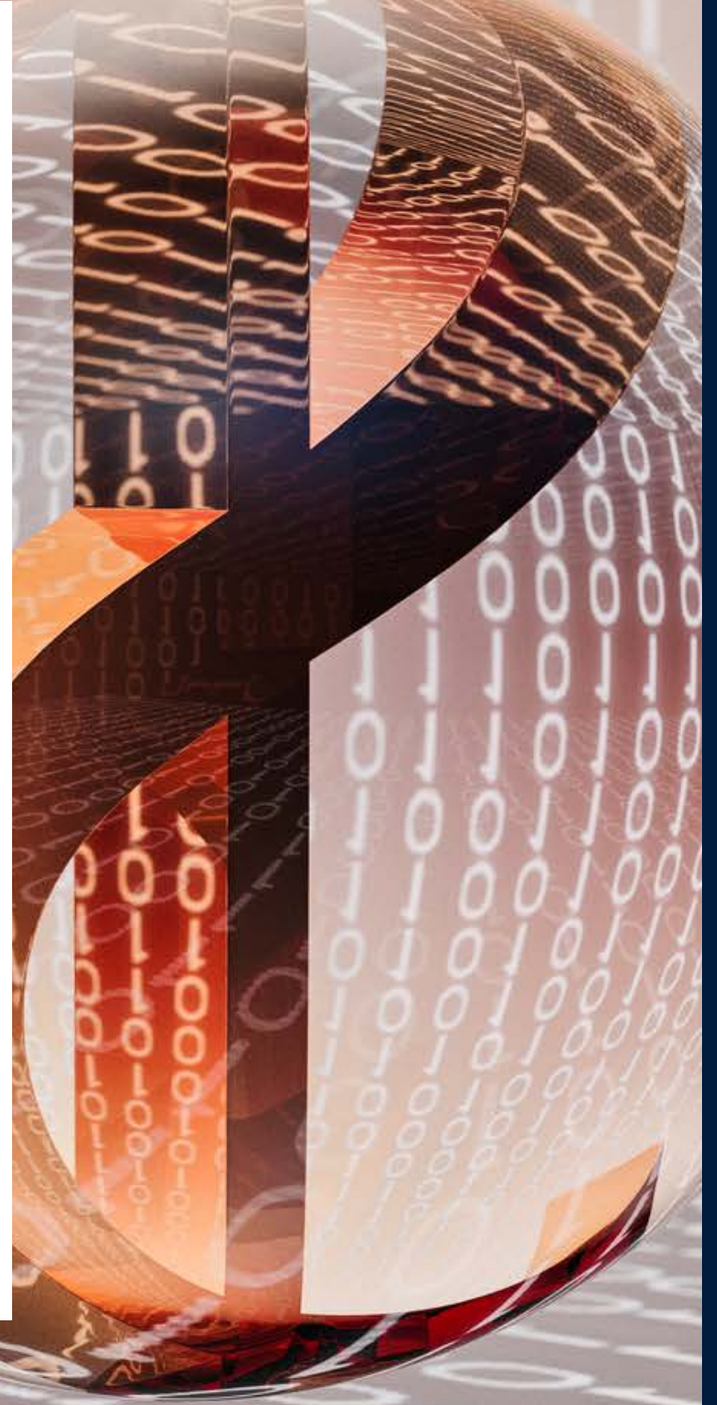
Zero trust 101

Adversaries frequently use loose permissions and privileged access to get inside a victim's network. By implementing the zero-trust model, organizations make it much more difficult for someone to receive access when they do not merit it. The following three concepts are central to the zero-trust framework:

- **Continuously verify.** The zero-trust framework operates on the basis that someone is already inside the network, executing a malicious attack. Trust is never freely extended, and instead must always be earned (or provided proof of) through continuous verification and authorization of user credentials and other behavioral data. This policy makes no distinction between users outside the network and those inside the network and eliminates the practice of one-and-done verification that previously determined successful access attempts.

- **Minimize breach impact.** Zero trust makes organizations more resilient in the event that a breach does take place. To limit the potential blast zone, organizations are encouraged to implement least privilege access so that a user's permissions extend only to those systems or data considered essential for their assignment. Identity-based segmentation is another way to limit the fallout, using risk-based policies to restrict access to individual resources based on the accesser's identity. These policies make it much more difficult for adversaries to move laterally through a network.

- **Data = context.** Zero trust is a data-hungry framework. With the aid of analytics and automation, a zero-trust approach means collecting — and making use of — as much data as possible to improve policy creation and enforcement. Data can include anything from network traffic, access requests, and workloads, to user credentials, endpoints, logs, and APIs. Such data is useful for fine-tuning trust algorithms that examine all the available evidence when deciding on access requests.



"Our organization has a large and complex architecture and infrastructure. It is quite challenging to map out and integrate all of the apps and tools that are relevant; particularly we have in-house developed apps, third-party highly customized apps, as well as off-the-shelf apps plus both on-premises, cloud hosting, and third-party cloud services."

– SURVEY RESPONDENT

Four key findings from the survey:

1.

Zero trust has a receptive audience, but few have actually laid the groundwork.

Just 30% have implemented zero-trust practices. Large organizations with more security staff have reported the most progress.

2.

Six in 10 respondents believe zero trust has become more important, especially for protecting business-critical data and establishing a more proactive security approach.

While MFA and encryption are popular components of a zero-trust strategy, other practices like behavior analysis and micro-segmentation are rare.

3.

Zero-trust initiatives are easily stalled.

It's costly to implement, complex in scope, and often meets resistance from workforce culture and entrenched IT systems. Explaining and justifying it to stakeholders is an uphill battle.

4.

AI could be a zero-trust catalyst.

By drawing on the power of generative AI, organizations could fine-tune zero trust policies to eliminate threats faster, improve automated response, and modify privileged access based on real-time monitoring.

1

THE STATE OF ZERO TRUST

Many unknowns and not enough details

A majority of those we surveyed support zero trust in principle but find it difficult to put these plans into motion. While 57% are receptive to zero trust, just 30% have actually implemented it to some degree — a disparity that we've observed in previous years of conducting this study.

What could be responsible for this disconnect?

When we segmented the audience based on receptiveness to zero trust and their progress in implementing it, we found that those showing the most progress ("Front runners") were predominately members of large organizations with well-staffed security teams.

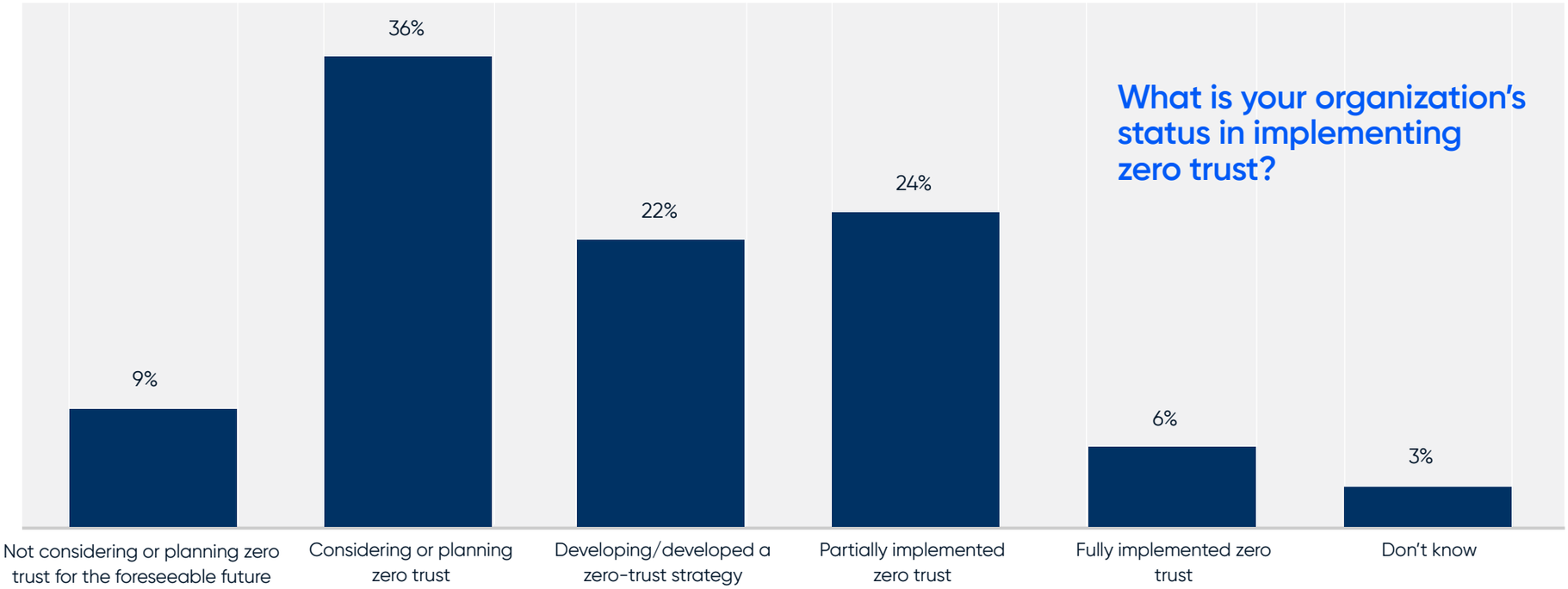
Conversely, those showing the least progress ("Holdouts") tended to work at smaller organizations with security teams comprising five or fewer members. Holdouts also more frequently cited lack of management buy-in and lack of qualified staff as reasons for not implementing zero trust and were moreover less likely to say zero trust was more important than compared to the previous year.

30%

have implemented zero trust at some level

Less than one-third of respondents indicate their organization has partially or fully implemented zero-trust practices.

Zero-trust adoption



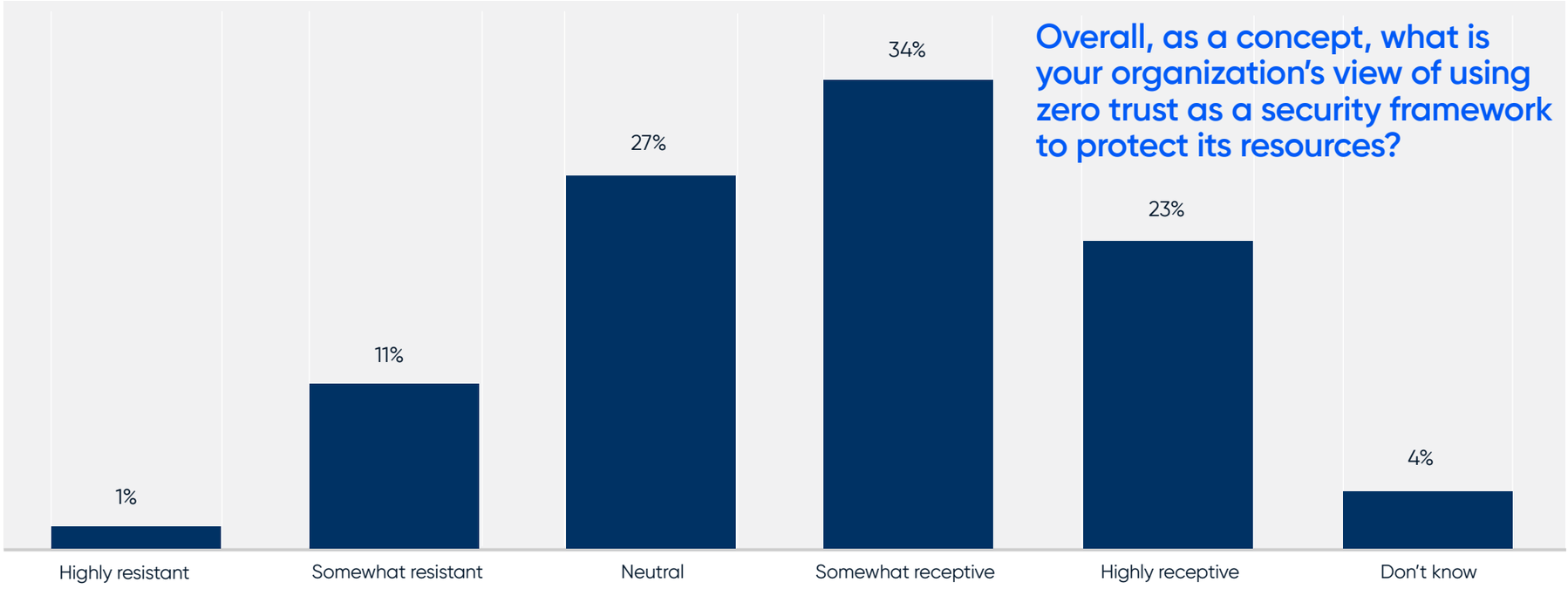
Base: All respondents (n=205).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Zero Trust Survey, December 2023.

"Cost is at the top. It has to make sense for us. We can turn on MFA for some of our systems already, that is included in software packages we own. To do zero trust we are probably looking at another software package and the question as to why would be asked. The disruption that it could cause to the users may be seen as enough to prevent us from implementing."

– SURVEY RESPONDENT

Just over half of all respondents (57%) report their organization is receptive at some level to the concept of zero trust as a security framework to protect its resources.

Receptiveness to zero trust



Base: All respondents (n=205).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Zero Trust Survey, December 2023.

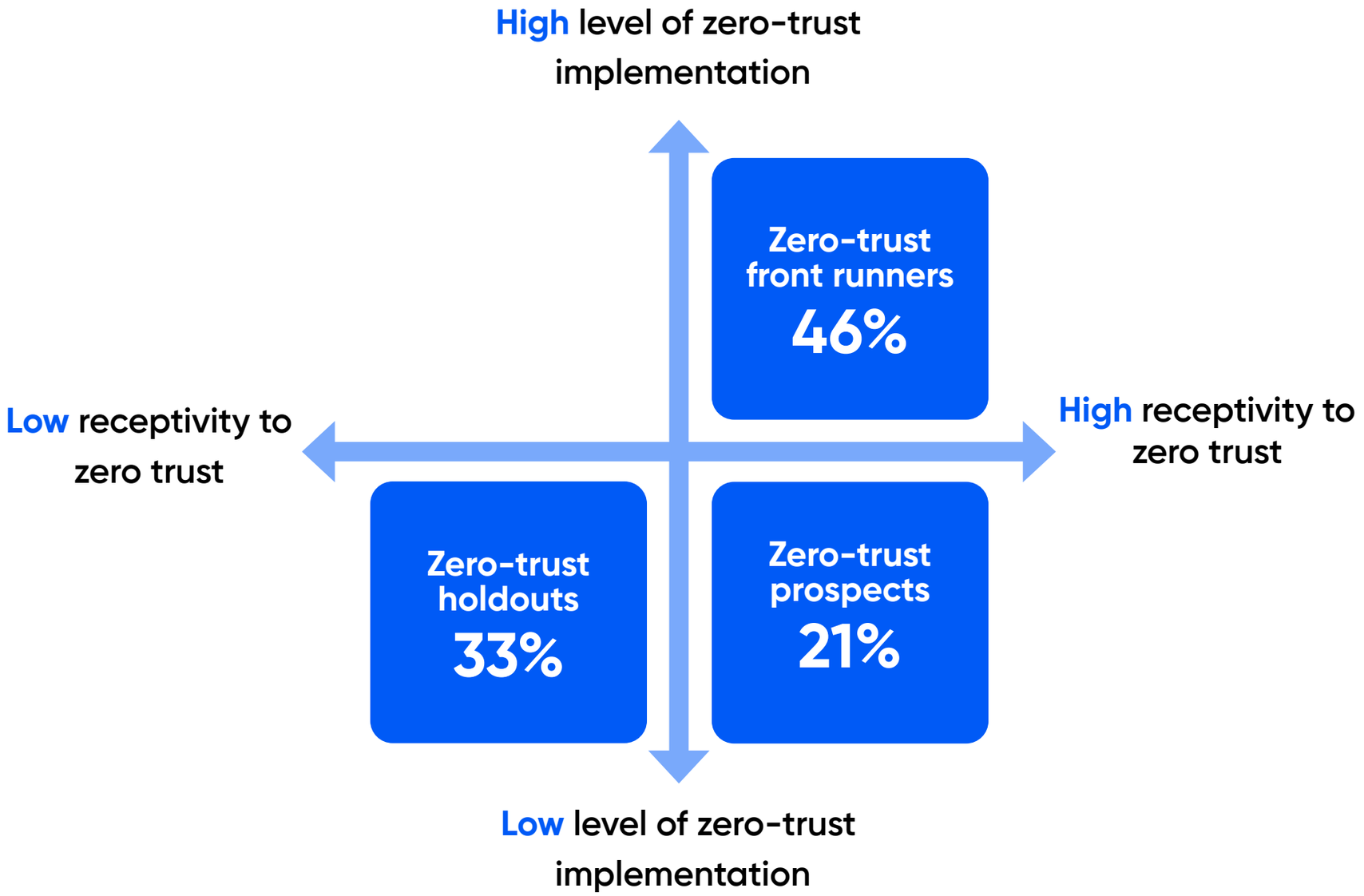
"Due to the security and nature of what we do for the federal government, zero trust is always on the horizon of what we're doing."

– SURVEY RESPONDENT

Respondents were segmented into the following mutually exclusive groups based on a combination of their organizations' level of zero-trust implementation as well as their overall receptivity to the zero-trust concept.

- **Zero-trust front runners** are implementing or building a zero-trust framework and are receptive to the zero-trust concept. They make up the largest segment (46% of all respondents).
- **Zero-trust prospects** are receptive to the zero-trust concept and most likely to implement zero trust in the future. They make up 21% of all respondents.
- **Zero-trust holdouts** are the least receptive to zero trust and least likely to implement zero trust in the foreseeable future. They make up one-third of all respondents.

Zero-trust segments



SEGMENT PROFILE

Zero-Trust Front Runners

Zero-trust receptivity and implementation	• Receptive to zero trust • Are in all stages of zero trust implementation: strategy development; and partial or full implementation
Organizational profile	• 1,000+ employees • Six or more security team members
Change in importance of zero trust in past 12 months	• 66% indicate it has become more important
Top zero-trust challenges	• Implementation costs • Integration with other technologies • Potential disruption to workflow/productivity • Ensuring positive user experience • Operational complexity

Note: Profile based on typical attributes of this segment.
Source: CyberRisk Alliance Business Intelligence (CRA BI), Zero Trust Survey, December 2023.

"Zero trust is fully implemented at all sites and levels of the organization and is a concern on any new installations."

– ZERO-TRUST "FRONT RUNNER"

SEGMENT PROFILE

Zero-Trust Prospects

Zero-trust receptivity and implementation	• Receptive to zero trust • Most are considering or planning zero trust; none have started implementing
Organizational profile	• 100+ employees • One to five security team members
Change in importance of zero trust in past 12 months	• 83% indicate it has become more important
Top zero-trust challenges	• Cost to implement • Compatibility with legacy systems • Potential disruption to workflow/productivity • Operational complexity • Organizational culture or employee resistance

Note: Profile based on typical attributes of this segment.
Source: CyberRisk Alliance Business Intelligence (CRA BI), Zero Trust Survey, December 2023.

"Our organization is somewhat receptive to using zero trust since it offers some security benefits, but must be weighed against the cost, complexity and inconvenience factors."

ZERO-TRUST "PROSPECT"

SEGMENT PROFILE

Zero-Trust Holdouts

Zero-trust receptivity and implementation	• Resistant or neutral to zero-trust concept • Many are not considering zero trust, while some are considering and even working on a strategy; none have started implementing zero trust
Organizational profile	• All size organizations, but mostly less than 10,000 employees • Five or fewer security team members
Change in importance of zero trust in past 12 months	• 40% indicate it has become more important
Top zero-trust challenges	• Implementation costs • Lack of management buy-in • Operational complexity • Lack of qualified staff to implement zero trust

Note: Profile based on typical attributes of this segment.
Source: CyberRisk Alliance Business Intelligence (CRA BI), Zero Trust Survey, December 2023.

"Our company has relied on traditional perimeter defenses like firewalls for many years, so completely changing our security model is seen as risky and complex given our resources. The unknown upfront costs to implement zero trust as well as training everyone on new systems causes hesitation in leadership despite understanding modern threats require a different defense paradigm."

– ZERO TRUST "HOLDOUT"

STRATEGIES AND TACTICS

2 Zero-trust roadmaps still under construction

Despite low rates of implementation, 62% of respondents believe the importance of a zero-trust strategy has grown in the last 12 months.

Many recognize it as a superior security approach to perimeter-based defenses that is better equipped to secure data across expanding geographies and endpoints. Others consider it a crucial step forward in securing identities and access against unauthorized users, insider threats, and malware attacks. Facing an onslaught of more sophisticated adversaries, some believe enforcing zero-trust policies could reduce blind spots and vulnerabilities found in third-party software, cloud-based applications, and shadow IT.

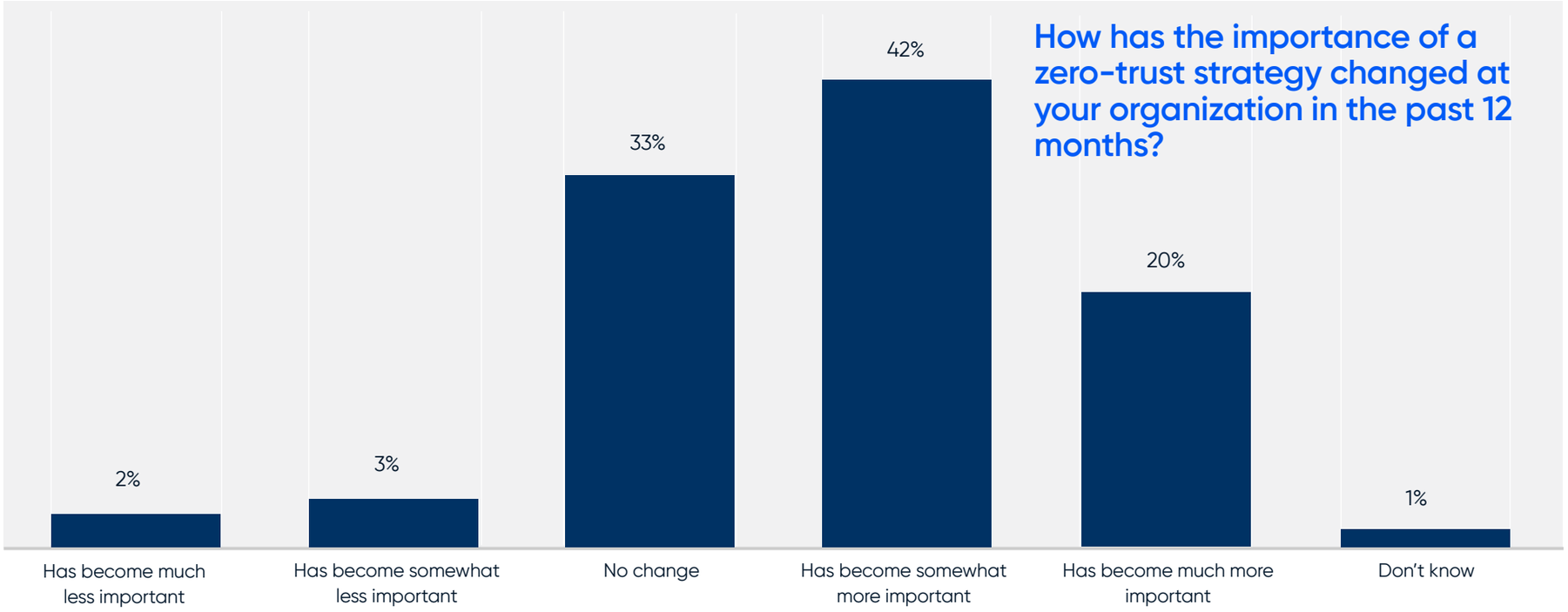
Many respondents, including those still developing or considering zero-trust policies, have already institutionalized basic zero-trust practices such as MFA, employee security training, and data encryption. A majority have plans to finalize a fully drawn-up zero-trust framework in 2024, and at least a third hint that behavior analysis and micro-segmentation are also on the horizon.

62%

believe zero trust has become more important in the past 12 months

About six in 10 respondents indicate that a zero-trust strategy has become more important in the past 12 months.

Change in importance of zero trust in past 12 months



Base: Respondents whose organizations are implementing zero trust, developing a zero-trust strategy, or considering zero trust (n=181).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Zero Trust Survey, December 2023.

"With threat actors becoming more sophisticated, we want our security posture to be more sound, and that includes strengthening our IAM solutions and zero trust."

– SURVEY RESPONDENT

Micro-segmentation, behavior analysis, and a zero-trust framework are the least likely to be included in organizations' zero-trust strategies; however, 54% indicate they are planning a zero-trust framework for 2024.

Status of zero-trust strategy components

	Currently included	Planned for 2024	Not planned
Multi-factor authentication (MFA)	86%	12%	2%
Employee cybersecurity training	75%	22%	4%
Data encryption (at rest and in transit)	70%	22%	8%
Identity and Access Management (IAM)	58%	31%	10%
Least privilege access	58%	33%	9%
Zero-trust framework	29%	54%	18%
Behavior analysis	27%	33%	40%
Micro-segmentation	19%	38%	43%

Which of the following are currently included, planned for 2024, or not planned to be included in your organization's zero-trust strategy?

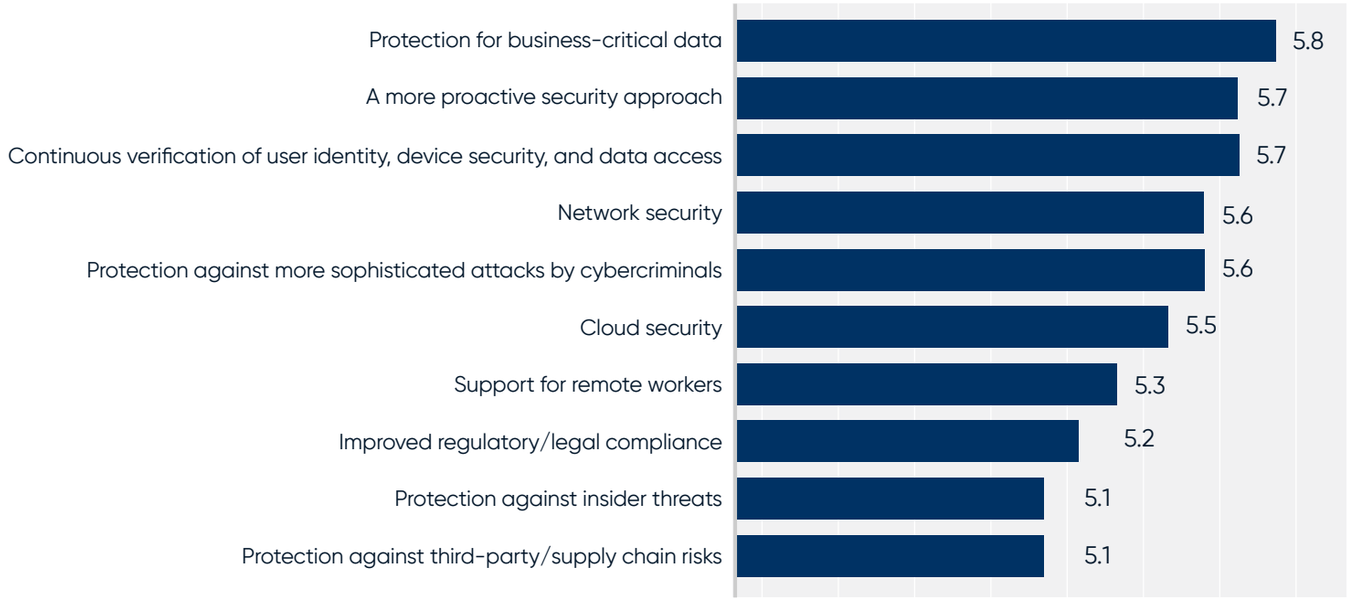
"[There's] misinformation in what a proper implementation would look like and how much inconvenience it will add to current workflow."

– SURVEY RESPONDENT

Base: Respondents whose organizations are implementing zero trust, developing a zero-trust strategy, or considering zero trust (n=181).
Note: Totals may not sum to 100% due to rounding.
Source: CyberRisk Alliance Business Intelligence (CRA BI), Zero Trust Survey, December 2023.

Protecting business-critical data; providing proactive security; and having continuous verification of user identity, device, and data access are deemed the top benefits of zero trust.

Benefits of zero trust (mean ratings out of 7)



In your opinion, how beneficial is zero trust in providing each of the following at your organization?

"As a concept, zero trust allows us to create rules and frameworks that prevent the proliferation of bad processes and practices and allows us as an organization to follow industry standards to maintain compliance."

– SURVEY RESPONDENT

Note: Respondents were asked to rate each on a scale from 1 to 7, where 1 is "Not at all beneficial" and 7 is "Extremely beneficial."
Base: Respondents whose organizations are implementing zero trust, developing a zero-trust strategy, or considering zero trust (n=181).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Zero Trust Survey, December 2023.

3

CHALLENGES

Getting zero-trust initiatives off the ground

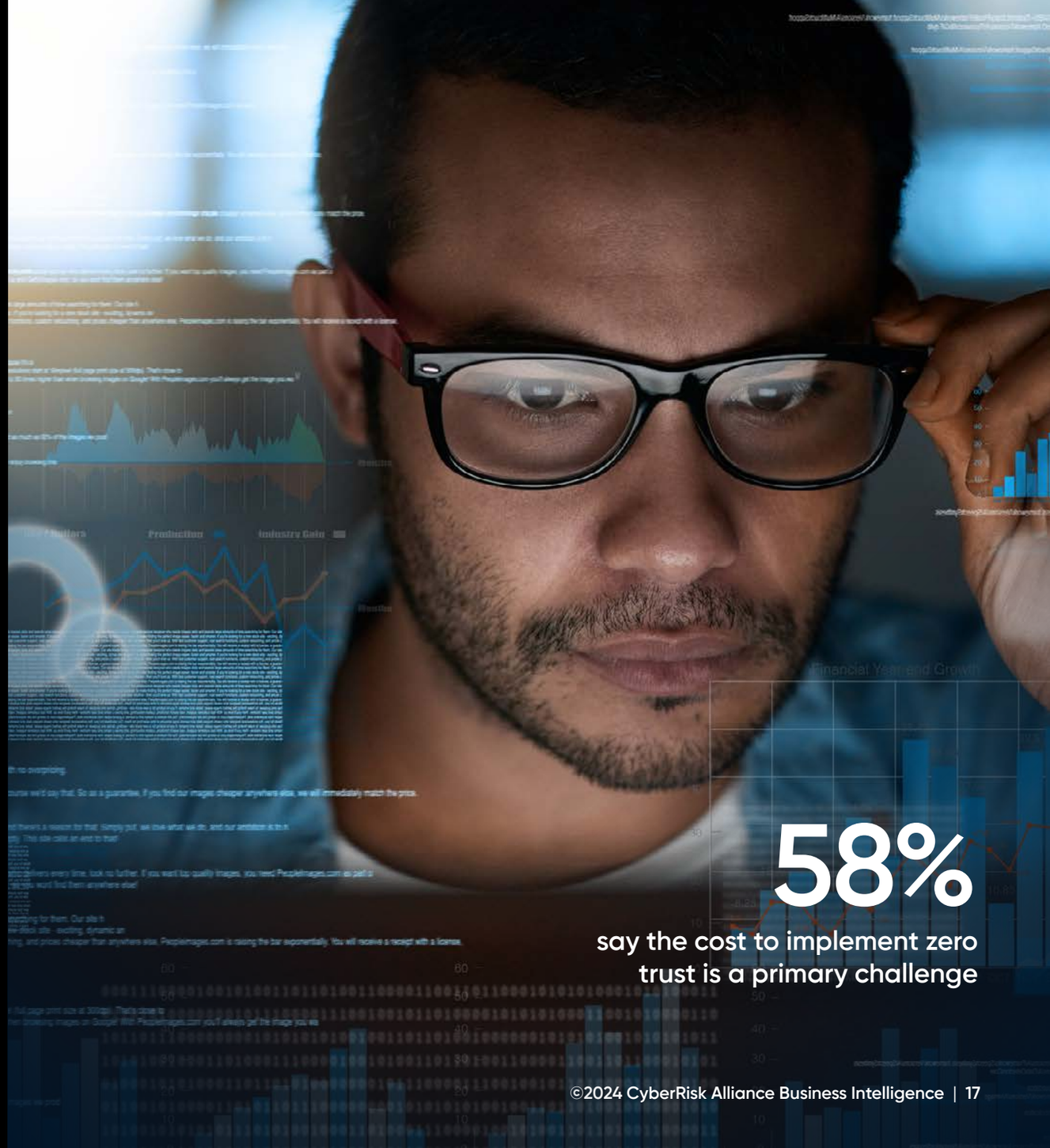
Respondents believe zero trust is in their organization's best interest, but for a variety of reasons find it hard to stick the landing.

The most common obstacles are costs to implement, potential disruptions to productivity, complexities of introducing a zero-trust architecture, and inflexibility of legacy IT systems.

"The complexity encountered in implementing zero trust requires making significant changes to our existing infrastructure," writes one respondent. Others anticipate that zero-trust policies would see backlash from both users and admins who are resistant to curtailed access or inconvenient UI.

"I don't think we've done a good job in the past at enforcing least privilege access for employees, and controls on laptops and computers have been lax," says one respondent. "Implementing more restrictions on users will upset the workforce and go against the culture of the institution."

Respondents say that confusion and lack of consensus on what zero trust entails hasn't helped matters, either. Forty-four percent describe vendors' attempts to define zero trust as "fair" or "poor," and that this has made it difficult to understand ROI or secure buy-in from financial decision-makers.

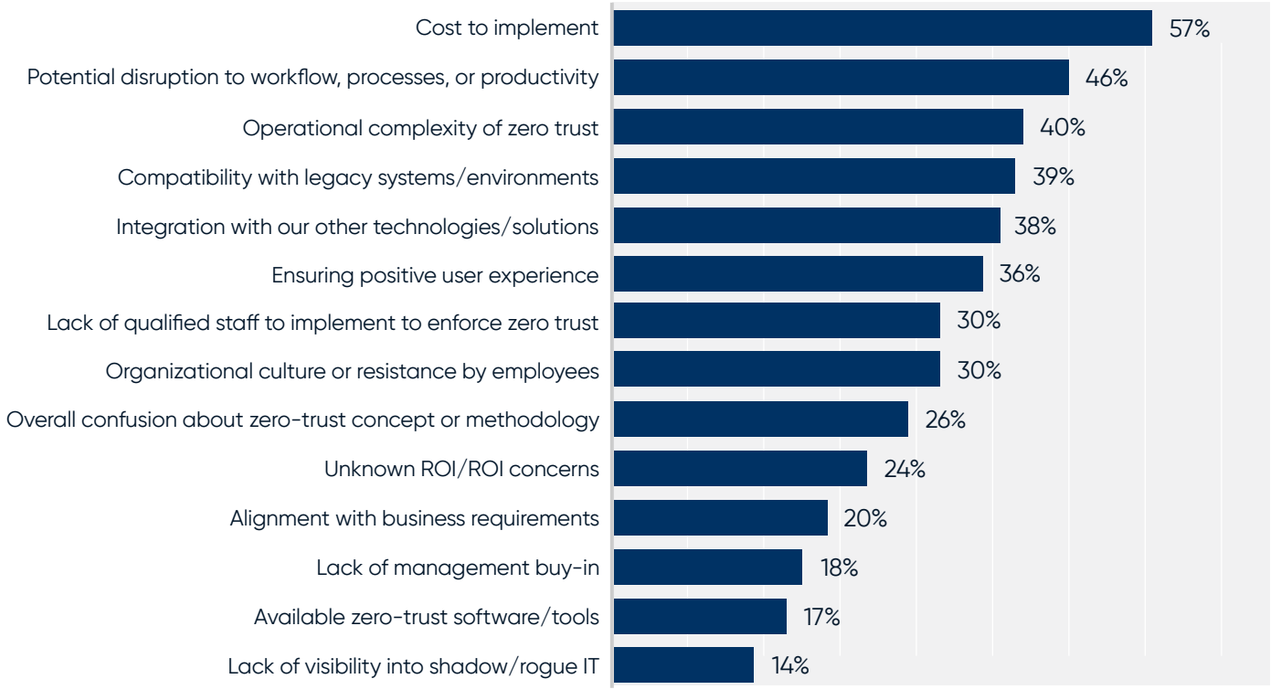


58%

say the cost to implement zero trust is a primary challenge

Implementation costs as well as the potential to disrupt workflow, processes, or productivity are considered the top challenges.

Zero-trust challenges



Which of the following are your organization's top challenges or potential challenges in implementing or planning for zero-trust security?

Note: Respondents were asked to select up to 5 choices.
Base: Respondents whose organizations are implementing zero trust, developing a zero-trust strategy, or considering zero trust (n=181).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Zero Trust Survey, December 2023.

"First, [zero trust] is a challenging initiative to communicate. Second, it can be expensive depending on how things are done and what kind of processes are in place."

– SURVEY RESPONDENT

Key challenges of implementing zero trust include:

- **Limited resources**
  - Budgetary
  - Lack of internal expertise
- **Organizational culture**
  - Executive buy-in
  - Employee resistance
- **Operational complexity**
  - Retrofitting older systems with zero trust
  - Complex environment/lack of integration
  - Large network infrastructure

Limited resources

"The budget for implementing zero trust needs to be increased."

"We do not have the expertise internally."

Organizational culture

"I think it's probably getting C-level to buy in or the accounting department because they need to see the benefits compared to cost."

"Getting buy-in from employees as they constantly question the why and the potential disruption and delays it can cause in accessing their systems and doing their work."

Please describe your organization's top challenges or issues in implementing zero trust.

Operational complexity

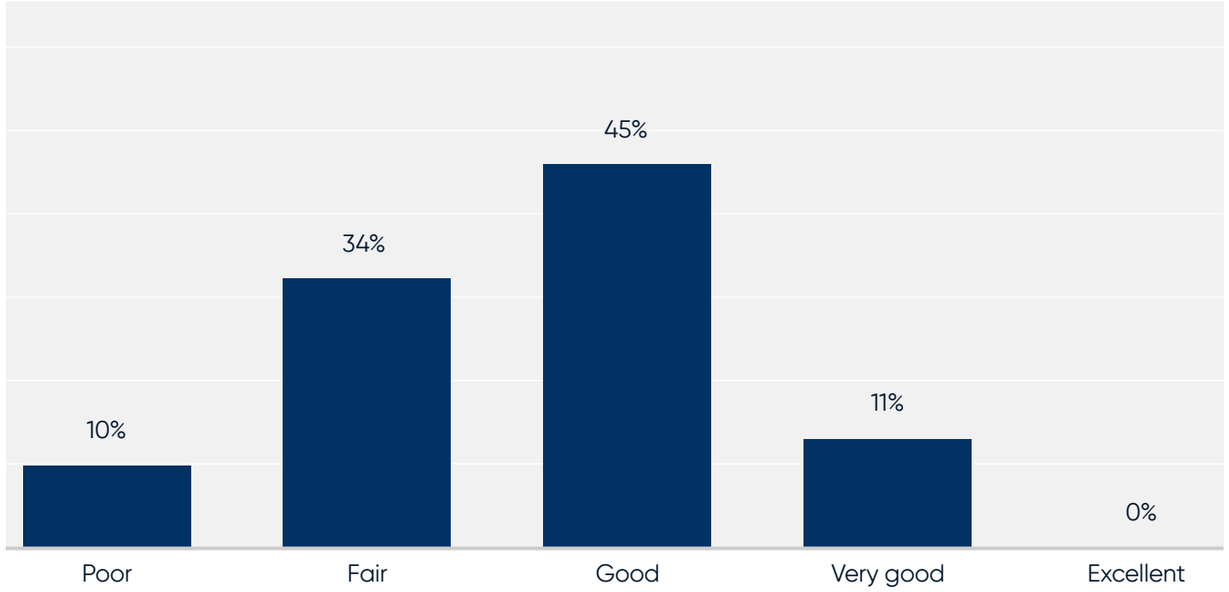
"Retrofitting older systems to align with the zero-trust model can be complex and costly."

"Complex environment which is not fully integrated."

"We have an existing and fully developed network infrastructure with hundreds of thousands of endpoints. We cannot implement zero trust in one fell swoop."

Overall, only 56% of respondents believe vendors have done a "good" or "very good" job of defining zero trust to the market.

Assessment of cybersecurity vendors' definition of zero trust



What is your overall assessment of how well cybersecurity vendors have defined zero trust?

"It's not well-defined. Standards aren't really there. It's a concept, not even a suite of products. Implementations are all over the map. Since I can't define it well, I can't estimate either the costs or benefits. Therefore, it will stay in limbo."

– SURVEY RESPONDENT

Base: All respondents (n=205).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Zero Trust Survey, December 2023.

4

THE AI FACTOR

Can AI rescue zero trust?

In the next few years, smart applications of generative AI could unlock even more value from the zero-trust playbook.

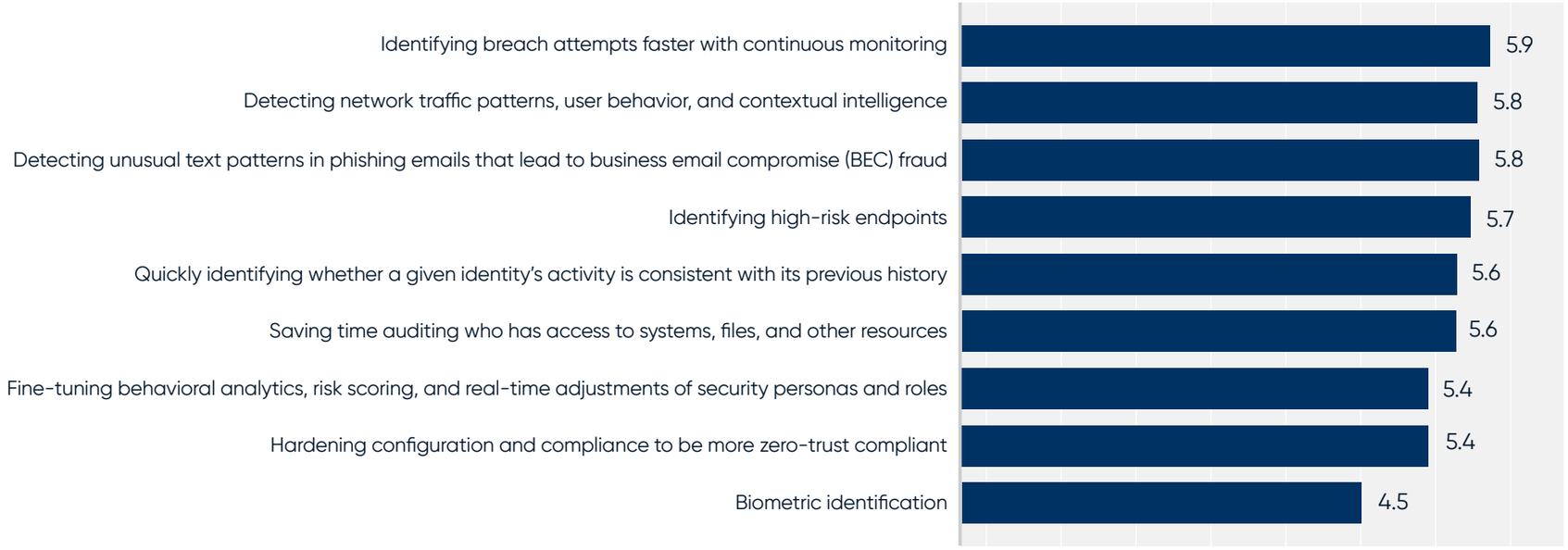
Respondents tell us they are most excited about how AI can help them identify breach attempts faster, reveal patterns in user behavior and network activity, and foil convincing phishing attempts.

The expectation is that AI could help shift security from being a fixed, static operation to one that is dynamic and adaptable based on context and continuous monitoring. For example, AI might be able to adjust user privileges from real-time risk assessments, automate incident response, and develop scripted actions that adjust over time as it learns from user activity and threat incidents.

"Faster identification of breach attempts" was rated the most important security benefit of integrating generative AI with zero trust.

Faster identification of breach attempts; detecting network patterns/user behavior, and contextual intelligence; and detecting unusual text patterns in phishing emails are top-rated benefits of integrating generative AI technology with zero trust.

Importance of integrating generative AI (e.g., ChatGPT) with zero trust (mean ratings out of 7)



In your opinion, how important are each of the following potential benefits of integrating generative AI technology with zero trust?

Note: Respondents were asked to rate each on a scale from 1 to 7, where 1 is "Not at all important" and 7 is "Extremely important."
Base: Respondents whose organizations are implementing zero trust, developing a zero-trust strategy, or considering zero trust (n=181).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Zero Trust Survey, December 2023.

Survey methodology

The data and insights in this report are based on an online survey conducted in December 2023 among 205 security and IT leaders and executives, practitioners, administrators, and compliance professionals in North America from CRA's Business Intelligence research panel.

The objective of this study was to explore various issues and topics related to organizations' zero-trust strategy, efforts, challenges, and related opinions.

Notes:

Some figures may not add up to 100% as a result of rounded percentages.

The respondent profile is as follows:

IT or IT security roles/titles:

- CISOs/CROs/CIOs/CTOs (10%)
- VPs/SVPs/EVPs (7%)
- Directors (32%)
- Managers (26%)
- IT/security admins (18%)
- Analysts/consultants (6%)

Organization sizes:

- Small (1 to 99 employees) (11%)
- Medium (100 to 999 employees) (25%)
- Large (1,000 to 9,999) (39%)
- Enterprise (10,000 or more) (25%)

Top industries:

- High-tech, IT, software, or telecom (20%)
- Education (17%)
- Manufacturing (15%)
- Healthcare (11%)
- Financial services (8%)
- Professional services (consulting, legal, etc.) (6%)
- Retail, trade, or eCommerce (6%)
- Media, communications, or advertising (4%)
- Non-profit (4%)
- Government (3%)

Other CRA Business Intelligence reports

2023

1. Tough on Ransomware: Organizations fighting ransomware with continuous monitoring, IR playbooks, backups, and user education (November 2023)
2. Cloud security: Gaps in skillsets and lack of visibility leaves many organizations flying blind (October 2023)
3. Easy Prey: The Danger of Vulnerable Endpoint and Devices (September 2023)
4. Threat Intelligence: Eyes on the Enemy (August 2023)
5. Vulnerability Management: A Maelstrom of Moving Targets (June 2023)
6. Controlling the Chaos: The Key to Effective Incident Response (May 2023)
7. Identity and Access Management: Can Security go hand-in-hand with User Experience? (April 2023)
8. Finding the Way to Zero Trust (March 2023)
9. Wanted: A Few Good Threat Hunters (February 2023)
10. Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations (January 2023)

2022

1. Threat Intelligence: Critical in the Fight Against Cyber Attacks, But Tough to Master (December 2022)
2. Ransomware Ready: Organizations Fight Back with More Aggressive Strategies and Technology (November 2022)
3. Harsh Realities of Cloud Security: Misconfiguration, Lack of Oversight and Little Visibility (October 2022)
4. Zero Trust Adoption Faces Ongoing Headwinds (October 2022)
5. Endpoint Security: Security Pros Concerned About the Proliferation of Non-Traditional Devices and Endpoints (September 2022)
6. Organizations Adopt Aggressive, More Proactive Vulnerability Management Strategies in 2022 (August 2022)
7. Threat Intelligence: The Lifeblood of Threat Prevention (July 2022)
8. CRA Study: Attackers on High Ground as Organizations Struggle with Email Security (July 2022)
9. Security Teams Struggle Amid Rapid Shift to Cloud-Based Operations (June 2022)
10. CRA Study: XDR Poised to Become a Force Multiplier for Threat Detection (May 2022)
11. CRA Study: Zero Trust Interest Surges, But Adoption Lags as Organizations Struggle with Concepts (April 2022)
12. CRA Study: Managing Third-Party Risk in the Era of Zero Trust (March 2022)
13. CRA Ransomware Study: Invest Now or Pay Later (February 2022)
14. CRA Research: A Turbulent Outlook on Third-Party Risk (January 2022)

CRA Business Intelligence contacts

Bill Brenner
SVP of Audience Content Strategy
bill.brenner@cyberriskalliance.com

Dana Jackson
VP of Research
dana.jackson@cyberriskalliance.com

Daniel Thomas
Custom Content Producer
daniel.thomas@cyberriskalliance.com

About CyberRisk Alliance

CyberRisk Alliance provides business intelligence that helps the cybersecurity ecosystem connect, share knowledge, accelerate careers, and make smarter and faster decisions. Through our trusted information brands, network of experts, and innovative events we provide cybersecurity professionals with actionable insights and act as a powerful extension of cybersecurity marketing teams. Our brands include SC Media, the Official Cybersecurity Summits, TechExpo Top Secret, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, Cybersecurity Collaborative, Security Weekly, ChannelE2E, MSSP Alert, and LaunchTech Communications. Learn more at www.cyberriskalliance.com.