The State of **Zero-Trust Architecture** in Organizations

CONVERGE
TECHNOLOGY SOLUTIONS
CYBERSECURITY

Ponemon
INSTITUTE

INTRODUCTION

Part 1

A zero-trust architecture aims to move defenses from static, networked-based perimeters to users, assets, and resources. Sponsored by Converge Technology Solutions Corp. and Ponemon Institute conducted research to determine the status of zero-trust adoption in organizations. According to the research, 48 percent of survey respondents believe traditional perimeter-based security solutions such as VPNs, next-gen firewalls, and network access control (NAC) products are ineffective at securing distributed hybrid cloud infrastructures.

The research shows that zero-trust architecture improves the ability to manage vulnerabilities and user access. Unlike VPNs which permit secure access to large sections of a network, zero trust segments access and limits user permissions to specific applications and services. Zero trust assumes no implicit trust is granted to assets or user accounts based solely on their physical or network location or asset ownership.

Ponemon Institute surveyed 694 IT and IT security, including cybersecurity practitioners, in the United States who are familiar with their organizations' zero-trust strategy. As part of the screening process, practitioners invited to complete the survey were asked if their organizations had adopted a zero-trust strategy. Thirty-one percent of these practitioners whose organizations did not adopt zero trust were excluded from the research. The two primary reasons for these organizations not adopting zero trust are that the value is not understood (40 percent) or there is no executive buy-in (33 percent).

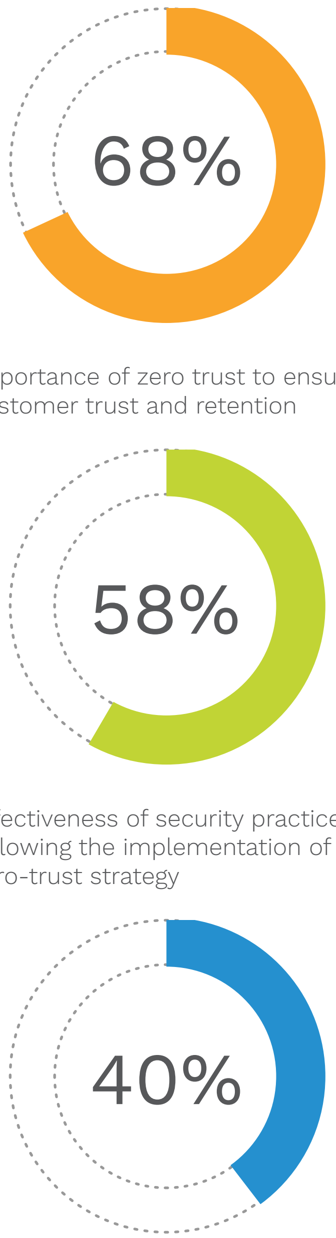
Respondents were asked to rate the effectiveness of their security practices before implementation and following implementation to determine the value of zero trust to organizations. Respondents used a scale of 1 = not effective to 10 = highly effective to rate their answers. Figure 1 shows the very and highly effective responses (7+ on the 10-point scale). Before implementation of a zero-trust strategy, 40 percent of respondents say their organization's security practices were effective or highly effective and this increased to 58 percent of respondents following implementation.

Respondents were also asked to rate zero trust's importance in ensuring customer trust and retention. According to Figure 1, 68 percent rate its importance as high or very high.

Figure 1. Zero trust strengthens the security posture of organizations

On a scale from
1 = not effective/not aligned
10 = highly effective/highly aligned

7+ responses presented



Importance of zero trust to ensure customer trust and retention

Effectiveness of security practices following the implementation of a zero-trust strategy

Effectiveness of security practices before implementing zero trust

The following findings reveal the value of a zero-trust strategy

- **Zero-trust architecture improves vulnerability management because it segments access and limits user permissions to specific applications and services.** The primary reasons for adopting zero-trust network architecture are: reducing connectivity issues; improving user experience; reducing difficulty in setting up, deploying, enrolling new users; and decommissioning departing users.
- **Zero trust is considered to improve security practices.** As a result, zero trust is regarded as important or very important in ensuring customer trust and retention.
- **Controlling access is a critical objective of zero-trust architecture.** Zero trust ensures attackers who gain access to users' accounts can only access their specific tools and services and nothing else. Identity and access management and authorization are the primary components of a zero-trust architecture. Some organizations use behavioral analytics and threat intelligence to improve asset security.
- **Identity management and authorization policies are important components in zero-trust security models.** As shown in the research, the primary components of a zero-trust strategy are a single strong source of identity for users and non-person entities (NPEs) and authorization policies around application or resource access
- **Zero trust is believed to reduce attacker "dwell time" in the network.** Respondents also say zero trust is very or highly effective in eliminating all lateral movement between users and servers because users are isolated from the corporate network. Zero trust is also considered highly effective in authenticating, authorizing, and inspecting all traffic flow at all times to ensure malware and attacks don't sneak in accidentally or maliciously.

According to the research, the following are steps to take to achieve a mature zero-trust strategy

- **Gain the support of senior leadership by regularly informing them about the effectiveness of the zero-trust program as measured by key performance indicators (KPIs).** Such support can make the implementation of a zero-trust strategy more of a priority and, as a result, secure the necessary resources such as budget and in-house expertise.
- **Quantify and track the benefits of zero trust.** The top three metrics used by organizations represented in this study measure the reduction in the number of data breach incidents, the reduction in the number of known vulnerabilities and reduction in the number of threats.
- **Identify existing security technologies that can be both cost-effective and aligned with the zero-trust strategy.** Prioritize what new security technologies are needed as part of the organization's zero trust implementation. A significant obstacle to achieving a strong zero-trust security posture is the continued use of legacy technologies.
- **Other obstacles to successfully implementing a zero-trust strategy include the lack of in-house expertise and budget.** According to the research, the average annual IT security budget is $32 million, with an average of $2.4 million dedicated to organizations' zero-trust strategy.

KEY FINDINGS

Part 2

This section provides an analysis of the research. The complete findings are presented in the Appendix of this report. The report is organized according to the following topics.

Maturity of organizations' zero-trust programs

Zero trust and a strong security posture

Zero trust minimizes risks from dwell time and lateral movement

Maturity of organizations' zero-trust programs

Achieving a mature zero-trust strategy can take several years. Respondents were asked to describe the maturity of their organizations' zero-trust strategy. According to Figure 2, only 33 percent of respondents say their organization has reached the full adoption stage with most zero-trust activities deployed across their enterprises and senior leadership support. Twenty-seven percent of respondents say zero-trust activities are fully deployed and maintained across their enterprise, and KPIs are used to measure program activities.

Seventy-one percent of respondents say it took their organization five to seven years (43 percent of respondents) or more than seven years (28 percent of respondents) to achieve full adoption or maturity. When asked how their organization's rate of adoption of a zero-trust strategy compares to its competitors, only 45 percent of respondents say they are ahead or way ahead of the competition.

Figure 2. What best describes the maturity of your organization's zero-trust strategy?

27%

Mature Stage
Zero-trust activities are fully deployed and maintained across the enterprise. C-Level executives are regularly informed about the effectiveness of the program. Program activities are measured with KPIs.

33%

Full Adoption Stage
Most zero-trust activities are deployed across the enterprise. The program has C-level support and adequate budget.

21%

Planning Stage
We are planning the adoption and defining what the zero-trust strategy is and how to implement it.

19%

Early Adoption Stage
Zero-trust activities are planned, defined, and partially deployed.

Quantifying and tracking the benefits of zero trust is important in achieving maturity

According to Figure 3, 66 percent of respondents say their organization's IT security team attempts to quantify and track how zero trust improves security posture.

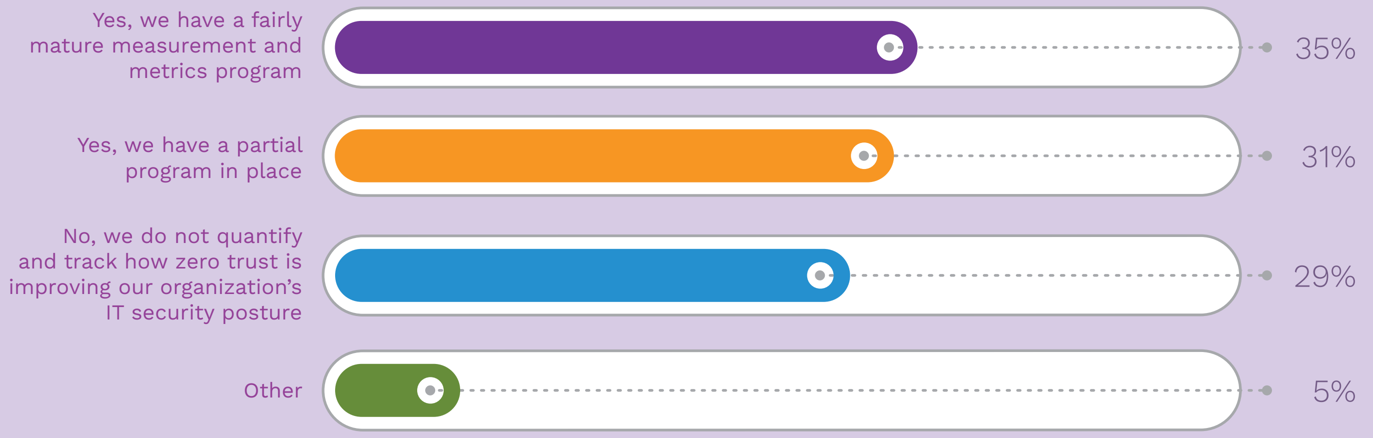
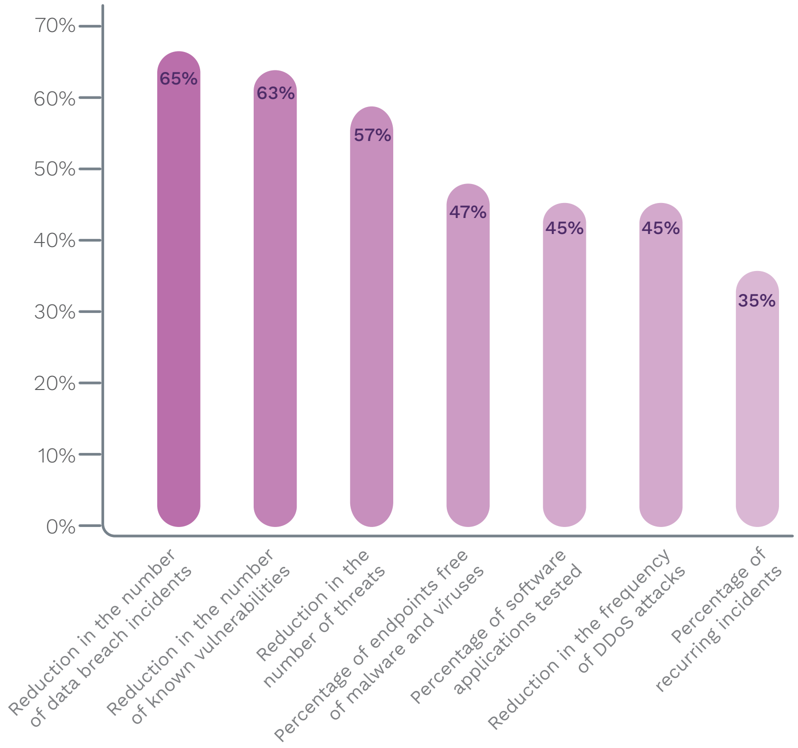


Figure 3. Does your IT security team attempt to quantify and track how zero trust is improving your organization's security posture?

As shown in Figure 4, the top three metrics used are reduction in the number of data breach incidents (65 percent of respondents), reduction in the number of known vulnerabilities (63 percent of respondents), and reduction in the number of threats (57 percent of respondents).

Figure 4. What metrics are used to quantify and track how zero trust is improving your organization's security posture?

More than one response permitted



To achieve maturity, it is important to identify security technologies that are aligned with the zero-trust strategy and are cost-effective. Respondents were asked to rate their organization's effectiveness in determining existing security technologies that could reduce costs in a zero-trust implementation and their effectiveness in prioritizing what new security technologies are needed on a scale of 1 = not effective to 10 = highly effective.

Figure 5 presents the very and highly effective and not aligned/highly aligned responses (7+ responses on the 10-point scale). Just 42 percent of respondents say their organization's current security tools are very or highly aligned with their zero-trust roadmap.

Only about half (50 percent) of respondents say their organization is very or highly effective in determining which existing security technologies can be part of the zero-trust implementation to reduce costs. However, more than half (54 percent) of respondents say their organization is very or highly effective in prioritizing which technologies should be acquired as part of the zero-trust implementation.

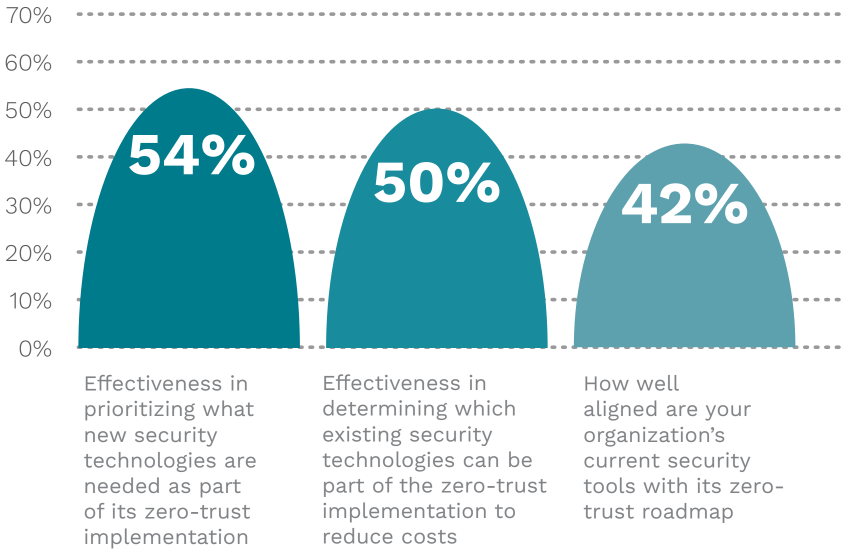


Figure 5. Effectiveness and alignment in using and prioritizing technologies in a zero-trust implementation

On a scale from
1 = not effective/not aligned
10 = highly effective/highly aligned

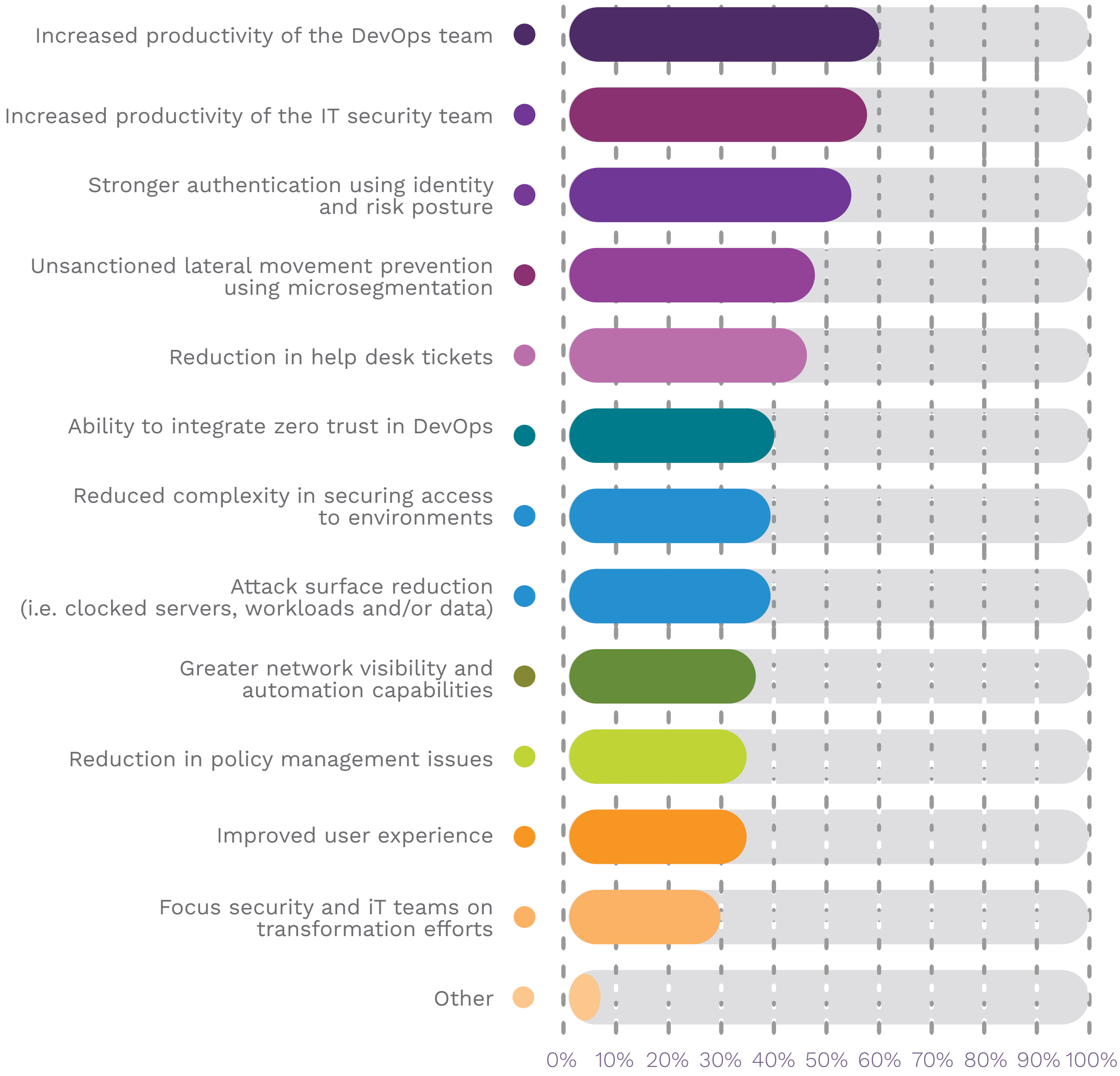
7+ responses presented

Zero trust and a strong security posture

Zero trust improves the productivity of DevOps and IT security teams. A primary objective of zero trust is to improve the management of vulnerabilities and user permissions. Figure 6 provides a list of the benefits of zero trust. Fifty-nine percent of respondents say the productivity of the DevOps team increases and 54 percent of respondents say the IT security team is more productive. More than half (52 percent) of respondents say zero trust results in stronger authentication. Another sign of improved productivity is the reduction in help desk tickets (44 percent of respondents).

Figure 6. What does your organization believe are the primary benefits of zero trust?

Five responses permitted



Zero-trust network architecture segments access and limits user permissions to only those applications, services, and datasets needed—resulting in reduced attack surface. More than half (51 percent) of respondents say their organization has adopted zero-trust network architecture.

According to Figure 7, the primary reasons for adopting zero-trust network architecture are: reduce connectivity issues and improve user experience; reduce the difficulty in setting up, deploying, enrolling new users; and decommissioning departing users. Thirty-eight percent of respondents say zero-trust network architecture improves visibility of user activity and application usage.

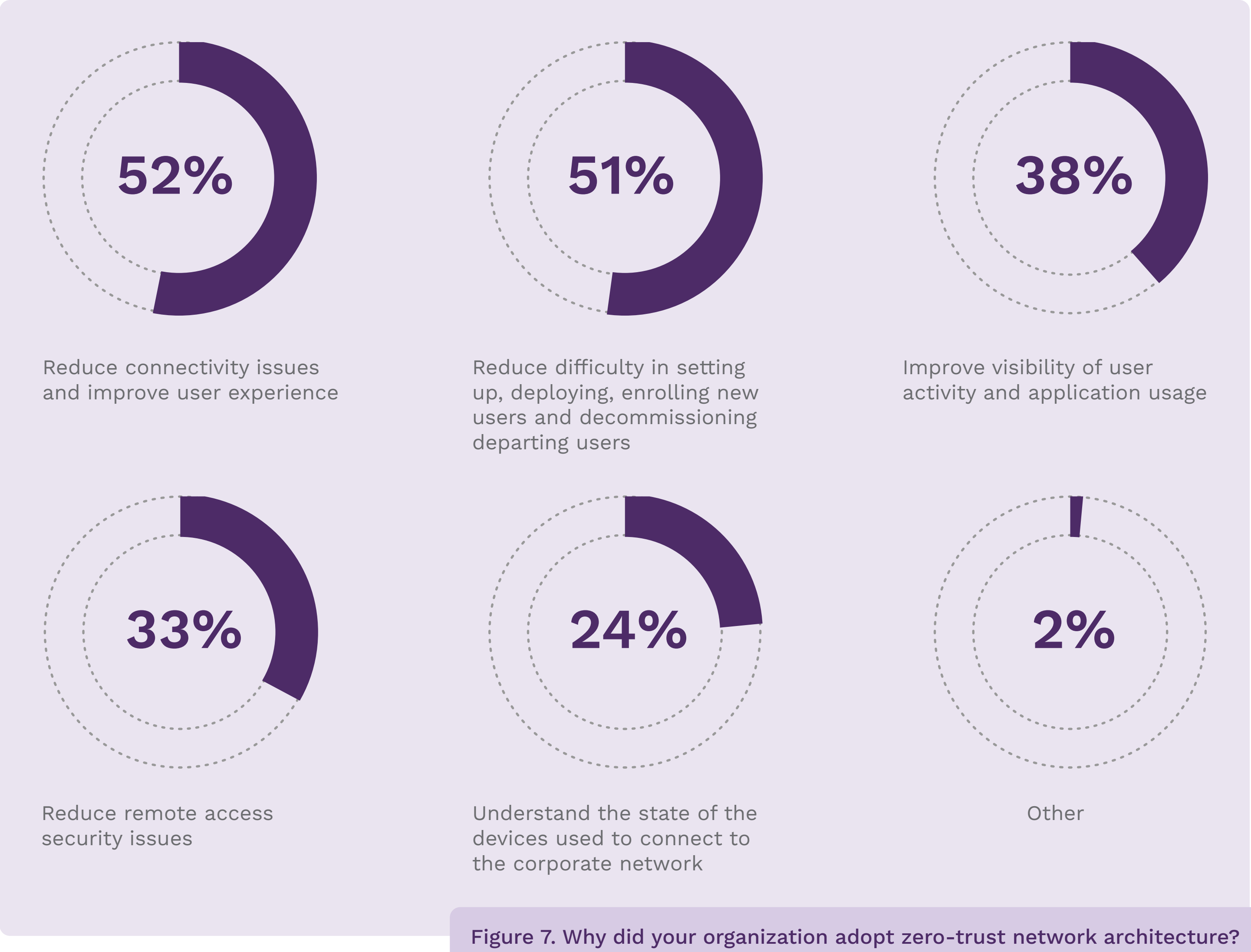


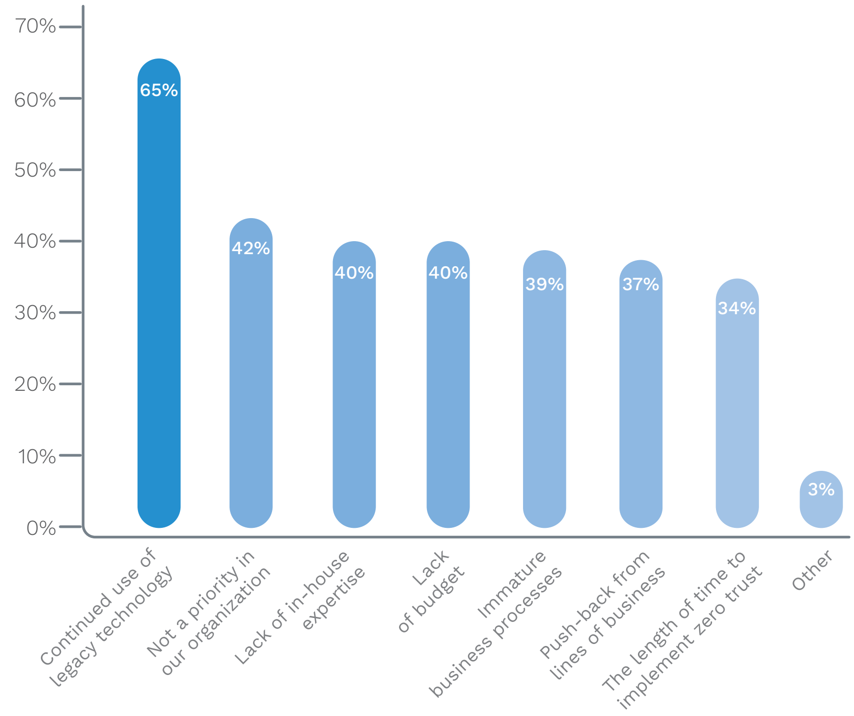
Figure 7. Why did your organization adopt zero-trust network architecture?

Two responses permitted

The continued use of legacy technology is the biggest obstacle to achieving a strong zero-trust security posture. Figure 8 presents the difficulties in implementing zero trust. Sixty-five percent of respondents say the number one obstacle is the continued use of legacy technologies, followed by zero trust not being a priority (42 percent of respondents) in the organization, as well as a lack of budget and in-house expertise (both 40 percent of respondents). According to the research, the average annual IT security budget is $32 million, and organizations are allocating an average of $2.4 million of the IT security budget to zero-trust strategies.

Figure 8. What obstacles have impacted your organization's implementation of zero trust?

Three responses permitted

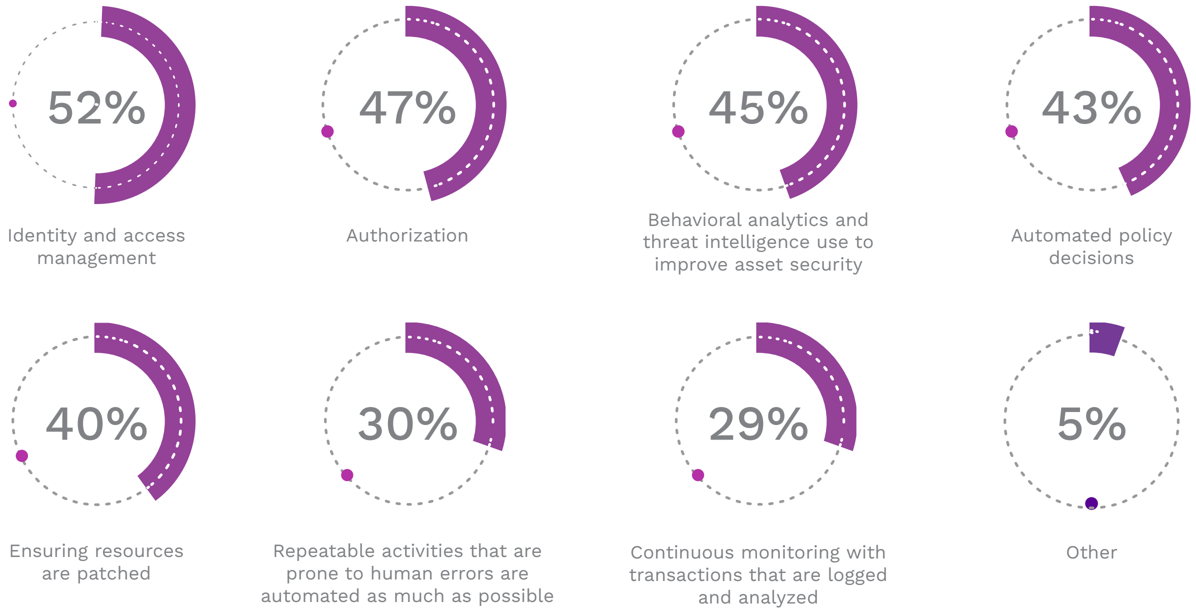


Controlling access is a critical objective of zero-trust architecture. Fifty-three percent of respondents say zero trust ensures attackers who gain access to users' accounts can only access those users' specific tools, services, and resources and nothing else.

According to Figure 9, identity and access management (52 percent of respondents) and authorization (47 percent of respondents) are the primary components of a zero-trust architecture. Forty-five percent of respondents say behavioral analytics and threat intelligence used to improve asset security are elements of zero-trust architecture.

Figure 9. Components in organizations' zero-trust architecture.

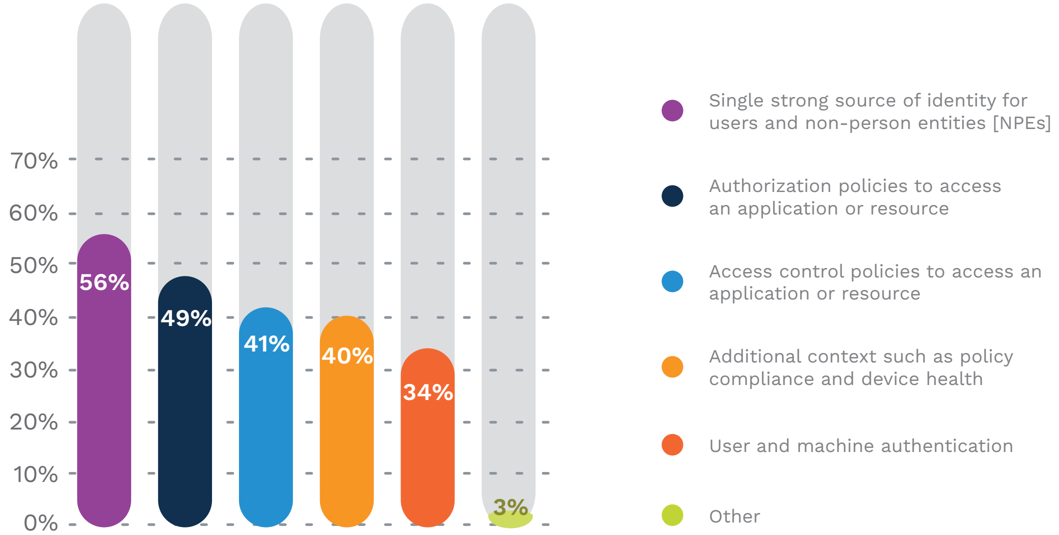
More than one response permitted



Identity management and authorization policies are important components of zero-trust security models. As shown in Figure 10, 56 percent of respondents say a single, strong source of identity for users and non-person entities (NPEs) is part of their zero-trust security model, and 49 percent of respondents say authorization policies for application and resource access are included.

Figure 10. Components in organizations' zero-trust security model.

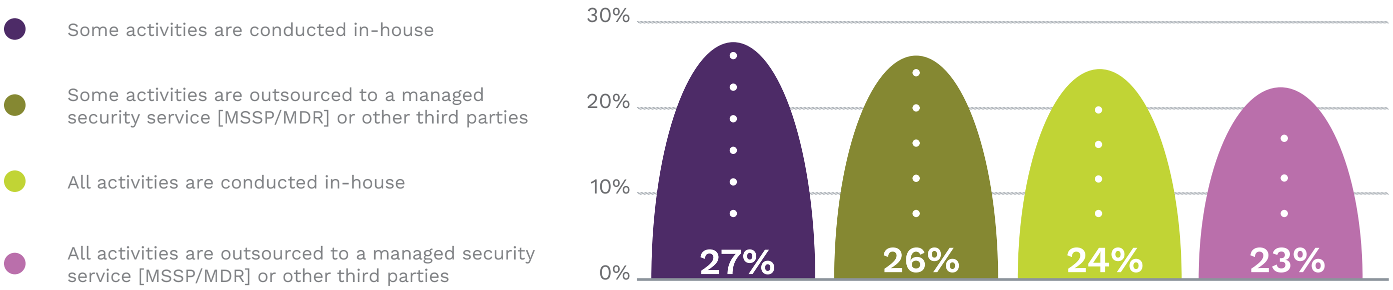
More than one response permitted



Most zero-trust activities are outsourced due to the lack of in-house expertise. As shown in Figure 11, only 24 percent of respondents say all zero-trust activities are handled in-house. If conducted in-house, an average of 45 hours each week is spent on zero-trust activities.

Seventy-six percent of respondents say at least some zero-trust activities are outsourced to a managed security service provider (MSSP/MDR) or other third parties. Whether zero-trust activities are conducted in-house or outsourced, 68 percent of respondents say their organizations have an average of six IT and IT security staff dedicated to zero-trust activities. Twenty-five percent of organizations say their staff has zero-trust certification.

Figure 11. How are zero-trust activities handled in your organization?

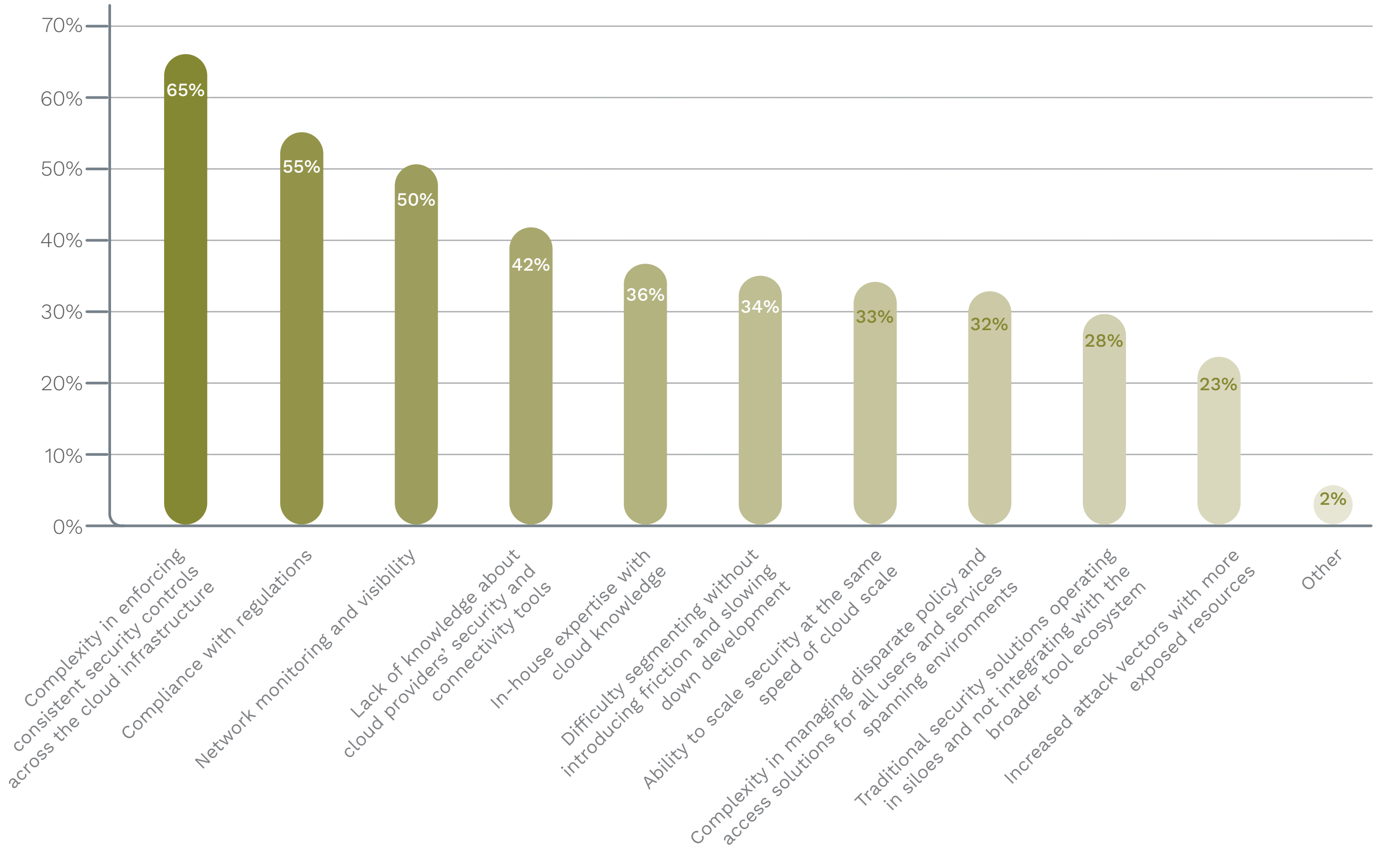


The complexity of enforcing consistent security controls across the cloud infrastructure is the most significant risk to the cloud environment. About half (48 percent) of respondents say zero trust is very effective in reducing cloud security risks. Zero-trust security for the cloud denies access to any user not explicitly permitted by policy and offers a unified policy model for secure access across hybrid and multi-cloud environments.

However, organizations struggle to reduce complexity in enforcing consistent security controls across the cloud infrastructure (65 percent of respondents) and to comply with regulations (55 percent of respondents), as shown in Figure 12. The lack of network visibility is also a risk (50 percent of respondents).

Figure 12. Which of the following poses the most significant risk to your organization's cloud environment

Four responses permitted



Zero trust minimizes risks from dwell time and lateral movement

Disruption/destruction of connected devices poses the greatest risk to organizations. As shown in Figure 13, other serious risks include disruption of the core business network (48 percent of respondents) and data breaches involving clients' proprietary information (45 percent of respondents).

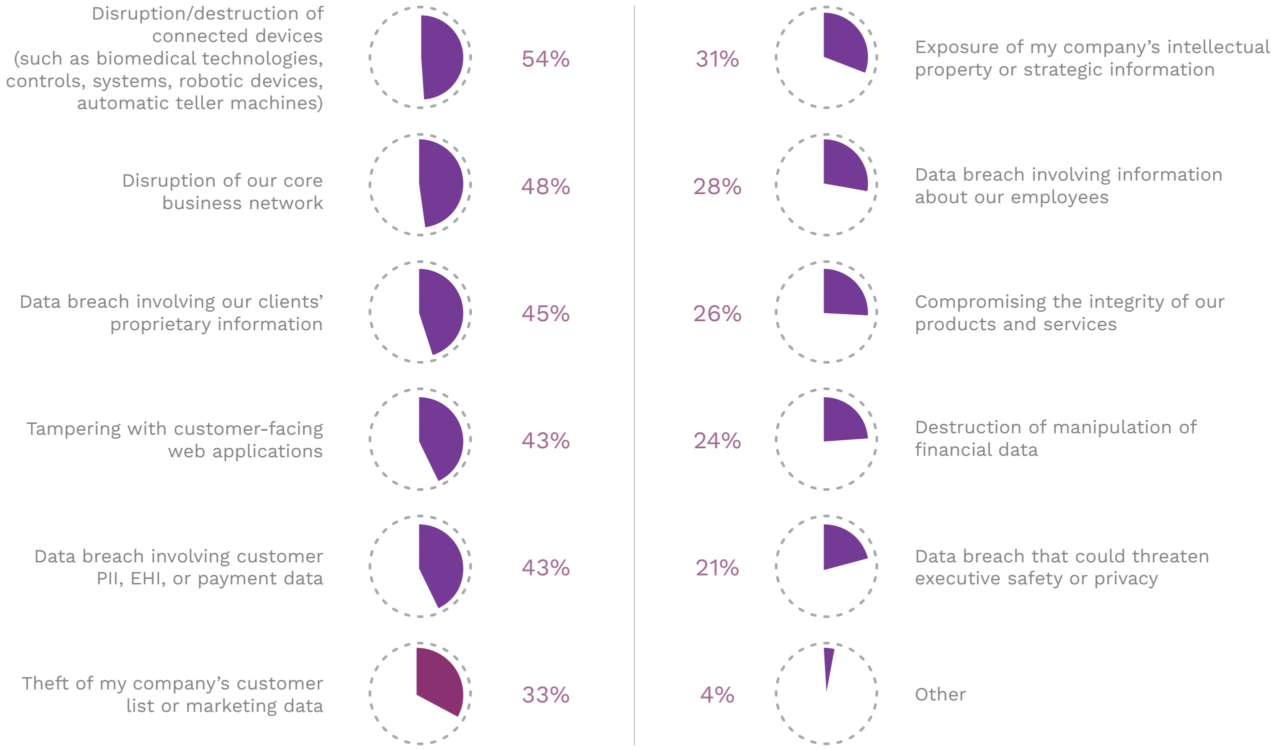


Figure 13. What types of cyberattacks pose the greatest risk to organizations?

Four responses permitted

Lateral movement in the network is a significant concern for organizations. Lateral movement after an attacker gains initial access to the network allows the attacker to maintain ongoing access. Attackers move deeper in search of sensitive data and other high-value assets and obtain increased privileges using various tools.

Sixty-four percent of respondents say their organization is very concerned about lateral movement in their network. Only 39 percent of respondents say their organization knows how an attacker could use a system to move laterally if compromised.

Figure 14 shows the primary obstacles to detecting cyber attackers operating within the network. These include the inability to properly maintain and enforce security configurations and security policies (46 percent of respondents), difficulty in distinguishing between false positives and "real" alerts (45 percent of respondents), and the lack of clarity on what threats or threat indicators their organization should look for (43 percent of respondents).

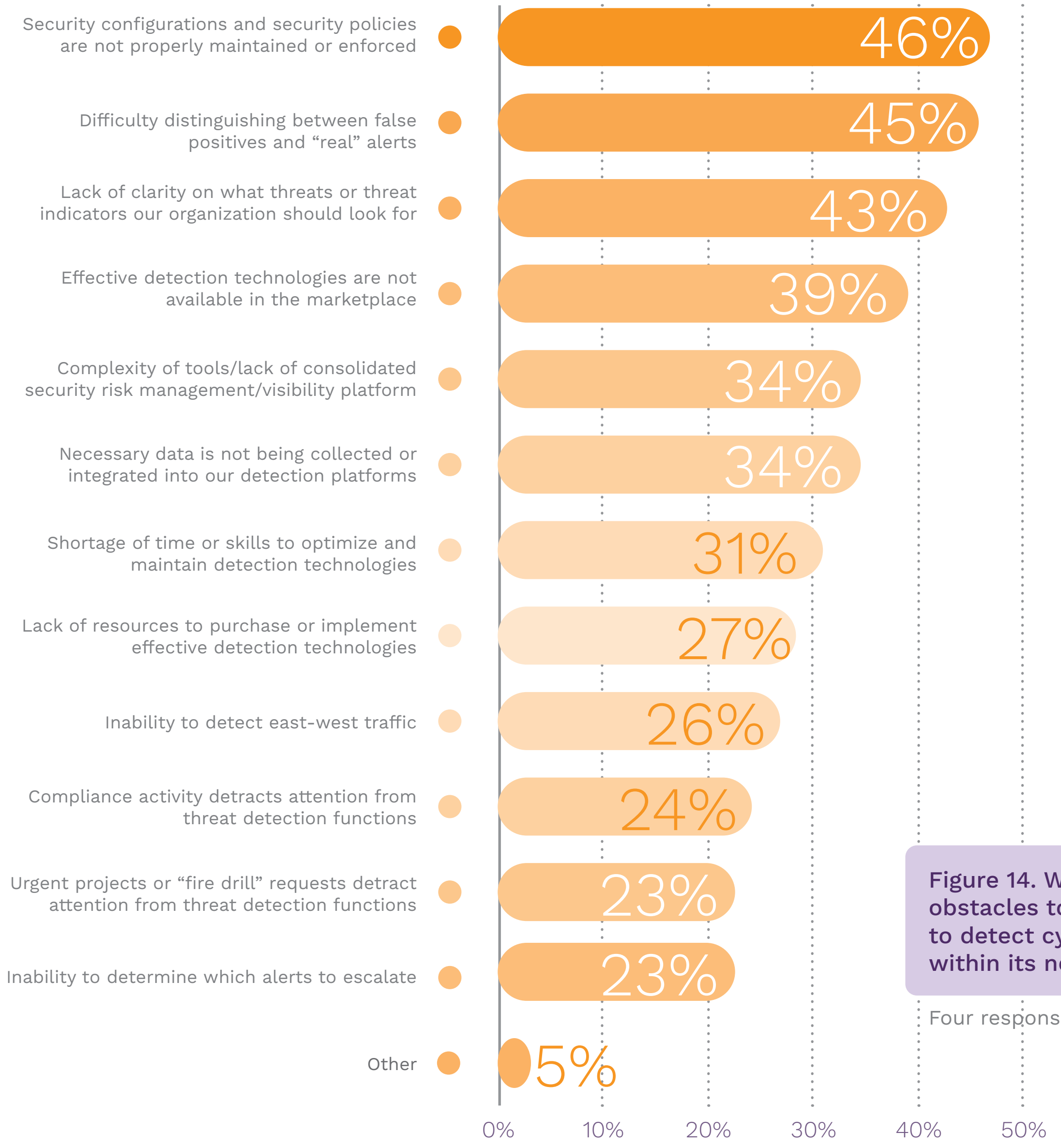


Figure 14. Which of the following are obstacles to your organization's ability to detect cyber attackers operating within its network?

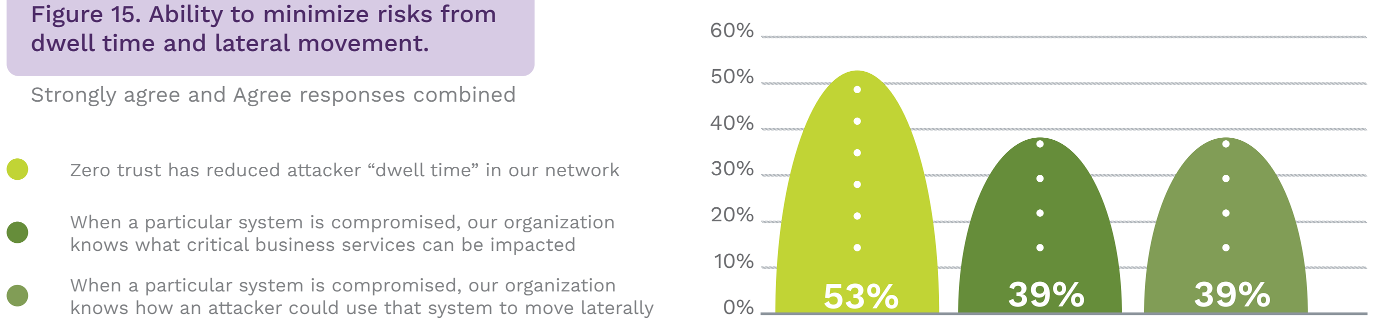
Four responses permitted

Threat actors successfully evade detection after gaining access into a network. Despite problems with static, network-based perimeters, 50 percent of respondents say their organization remains reliant or highly reliant on perimeter security.

As shown in Figure 15, only 39 percent of respondents say their organization knows how an attacker could use a compromised system to move laterally and only 39 percent of respondents say their organization can identify the critical business services impacted if a system is compromised.

Figure 15. Ability to minimize risks from dwell time and lateral movement.

Strongly agree and Agree responses combined



Zero trust improves the ability to minimize risks from dwell time and lateral movement. According to Figure 16, 56 percent of respondents say zero trust is very or highly effective in eliminating all lateral movement between users and servers because users are isolated from the corporate network. Sixty-five percent of respondents say zero trust makes their organizations very or highly effective in authenticating, authorizing, and inspecting all traffic flow at all times to ensure malware and attacks don't sneak in accidentally or maliciously.

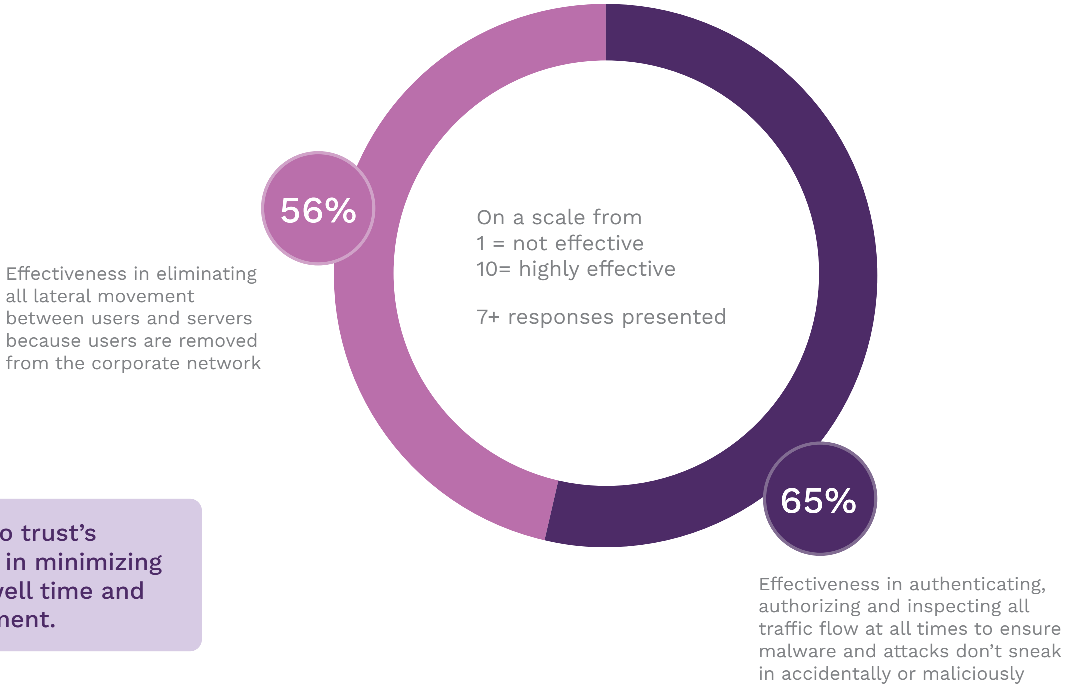


Figure 16. Zero trust's effectiveness in minimizing risks from dwell time and lateral movement.

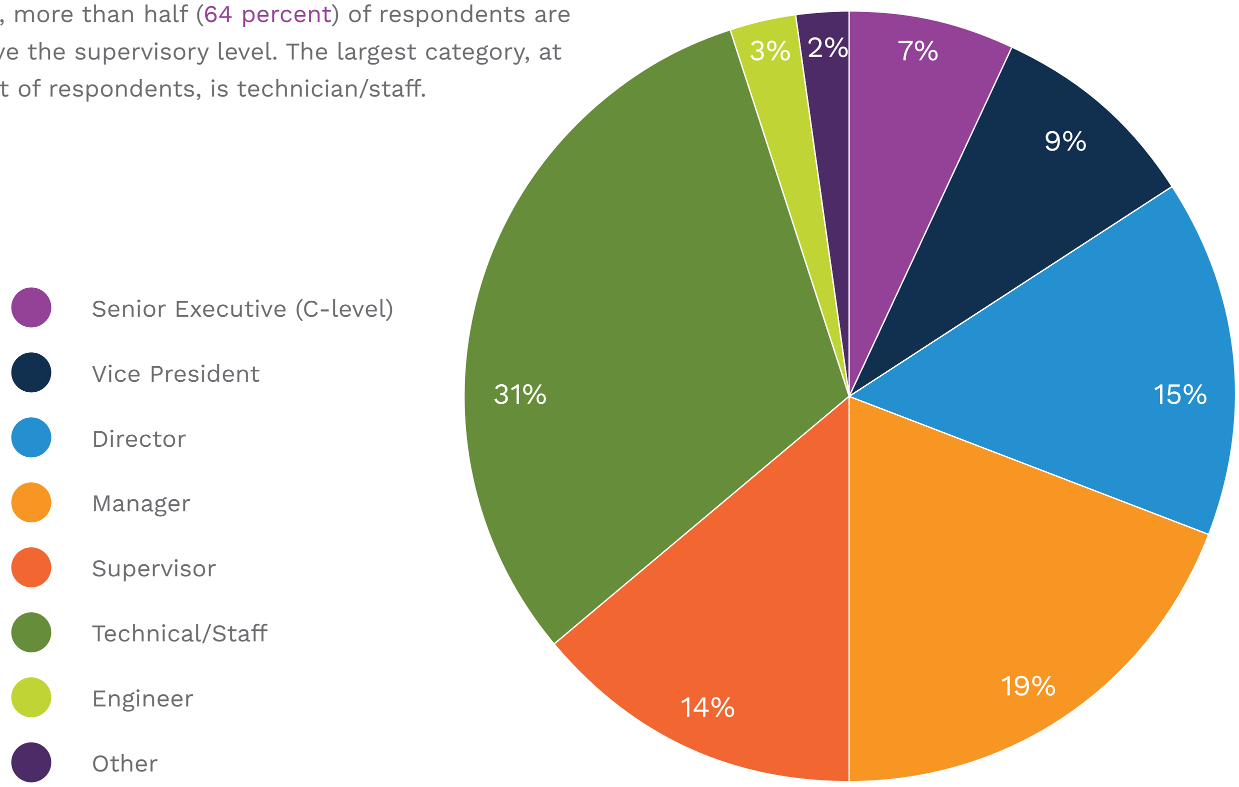
METHODOLOGY

Part 3

A sampling frame of 17,050 IT and IT security practitioners in the United States who are familiar with their organizations' zero-trust strategy were selected as participants to this survey. Table 1 shows 763 total returns. Screening and reliability checks required the removal of 69 surveys. Our final sample consisted of 694 surveys or a 4.1 percent response.

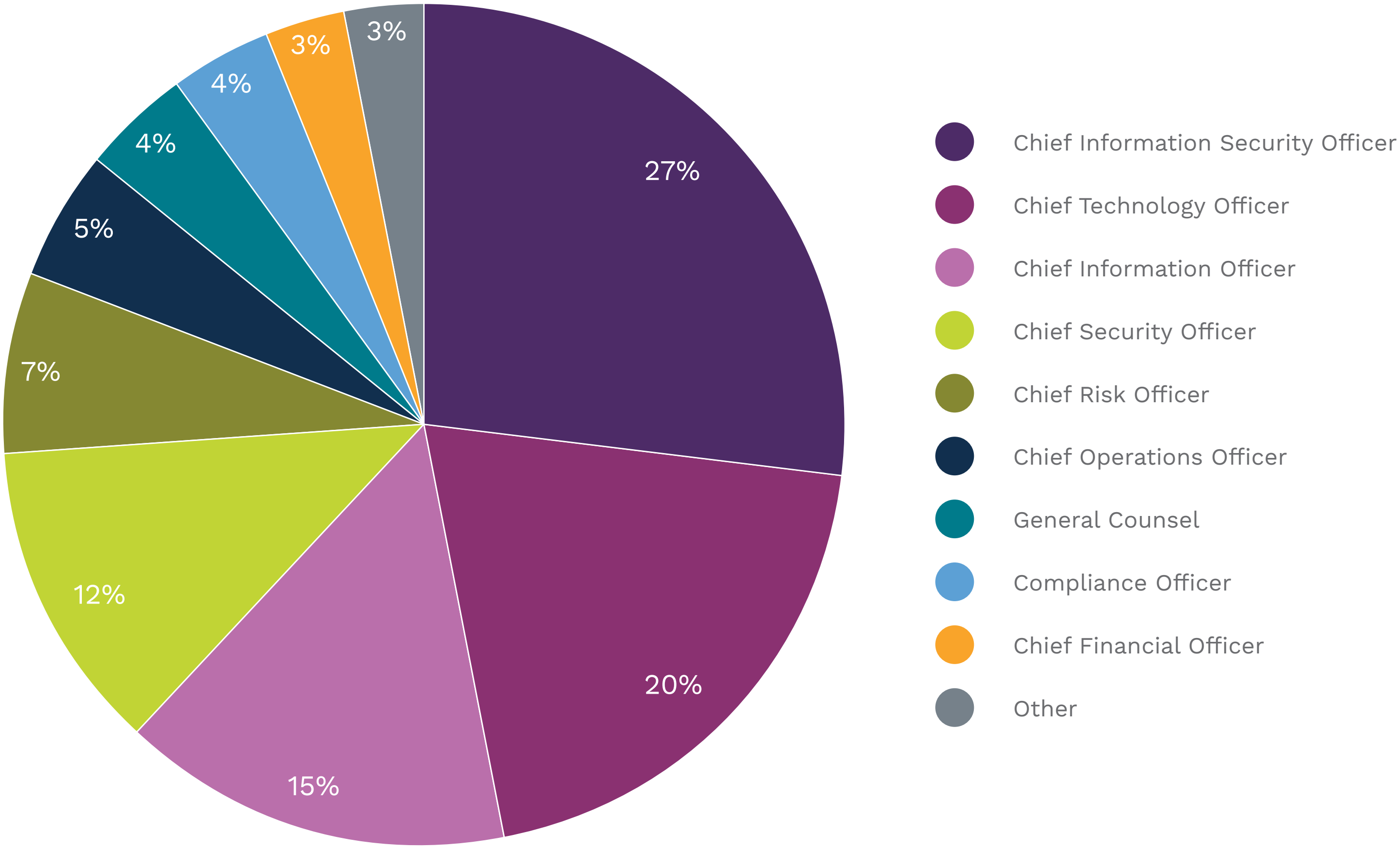
Table 1. Sample response	**Freq**	**Pct%**
Sampling Frame	17,050	100.0%
Total Returns	763	4.5%
Rejected or Screened Surveys	69	0.4%
Final Sample	694	4.1%

Pie Chart 1 reports the respondent's organizational level. By design, more than half (64 percent) of respondents are at or above the supervisory level. The largest category, at 31 percent of respondents, is technician/staff.



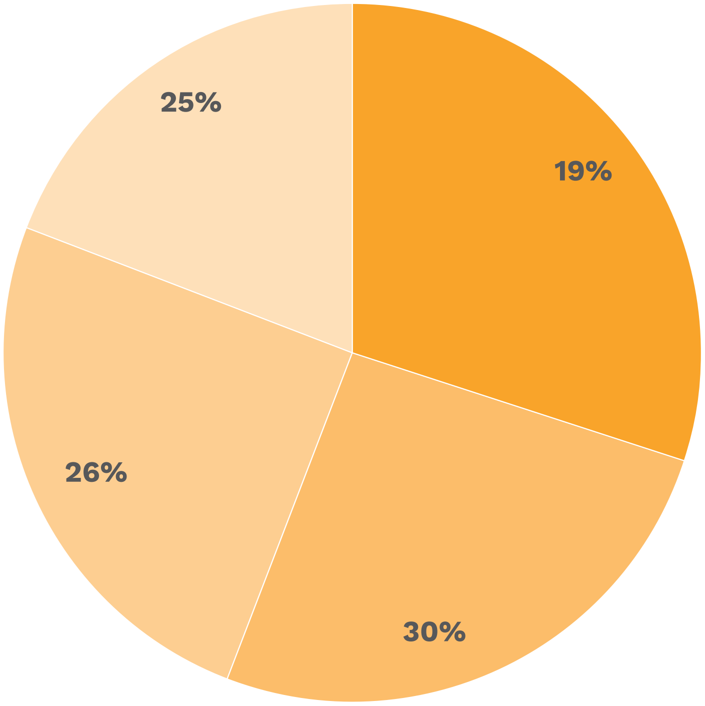
Pie Chart 1. Current Position Within the Organization

As shown in **Pie Chart 2**, 27 percent of respondents report to the chief information security officer, 20 percent report to the chief technology officer, 15 percent report to the chief information officer, 12 percent report to the chief security officer, and 7 percent report to the chief risk officer.



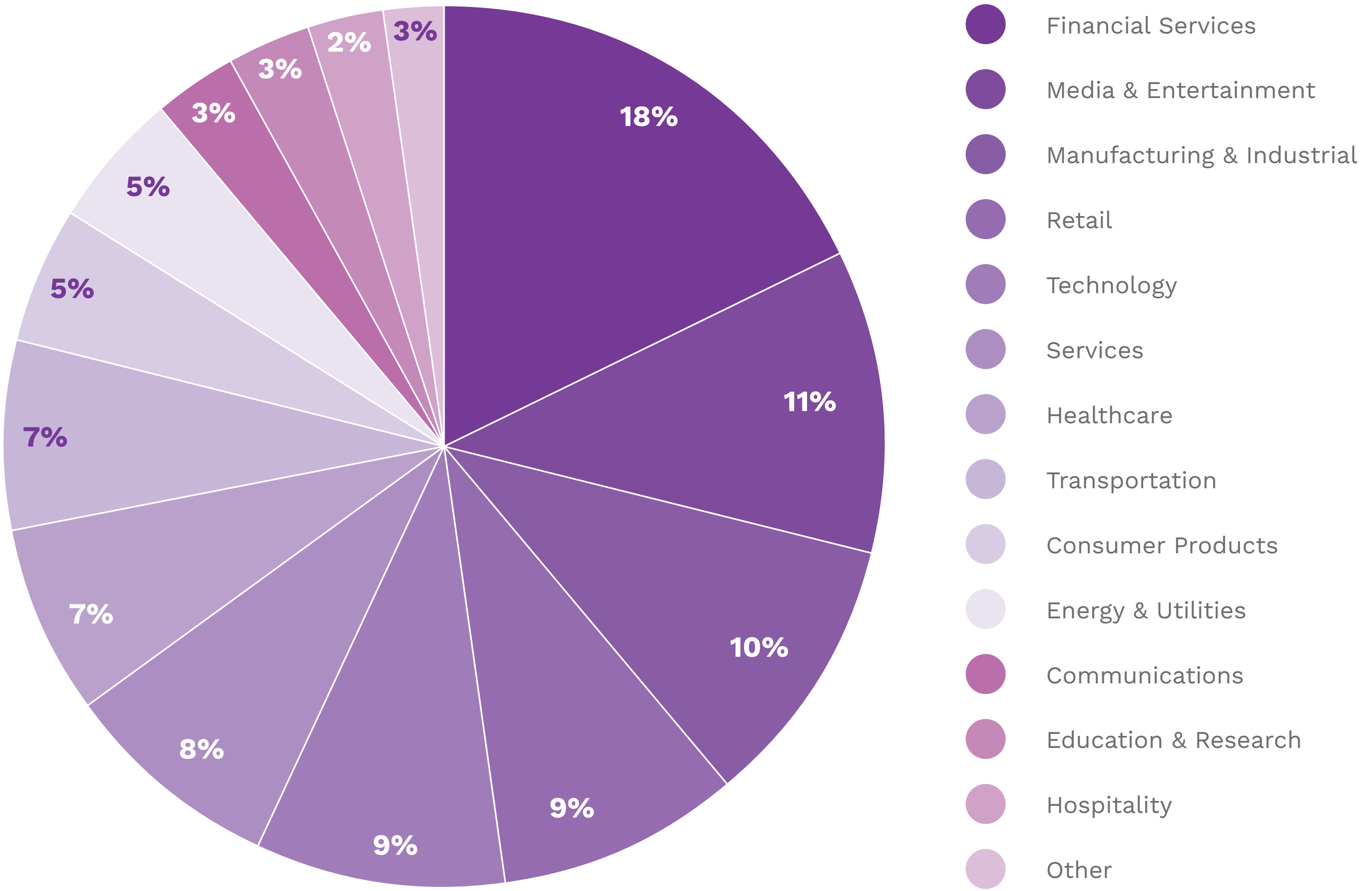
Pie Chart 2. Direct Reporting Channel

As shown in **Pie Chart 3**, 75 percent of respondents are from organizations with a total headcount of more than 5,000.



Pie Chart 3. Total Headcount

Pie Chart 4 reports the industries represented in this research. This chart identifies financial services (18 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments, and credit cards. This is followed by media and entertainment, industrial and manufacturing (10 percent of respondents), retail (9 percent of respondents), technology (9 percent of respondents), and services (8 percent of respondents).



Pie Chart 4. Primary Industry Focus

CAVEATS TO THIS STUDY

Part 4

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-Response Bias

The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling-Frame Bias

The accuracy is based on contact information and the degree to which the list is representative of IT or IT security professionals who are familiar with their organizations' zero-trust strategy. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

Self-Reported Results

The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

APPENDIX WITH DETAILED, AUDITED FINDINGS

Part 5

The following tables provide the percentage frequency of responses to all survey questions.
All survey responses were captured in July 2022.

SURVEY RESPONSE	FREQ
Total sampling frame	17,050
Total survey returns	763
Rejected surveys	69
Final sample	694
Response rate	4.1%

PART 1 SCREENING	Pct%
S1. Has your organization adopted a zero-trust strategy?	
Yes	69%
No (please skip to S3)	31%
Total	100%
S2. How familiar are you with your organization's zero-trust strategy?	
Very familiar	43%
Familiar	41%
Somewhat familiar	16%
Not familiar (stop)	0%
Total	100%
S3. What was the primary reason for not adopting zero trust? Please select only one answer	
No executive buy-in	33%
Too expensive	15%
Lack of internal expertise	12%
Value is unclear/not fully understood	40%
Other (please specify)	0%
Total	100%
S4. Which of the following best describes your role in IT or IT security within your organization? Please select all that apply.	
Setting IT security priorities	45%
Managing IT security budgets	39%
Selecting vendors and contractors	41%
Participating in IT security strategies	35%
Evaluating and measuring the effectiveness of security strategies	37%
Overseeing governance and compliance specific to tool, services and nothing else	49%
None of the above (stop)	0%
Total	280%

PART 2 EFFECTIVENESS IN ZERO-TRUST STRATEGIES	Pct%
Q1. In our organization, zero trust ensures attackers who gain access to users' accounts can only access their specific tools and services and nothing else.	
Strongly agree	29%
Agree	24%
Unsure	17%
Disagree	16%
Strongly disagree	14%
Total	100%
Q2. Our third-party risk management program is thoroughly aligned with zero-trust principles.	
Strongly agree	24%
Agree	25%
Unsure	23%
Disagree	17%
Strongly disagree	11%
Total	100%
Q3. How effective is your organization in determining which of its existing security technologies can be part of the zero-trust implementation to reduce costs on a scale from 1 = not effective to 10 = highly effective?	
1 to 2	8%
3 to 4	17%
5 to 6	25%
7 to 8	27%
9 to 10	23%
Total	100%
Extrapolated value	6.30
Q4. How effective is your organization in prioritizing what new security technologies are needed as part of its zero-trust implementation on a scale from 1 = not effective to 10 = highly effective?	
1 to 2	6%
3 to 4	15%
5 to 6	25%
7 to 8	29%
9 to 10	25%
Total	100%
Extrapolated value	6.54
Q5. How effective were your organization's security practices before implementing zero trust on a scale from 1 = not effective to 10 = highly effective?	
1 to 2	14%
3 to 4	16%
5 to 6	30%
7 to 8	23%
9 to 10	17%
Total	100%
Extrapolated value	5.76

Q6. How effective are your organization's security practices following the implementation of zero-trust strategy on a scale from 1 = not effective to 10 = extremely effective?

1 to 2	7%
3 to 4	12%
5 to 6	23%
7 to 8	30%
9 to 10	28%
Total	100%
Extrapolated value	6.70

Q7. How does your organization's rate of adopting a zero-trust strategy compare to its competitors on a scale from 1 = not keeping pace with competitors to 10 = way ahead of competition?

1 to 2	10%
3 to 4	13%
5 to 6	32%
7 to 8	25%
9 to 10	20%
Total	100%
Extrapolated value	6.14

Q8. How well aligned are your organization's current security tools with its zero-trust roadmap on a scale from 1 = not aligned to 10 = highly aligned?

1 to 2	14%
3 to 4	19%
5 to 6	25%
7 to 8	19%
9 to 10	23%
Total	100%
Extrapolated value	5.86

Q9. How important is zero trust to ensuring customer trust and retention on a scale from 1 = not important to 10 = highly important?

1 to 2	3%
3 to 4	9%
5 to 6	20%
7 to 8	29%
9 to 10	39%
Total	100%
Extrapolated value	7.34

PART 3 THE STATE OF ZERO TRUST IN ORGANIZATIONS	Pct%
Q10. What types of cyberattacks pose the greatest risk to your business? Please select the top 4.	
Data breach involving customer PII, EHI, or payment data	43%
Data breach involving information about our employees	28%
Data breach involving our clients' proprietary information	45%
Exposure of my company's intellectual property or strategic information	31%
Theft of my company's customer list or marketing data	33%
Data breach that could threaten executive safety or privacy	21%
Compromising the integrity of our products and services	26%
Destruction or manipulation of financial data	24%
Disruption of our core business network	48%
Disruption/destruction of connected devices (such as biomedical technologies, controls, systems, robotic devices, automatic teller machines)	54%
Tampering with customer-facing web applications	43%
Other (please specify)	4%
Total	400%
Q11a. Have cyberattacks against your organization increased in the past 12 months?	
Yes	67%
No (please skip to Q12)	33%
Total	100%
Q11b. If yes, what was the increase in cyberattacks?	
Less than 10%	17%
10% to 25%	38%
26% to 50%	21%
More than 50%	24%
Total	100%
Q12. What best describes the maturity of your organization's zero-trust strategy?	
Planning stage – We are planning the adoption and defining what the zero- trust strategy is and how to implement it (please skip to Q14a).	21%
Early adoption stage – Zero-trust activities are planned, defined and partially deployed (please skip to Q14a).	19%
Full adoption stage – most zero-trust activities are deployed across the enterprise The program has C-level support and adequate budget.	33%
Mature stage – Zero-trust activities are fully deployed and maintained across the enterprise. C-level executives are regularly informed about the effectiveness of the program. Program activities are measured with KPIs.	27%
Total	100%
Q13. If your organization has achieved full adoption to a mature stage with zero trust as described above, approximately how long did it take?	
Less than 5 years	29%
5 years to 7 years	43%
More than 7 years	28%
Total	100%

Q14a. Does your IT security team attempt to quantify and track how zero trust is improving your organization's security posture?

Yes, we have a fairly mature measurement and metrics program	35%
Yes, we have a partial program in place	31%
No, we do not quantify and track how zero trust is improving our organization's IT security posture	29%
Other (please specify)	5%
Total	100%

Q14b. If yes, what metrics are used? Please select all that apply.

Reduction in the number of known vulnerabilities	63%
Reduction in the number of threats	57%
Reduction in the frequency of DDoS attacks	45%
Reduction in the number of data breach incidents	65%
Percentage of endpoints free of malware and viruses	47%
Percentage of software applications tested	45%
Percentage of recurring incidents	35%
Other (please specify)	0%
Total	357%

Q15. What obstacles, if any, have impacted your organization's implementation of zero trust? Please select the top three reasons only.

Continued use of legacy technology	65%
Immature business processes	39%
Not a priority in our organization	42%
Lack of budget	40%
Lack of in-house expertise	40%
The length of time to implement zero trust	34%
Push-back from lines of business	37%
Other (please specify)	3%
Total	300%

Q16. What does your organization believe are the primary benefits of zero trust? Please select the top five benefits.

Attack surface reduction (i.e. cloaked servers, workloads and/or data)	38%
Stronger authentication using identity and risk posture	52%
Unsanctioned lateral movement prevention using micro-segmentation	46%
Reduced complexity in securing access to environments	38%
Improved user experience	32%
Increased productivity of the IT security team	54%
Increased productivity of the DevOps team	59%
Reduction in help desk tickets	44%
Reduction in policy management issues	32%
Focus security and IT teams on transformation efforts	28%
Greater network visibility and automation capabilities	35%
Ability to integrate zero trust into DevOps	39%
Other (please specify)	3%
Total	500%

Q17. Which of the following components are in your organization's zero-trust architecture? Please select all that apply.

Identity and access management	52%
Authorization	47%
Automated policy decisions	43%
Ensuring resources are patched	40%
Continuous monitoring with transactions that are logged and analyzed	29%
Repeatable activities that are prone to human errors are automated as much as possible	30%
Behavioral analytics and threat intelligence used to improve asset security	45%
Other (please specify)	5%
Total	291%

Q18. Which of the following components are in your organization's zero-trust security model? Please select all that apply.

Single strong source of identity for users and non-person entities (NPEs)	56%
User and machine authentication	34%
Additional context such as policy compliance and device health	40%
Authorization policies to access an application or resource	49%
Access control policies to access an application or resource	41%
Other (please specify)	3%
Total	223%

Q19. Which of the following poses the most significant risk to your organization's cloud environment? Please select the top four.

Increased attack vectors with more exposed resources	23%
Complexity in managing disparate policy and access solutions for all users and services spanning environments	32%
Ability to scale security at the same speed of cloud scale	33%
Traditional security solutions operating in siloes and not integrating with the broader tool ecosystem	28%
Difficulty segmenting without introducing friction and slowing down development	34%
Lack of knowledge about cloud providers' security and connectivity tools	42%
Network monitoring and visibility	50%
Complexity in enforcing consistent security controls across the cloud infrastructure	65%
Compliance with regulations	55%
In-house expertise with cloud knowledge	36%
Other (please specify)	2%
Total	400%

Q20. How effective is zero trust in reducing risks to cloud security on a scale from 1 = not effective to 10 = highly effective?

1 to 2	38%
3 to 4	52%
5 to 6	46%
7 to 8	38%
9 to 10	32%
Total	100%
Extrapolated value	6.06

Q21. Traditional perimeter-based security solutions such as VPNs, next-gen firewalls, and network access control (NAC) products are ineffective at securing distributed, hybrid cloud infrastructures.

Strongly agree	25%
Agree	23%
Unsure	28%
Disagree	13%
Strongly disagree	11%
Total	100%

Q22. How much zero trust experience does your cloud architect have on a scale from 1 = little experience to 10 = significant experience?

1 to 2	10%
3 to 4	12%
5 to 6	24%
7 to 8	31%
9 to 10	23%
Total	100%
Extrapolated value	6.40

Q23a. How are zero-trust activities handled in your organization?

All activities are conducted in-house	24%
Some activities are conducted in-house (please skip to Q24)	27%
All activities are outsourced to a managed security service (MSSP/MDR) or other third parties (please skip to Q24)	23%
Some activities are outsourced to a managed security service (MSSP/MDR) or other third parties (please skip to Q24)	26%
Total	100%

Q23b. If all zero-trust activities are done in-house, how many hours each week are spent on zero-trust activities?

Less than 10 hours	9%
10 hours to 25 hours	21%
26 hours to 50 hours	28%
51 hours to 75 hours	19%
More than 75 hours	23%
Total	100%
Extrapolated value	45.04

Q23c. Does your organization have staff dedicated to zero trust?

Yes	68%
No	32%
Total	100%

Q23d. If yes, how many IT and IT security staff are dedicated to zero trust?

1 to 2	16%
3 to 5	33%
6 to 10	35%
More than 10	16%
Total	100%
Extrapolated value	6.28

Q24. Does your staff have zero-trust certifcations?

Yes	25%
No	75%
Total	100%

Q25a. Did your organization adopt zero-trust network access as defined in this survey?

Yes	51%
No	49%
Total	100%

Q25b. If yes, why did your organization adopt zero-trust network access? Please select your top two reasons.

Reduce remote access security issues	33%
Improve visibility of user activity and application usage	38%
Reduce connectivity issues and improve user experience	52%
Reduce difficulty in setting up, deploying, enrolling new users, and decommissioning departing users	51%
Understand the state of the devices used to connect to the corporate network	24%
Other (please specify)	2%
Total	200%

PART 4 DWELL TIME AND LATERAL MOVEMENT	Pct%

Q26. How concerned is your organization about lateral movement in its network on a scale from 1 = not concerned to 10 = highly concerned?

1 to 2	5%
3 to 4	12%
5 to 6	19%
7 to 8	15%
9 to 10	49%
Total	100%
Extrapolated value	7.35

Q27. How much does your organization rely upon perimeter security on a scale from 1 = no reliance to 10 = highly reliant?

1 to 2	10%
3 to 4	19%
5 to 6	21%
7 to 8	30%
9 to 10	20%
Total	100%
Extrapolated value	6.18

Q28. When a particular system is compromised, our organization knows how an attacker could use that system to move laterally.

Strongly agree	16%
Agree	23%
Unsure	16%
Disagree	22%
Strongly disagree	23%
Total	100%

Q29. When a particular system is compromised, our organization knows what critical business services can be impacted.

Strongly agree	19%
Agree	20%
Unsure	15%
Disagree	20%
Strongly disagree	26%
Total	100%

Q30. Zero trust has reduced attacker "dwell time" in our network.

Strongly agree	28%
Agree	25%
Unsure	15%
Disagree	19%
Strongly disagree	13%
Total	100%

Q31. How effective is zero trust in eliminating all lateral movement between users and servers because users are removed from the corporate network on a scale from 1 = not effective to 10 = highly effective

1 to 2	13%
3 to 4	12%
5 to 6	19%
7 to 8	27%
9 to 10	29%
Total	100%
Extrapolated value	6.49

Q32. How effective is zero trust in authenticating, authorizing, and inspecting all traffic flow at all times to ensure malware and attacks don't sneak in accidentally or maliciously on a scale from 1 = not effective to 10 = highly effective?

1 to 2	13%
3 to 4	12%
5 to 6	19%
7 to 8	27%
9 to 10	29%
Total	100%
Extrapolated value	7.14

Q33. Which of the following are obstacles to your organization's ability to effectively detect cyber attackers operating within its network? Please select the top four.

Lack of clarity on what threats or threat indicators our organization should look for	43%
Security configurations and security policies are not properly maintained or enforced	46%
Effective detection technologies are not available in the marketplace	39%
Lack of resources to purchase or implement effective detection technologies	27%
Shortage of time or skills to optimize and maintain detection technologies	31%
Necessary data is not being collected or integrated into our organization's detection platforms	34%
Difficulty distinguishing between false positives and "real" alerts	45%
Inability to determine which alerts to escalate	23%
Inability to detect east-west traffic	26%
Complexity of tools/lack of a consolidated security risk management/visibility platform	34%
Compliance activity detracts attention from threat detection functions	24%
Urgent projects or "fire drill" requests detract attention from threat detection functions	23%
Other (please specify)	5%
Total	400%

Q34. Approximately what range best describes your organization's annual IT budget in the current fiscal year?

Less than $1 million	1%
$1 to $10 million	5%
$11 to $25 million	12%
$26 to $50 million	13%
$51 to $100 million	21%
$101 to $250 million	24%
$251 to $500 million	16%
More than $500 million	8%
Total	100%
Extrapolated value (US$ Millions)	$174

Q35. Approximately what percentage of your organization's IT budget is dedicated to IT security?

Less than 5%	4%
5% to 10%	15%
11% to 20%	35%
More than 20%	46%
Total	100%
Extrapolated value	18%

Q36. Approximately what percentage of your organization's IT security budget is dedicated to its zero-trust strategy?

None	6%
Less than 1%	7%
1% to 5%	24%
6% to 10%	23%
More than 10%	40%
Total	100%
Extrapolated value	7.4%

PART 5 YOUR ROLE	Pct%
D1. What organizational level best describes your current position?	
Senior Executive (C-level)	7%
Vice President	9%
Director	15%
Manager	19%
Supervisor	14%
Technician/Staff	31%
Engineer	3%
Other	2%
Total	100%
D2. Check the primary person you report to within the organization	
Chief Information Security Officer	27%
Chief Technology Officer	20%
Chief Information Officer	15%
Chief Security Officer	12%
Chief Risk Officer	7%
Chief Operations Officer	5%
General Counsel	4%
Compliance Officer	4%
Chief Financial Officer	3%
Other	3%
Total	100%
D3. Total headcount	
1,001 to 5,000 people	25%
5,001 to 25,000 people	26%
25,001 to 75,000 people	30%
More than 75,000 people	19%
Total	100%
D4. Industry sector	
Aerospace & defense	1%
Agriculture & food service	1%
Communications	3%
Consumer products	5%
Education & research	3%
Energy & utilities	5%
Financial services	18%
Healthcare	7%
Hospitality	2%
Manufacturing & industrial	10%
Media & entertainment	11%
Retail	9%
Services	8%
Technology	9%
Transportation	7%
Other	1%
Total	100%

Please contact **research@ponemon.org** or call us at **800.877.3118** if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.