Ponemon INSTITUTE

GLOBAL STUDY ON ZERO TRUST SECURITY **FOR THE CLOUD**

Sponsored by:

appgate

Independently conducted by Ponemon Institute LLC

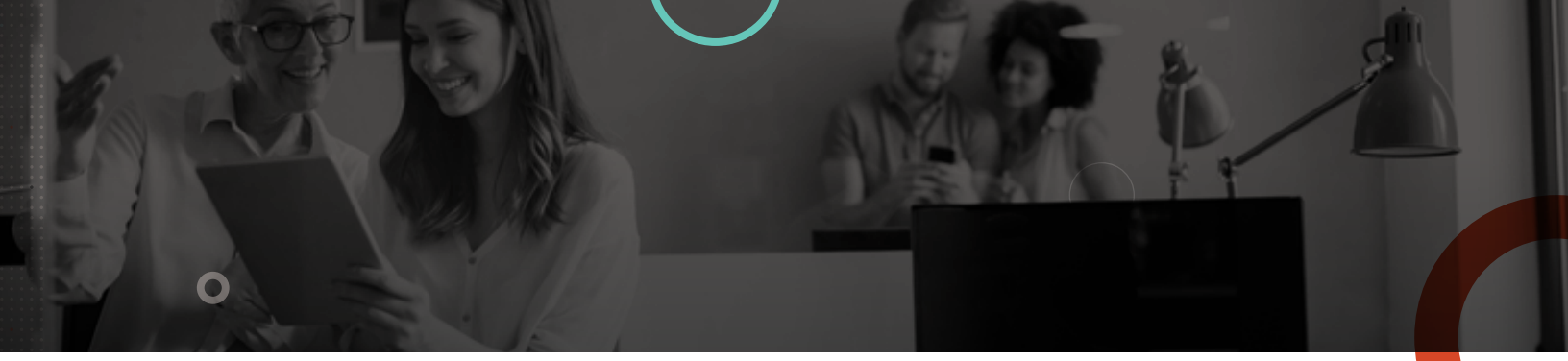
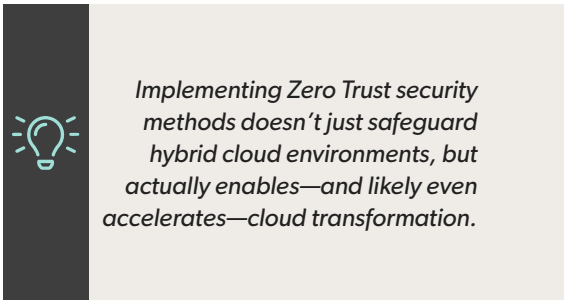


TABLE OF CONTENTS

PART 1. EXECUTIVE SUMMARY

Implementing Zero Trust security methods doesn't just safeguard hybrid cloud environments, but actually enables—and likely even accelerates—cloud transformation, according to a survey of nearly 1,500 IT decision makers and security professionals in the U.S., Europe and the Middle East (EMEA) and Latin America (LATAM).

The survey, conducted by Ponemon Institute on behalf of Appgate, the secure access company, reveals a clear link between the implementation of Zero Trust security measures to mitigate distributed IT infrastructure risks and the realization of cloud transformation objectives.



Different cloud environments, but consistent motivations

This report presents consolidated global findings and insights from the research. According to the study, there is enormous cloud environment diversity in respondents' organizations. Specifically, there are varied mixes of public/private clouds and on-premises infrastructure, different adoption rates for containers and disparate portions of IT and data processing in the cloud. However, as the research reveals, the drivers of cloud investments are broadly consistent from region to region.

Overall, increasing efficiency is the top motivation for cloud transformation, according to 62 percent of respondents. The second most common motivation is reducing costs (53 percent) followed by a virtual tie between improving security (48 percent) and shortening deployment timelines (47 percent).

New cybersecurity risks not addressed by traditional solutions

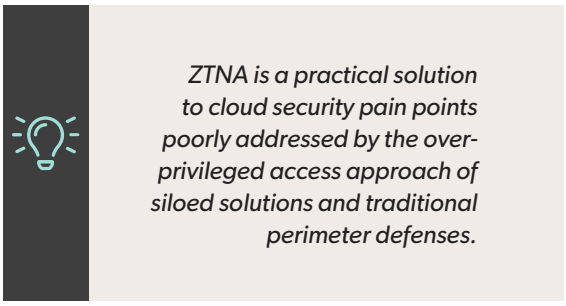
But cloud transformation has its own set of security risks and challenges. In fact, nearly 50 percent of respondents flag network monitoring and visibility difficulties as the most significant challenge, followed by a lack of in-house expertise (45 percent) and a recognition of the increased attack vectors that come with having more resources in the cloud (38 percent).

Focusing on specific security threats, 59 percent of study participants indicate account takeover or credential theft is a major concern, just ahead of third-party access risks. This points to widespread worries about secure access to cloud resources by an organization's users and outside vendors/suppliers alike.

Addressing cloud security risks is a known hurdle, with 36 percent of respondents reporting that the siloed nature of traditional security solutions creates cloud integration challenges. Modern "shift left" development methodologies only partially address the issue and may even add new risks into the mix. For instance, 52 percent of respondents agree or strongly agree that the inability of current network security controls to scale fast enough affect DevOps productivity or introduce vulnerabilities.

Zero Trust Network Access (ZTNA) offers a proven solution

The research also reveals that Zero Trust Network Access (ZTNA) is a practical solution to cloud security pain points poorly addressed by the over-privileged access approach of siloed solutions and traditional perimeter defenses. As evidence, the top two security practices identified as being the most important to achieving secure cloud access are enforcing least privilege access (62 percent of respondents) and evaluating identity, device posture and contextual risk as authentication criteria (56 percent of respondents).



Ranking third and fourth are a consistent view of all network traffic across IT environments (53 percent of respondents) and cloaking servers, workloads and data to prevent visibility and access until the user or resource is authenticated (51 percent of respondents). The robust capabilities of ZTNA directly addresses all four of these major cloud security practices deemed as necessities.

Zero Trust is a victim of its own success

The survey also hints that Zero Trust security may be dismissed by some as a buzzword despite high-profile industry calls for action, including a U.S. White House mandate for federal agencies to meet a series of Zero Trust security requirements by 2024. However, there is evidence that this dismissal is based on a poor understanding of what Zero Trust actually is. For example, of those respondents who have not deployed Zero Trust measures, roughly a quarter of respondents point to it as being "just about marketing." Many of these respondents also highlight specific ZTNA capabilities as being essential to protect cloud resources.

Similarly, many of the respondents who indicate their organizations are not implementing Zero Trust nevertheless believe that security components that strongly align with Zero Trust security principles are important. This further indicates the confusion about what Zero Trust security actually means.

Those who have knowingly adopted Zero Trust tenets (49 percent of respondents) report a range of benefits. Of this 49 percent of respondents, 65 percent say the top benefit is increased productivity of the IT security team, followed by stronger authentication using identity and risk posture (61 percent) and a tie between increased productivity for DevOps and greater network visibility and automation capabilities (both 58 percent).

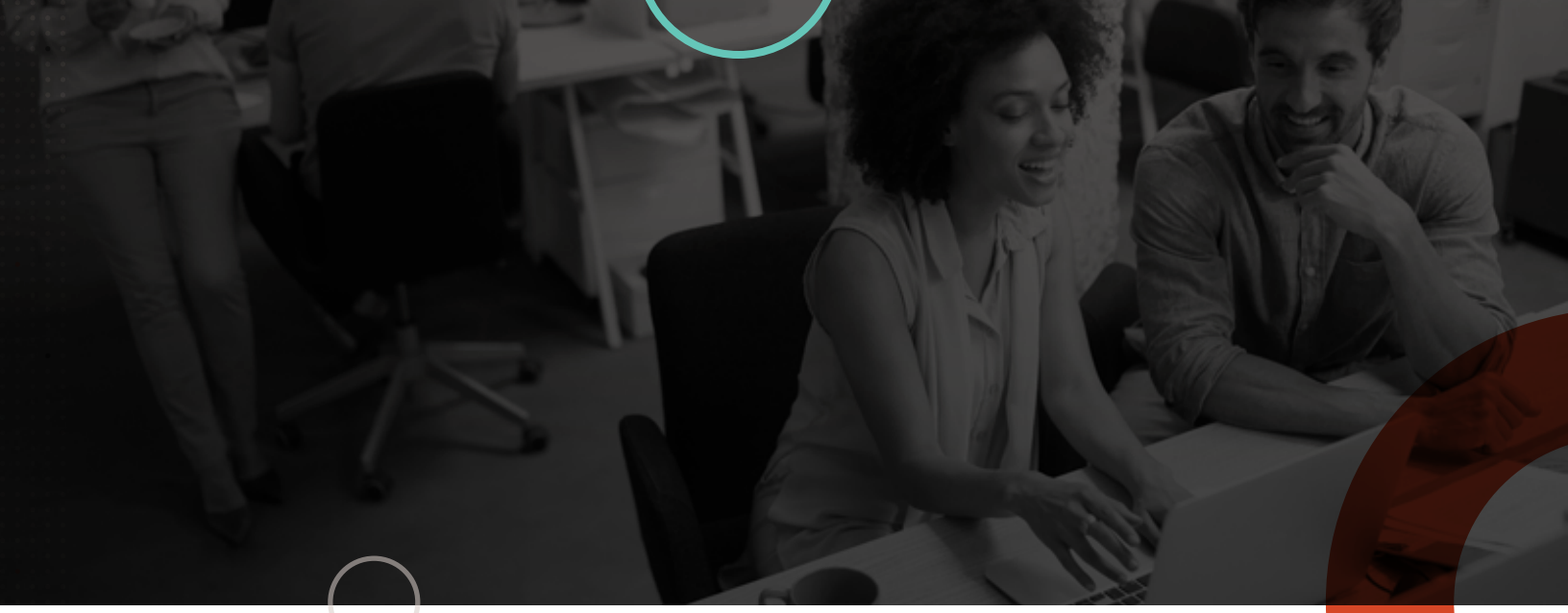
Zero Trust is an enabler—not an add-on

These benefits suggest that Zero Trust goes beyond "simply" protecting valuable data and mission-critical services within hybrid cloud environments. In fact, it can drive enterprise productivity gains and accelerate digital transformation. In other words, Zero Trust security principles shouldn't be regarded as something to add after completing a cloud migration, but instead can be recognized as supporting the speeding up and securing of the transformation.

Ultimately, the speed of business is only going to continue to accelerate the adoption of cloud, containers, DevOps and microservices. Zero Trust security can help organizations quickly and securely keep pace with agile cloud deployments. A comprehensive Zero Trust Network Access solution is the unified policy engine glue that delivers secure access for all users, devices and workloads, regardless of where they reside.

The cloud train has left the station and continues to accelerate without regard for increased risk and security complexity. The results of this study demonstrate the ability for Zero Trust principles to help security keep pace.

A comprehensive ZTNA solution is the unified policy engine glue that delivers secure access for all users, devices and workloads, regardless of where they reside.



PART 2.
KEY FINDINGS

This section presents the research findings on the following topics:

- Diversity in cloud environments
- Obstacles to securing diverse cloud environments
- Zero Trust and other solutions to common cloud security problems
- Lessons learned from high-performing organizations

The complete survey questions and findings are presented in the Appendix of this report.

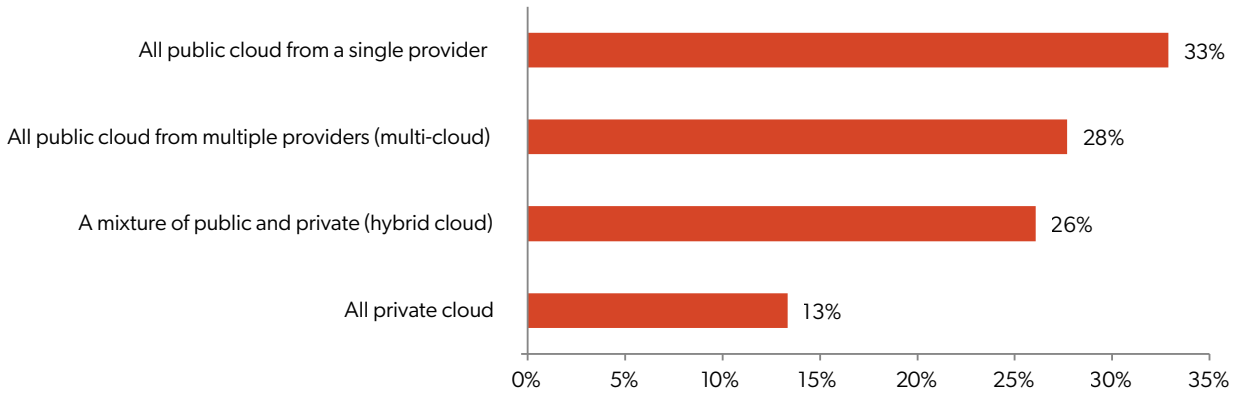
Diversity in cloud environments

AT A GLANCE

- Motivations for adopting cloud environments are many and varied, with increased efficiency, reduced cost, improved security and shorter deployment times cited most frequently.
- There is, and will continue to be, enormous diversity in cloud environments. As a result, architectures leveraging a containerized, microservices-oriented, multi-cloud architecture will be the most common.
- Within the next two years, the total IT and data processing in the cloud will increase from 45 percent of an organization's needs to an average of 53 percent. At the same time, on-premises processing will remain important for years to come further adding to complexity in applying security policies.

There is enormous diversity in the cloud environment. As shown in Figure 1, 87 percent of respondents say their organizations use some form of public cloud—whether from a single provider (33 percent), multiple providers (28 percent) or as part of a hybrid environment (26 percent). Only 13 percent of respondents say their organizations use private cloud exclusively.

Figure 1. What best describes your cloud hosting infrastructure?



On average, those with some form of a public cloud infrastructure estimate that 46 percent of their applications run in the public cloud. Multi-cloud organizations reported an average of four different clouds, while hybrid cloud organizations average three different clouds.

The majority of respondents whose organizations don't have a multi-cloud environment today plan to adopt this architecture in the near term. Twenty-four percent of respondents indicate the shift will happen in the next six months, 16 percent of respondents expect to make the transition in the next year and 14 percent of respondents plan to follow in the next two to three years.

If those organizations are already using a multi-cloud architecture maintain this approach, the findings indicate that three years from now 67 percent of organizations represented in this study will have a multi-cloud environment.

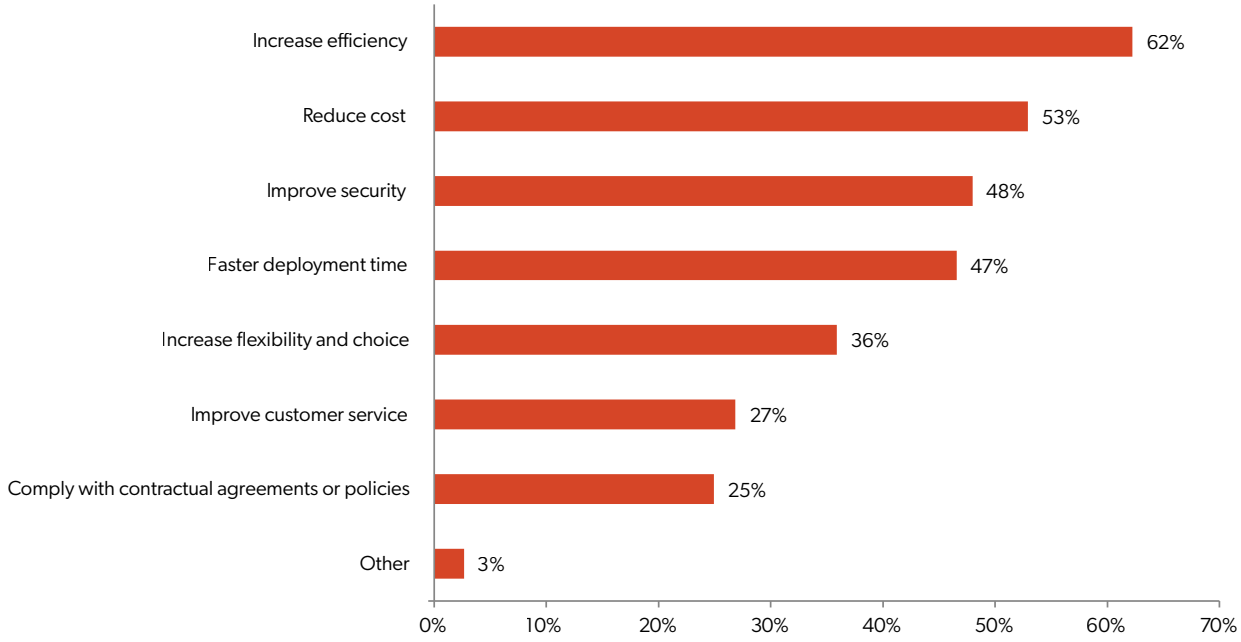
Multi-cloud organizations reported an average of four different clouds; hybrid cloud organizations average three.

Three years from now 67% of organizations represented in this study will have a multi-cloud environment.

As shown in Figure 2, increasing efficiency (62 percent of respondents) and reducing costs (53 percent of respondents) are the primary reasons why organizations use cloud resources. About half of respondents (48 percent) say it is to improve security narrowly edging out faster deployment time (47 percent).

Figure 2. What are the primary reasons cloud resources are used within your organization?

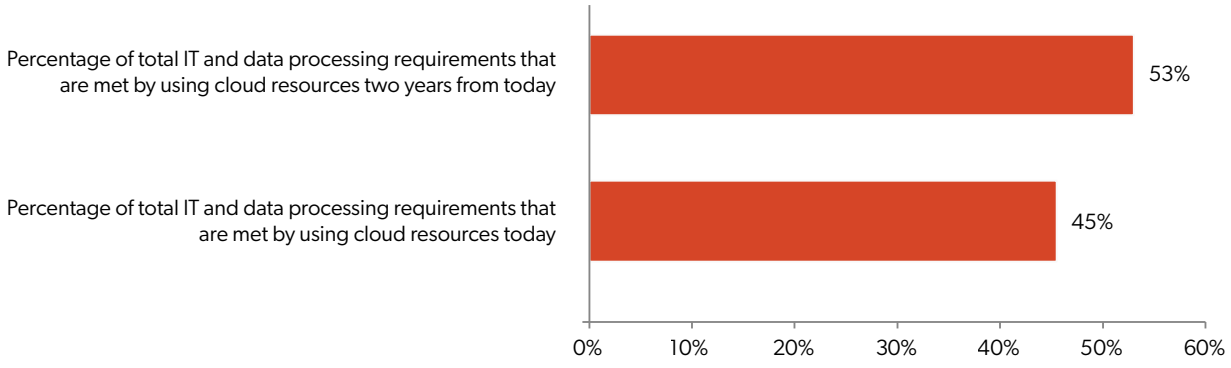
Three responses permitted



Total IT and data processing in the cloud will increase significantly. According to Figure 3, today an average of 45 percent of organizations' total IT and data processing requirements are in the cloud, and this will increase to an average of 53 percent two years from today. This can be attributed to respondents' perceptions that the cloud improves efficiencies and reduces costs as discussed above.

Figure 3. What percentage of your organization's total IT and data processing requirements are met by using cloud resources today and two years from now?

Extrapolated values presented



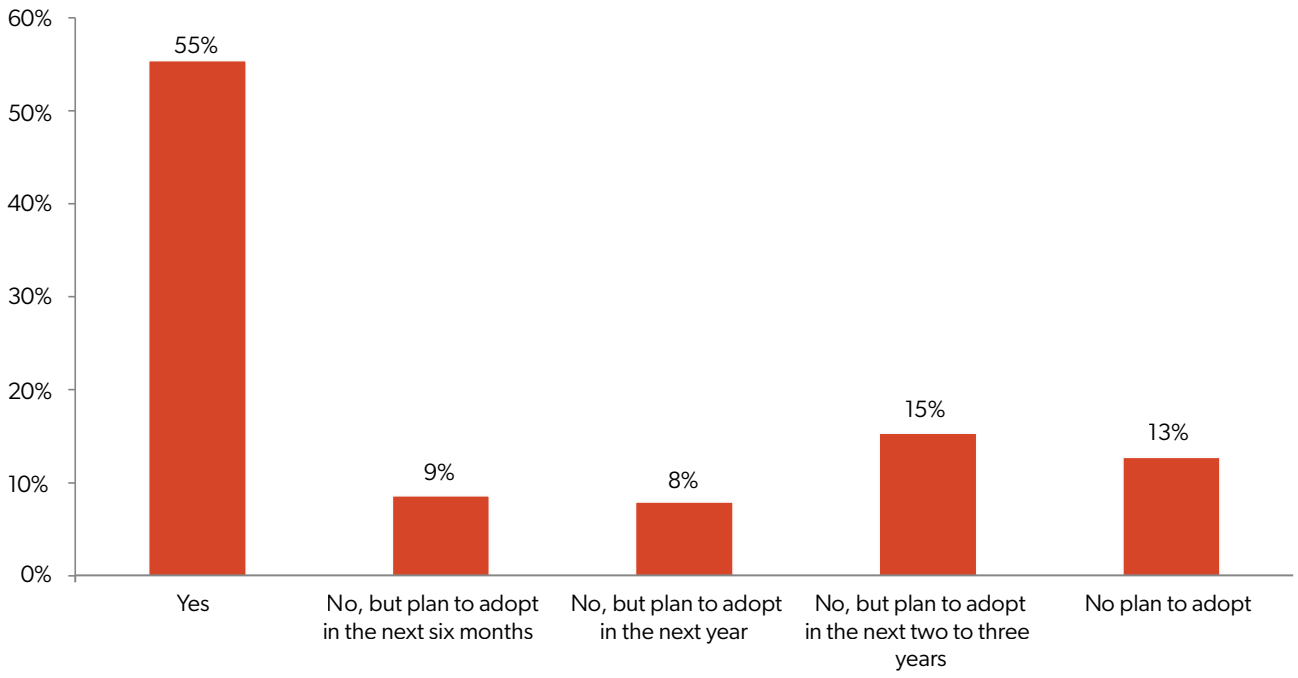
Containers are important in the use of the cloud and most organizations are adopting them. Containers are executable units of software in which application code is packaged, along with its libraries and dependencies, in common ways so that it can be run anywhere, whether on a desktop, traditional IT systems or the cloud. On average, 55 percent of organizations' applications are built using containers.

In addition, 61 percent of respondents say their organizations are using containers for microservices architectures and another 32 percent of respondents say they will use containers for microservices architecture within the next two to three years.

According to Figure 4, 55 percent of respondents say their organizations have already adopted the use of containers and another 32 percent of respondents say they will adopt them within the next two to three years. Only 13 percent of respondents say their organizations have no plans to adopt.

*While **microservices architectures** enable developers to accelerate application delivery, they also introduce new cybersecurity challenges. For example, applications that use a microservices architecture are more complicated and more open than their monolithic counterparts. Plus many APIs are needed to facilitate communication between different microservices, resulting in a greatly expanded attack surface.*

Figure 4. Has your organization adopted the use of containers for the cloud?



Barriers to securing diverse cloud environments

AT A GLANCE

- Only a minority of respondents express high confidence in their organizations' ability to segment their environments and apply the principle of least privilege.
- Although monitoring and visibility are essential elements of cyber defense, implementing these functions effectively is cited as the most significant cloud security challenge—with the issue likely exacerbated both by the siloed nature of traditional security solutions and a lack of specific cloud skills and expertise.
- A strong majority of respondents view perimeter-oriented solutions as ill-equipped to protect cloud infrastructure from the most significant threats, which experts believe to be account takeover, credential theft and risks related to third-party access

Organizations struggle to effectively segment networks as mitigations against the risk of lateral movement and insecure access. The purpose of network segmentation is to improve network performance and security by dividing a network into smaller parts. Through segmentation, organizations can stop all traffic in one part from reaching another or limit the flow by traffic type, source destination and other options.

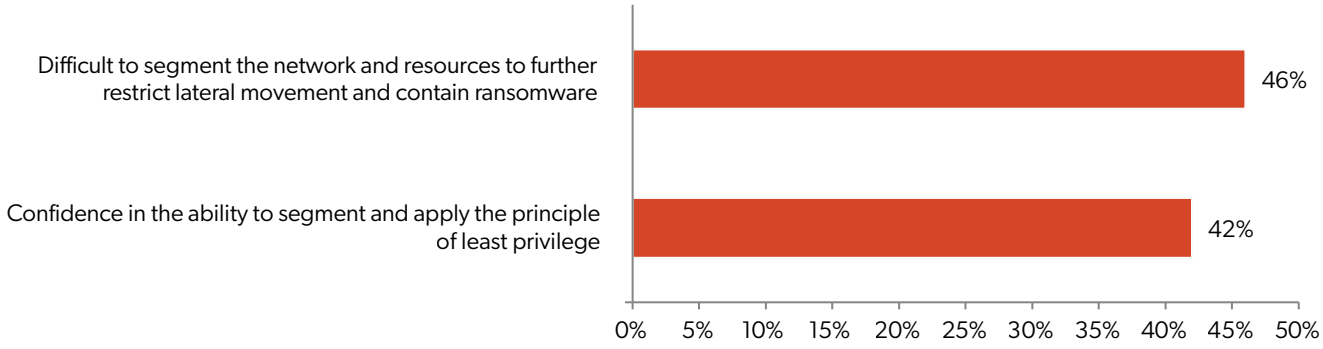
Respondents were asked to rate the difficulty of segmenting the network and resources to further restrict lateral movement and contain ransomware on a scale from 1 = not difficult to 10 = very difficult. Figure 5 presents the very difficult responses (7+ on the 10-point scale). As shown, almost half (46 percent of respondents) say segmenting is very difficult.

Similarly, only 42 percent of respondents are very confident in the ability to segment the network and apply the principle of least privilege.

*As defined in this research, **least privilege** is the practice of only assigning the minimum necessary rights to a user who requests access to a resource and should be in effect for the shortest duration necessary.*

Figure 5. Difficulty in achieving effective segmentation and confidence in the ability to apply least privilege

On a scale from 1 = not confident/difficult to 10 = very confident/difficult, 7+ responses presented



Monitoring is critical to having visibility across the entire network and improving cloud security. However, many organizations say it is the most significant challenge. According to Figure 6, almost half of respondents (48 percent) say network monitoring to achieve visibility is the top challenge.

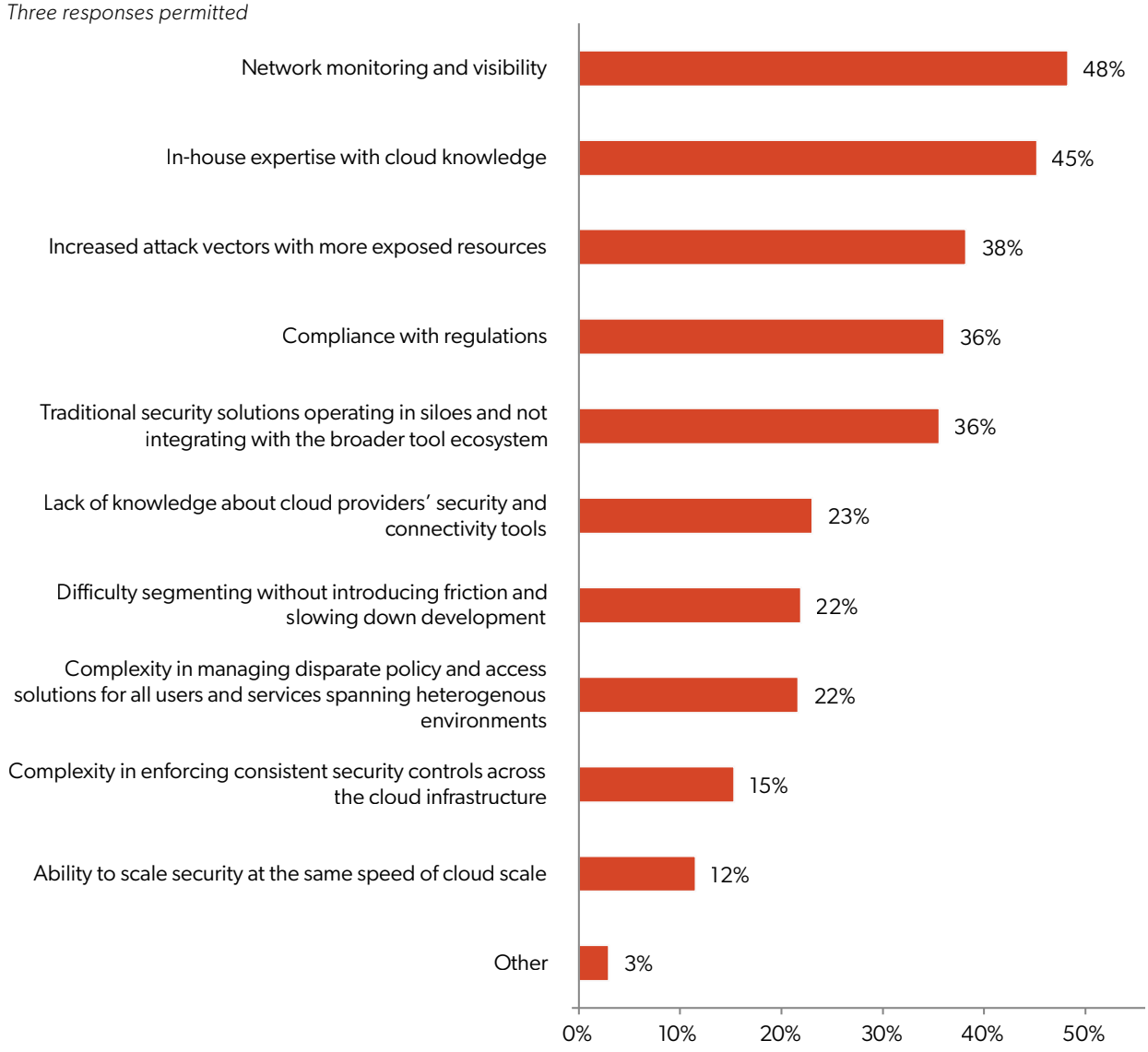
To improve the ability to monitor, organizations need tools that provide detailed analytics, easy to understand real-time information to gain visibility and multiple user interfaces to accommodate the use of smartphones and tablets in a remote/hybrid workforce. The tools should also provide customizable alerts when there are anomalies in the network, breaches or device disconnections.

Almost half of respondents say network monitoring to achieve visibility is the top challenge.

Other challenges are not having the personnel who have cloud security expertise (45 percent of respondents) and the increase in attack vectors with more exposed resources (38 percent of respondents).

Figure 6. What are the most significant challenges to having a secure cloud environment?

Three responses permitted



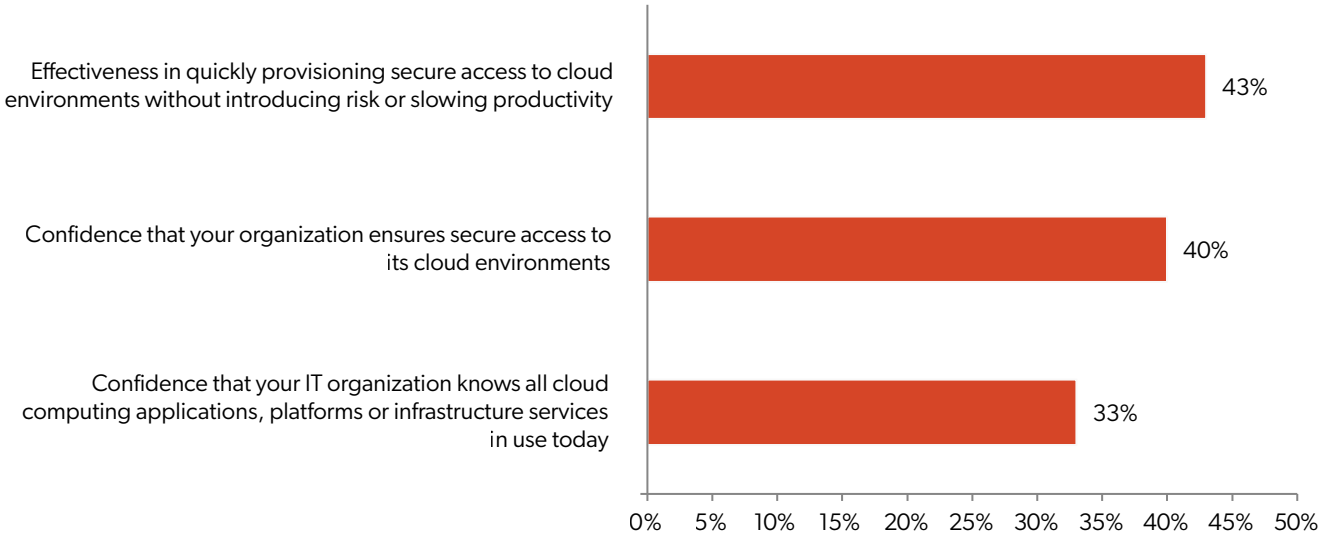
To effectively secure the cloud, organizations need greater visibility of their cloud infrastructures and the ability to secure access to their cloud environments. Respondents were asked to rate their organizations' confidence in the ability to know all cloud computing applications, platforms or infrastructure services on a scale from 1 = no confidence to 10 = very confident.

As shown in Figure 7, only 33 percent of respondents say their organizations have confidence in having such visibility. With respect to secure access, only 40 percent of respondents are confident that their organization ensures secure access to its cloud environments and only 43 percent of respondents say their organizations are very effective in quickly provisioning secure access to cloud environments without introducing risk or slowing productivity.

Only 40 percent of respondents are confident that their organization ensures secure access to its cloud environments.

Figure 7. Confidence and effectiveness in securing the cloud

On a scale from 1 = not confident/effective to 10 = very confident/effective, 7+ responses presented



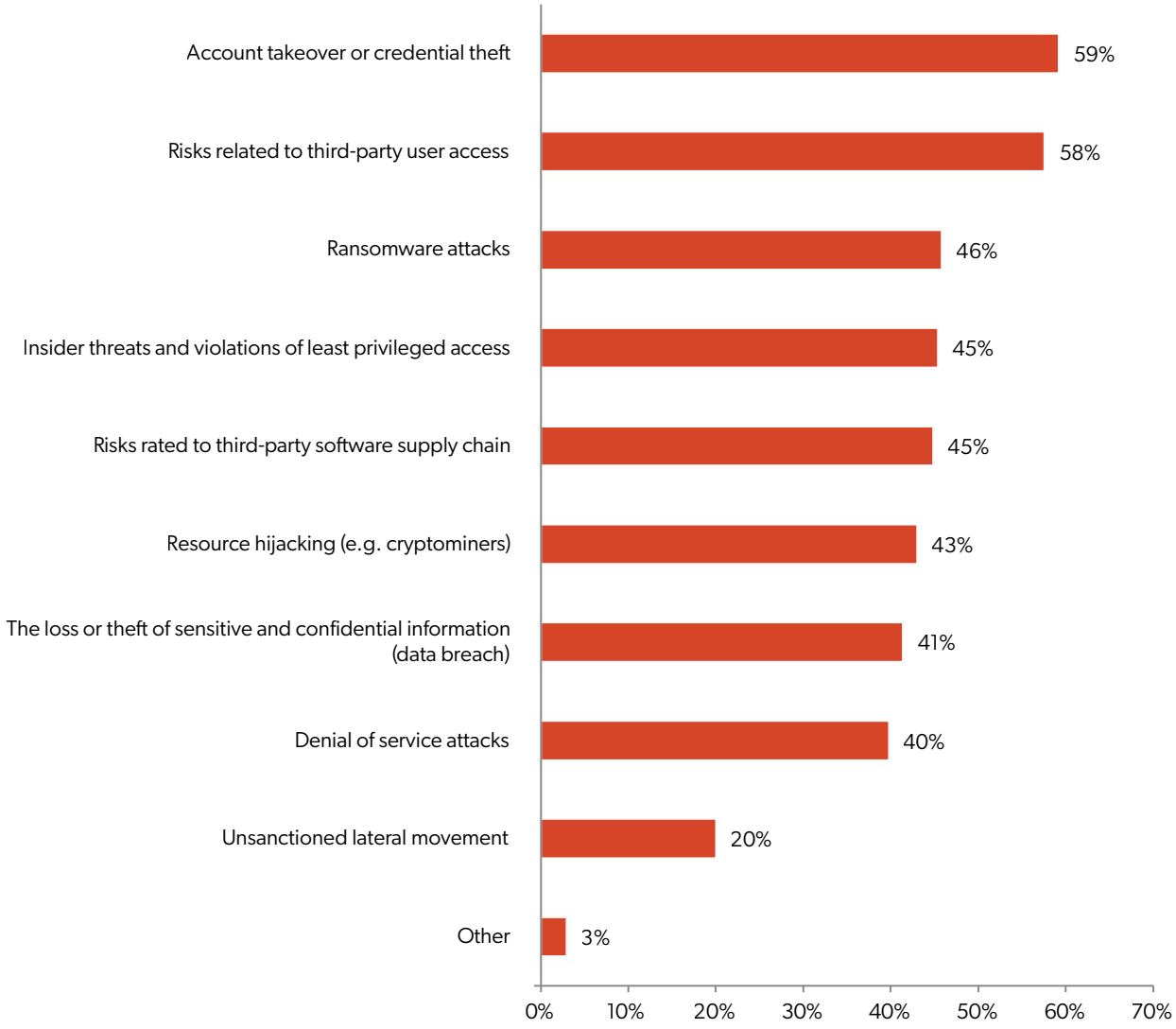
Risks related to attacks against insiders' credentials and insecure third-party access are the top threats to the cloud infrastructure. Figure 8 presents a list of threats to the cloud infrastructure. The top two threats are concerns that bad actors will steal employees' account information and credentials to gain access to sensitive and confidential information in the cloud (59 percent of respondents) followed by the inability to ensure the security of third-party access to the cloud (58 percent of respondents). The top five threats all concern the security of cloud access.

Authentication credentials are a common target during intrusions because they can be used to facilitate account takeover attacks and to gain access to sensitive information. At the same time, detecting credential misuse presents significant challenges. Accordingly, account takeover and credential theft was the number one threat.

Similarly, many organizations rely upon third-party service providers who often need access to sensitive data and systems. While outsourcing functions is a proven strategy, it does introduce new risks and creates additional access management complexities. Fifty-eight percent of respondents say third-party access is a major threat.

Figure 8. What are the top threats to your organization's cloud infrastructure?

Four responses permitted

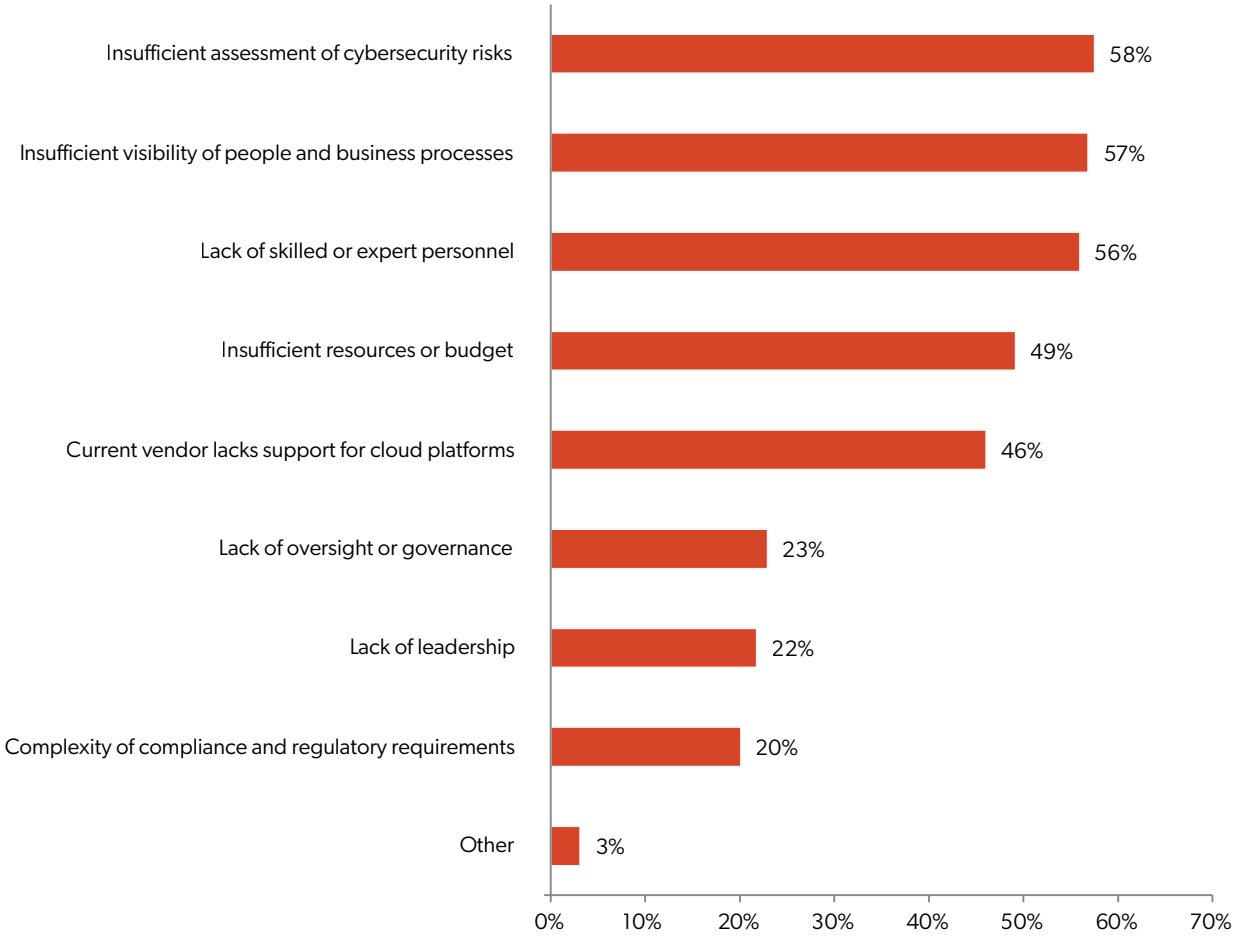


To achieve security in the cloud and in digital transformation, organizations need to understand their cybersecurity risks. Figure 9 presents a list of the barriers to securing the cloud. A recurrent theme of this research is the inability to understand and have visibility into the threats facing organizations. Fifty-eight percent of respondents say an insufficient assessment of cybersecurity risks and visibility of people and business processes are the most significant barriers. These barriers are followed by a lack of skilled or expert personnel (56 percent of respondents).

The fact that 58 percent of respondents report an insufficient assessment of cybersecurity risks should be a concern for at least two reasons. First, understanding risk is a crucial element of any proactive security program. While reactive capabilities are an essential component, proactive preparation and defenses are vital for limiting incident volume and impact. Second, the risk-based approach is emerging as a cost-effective and attainable alternative to maturity-based and compliance-based approaches that are beyond the reach of many organizations, so getting the most out of every dollar invested in security requires understanding risks.

Figure 9. What are the most significant barriers to achieving a secure digital transformation process and cloud adoption?

Four responses permitted

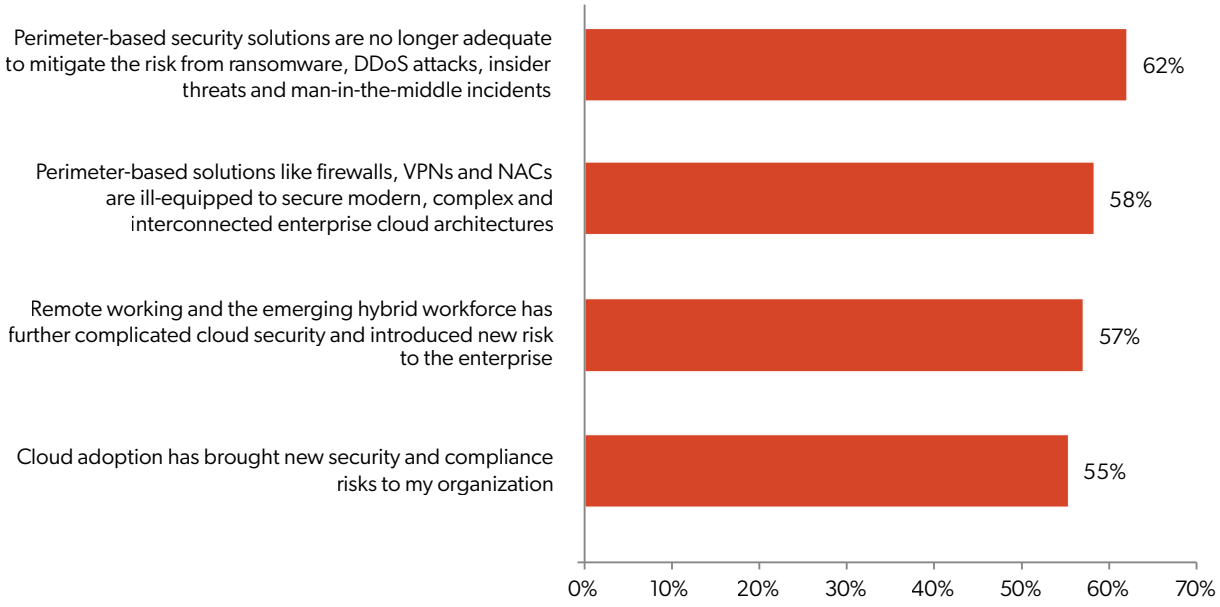


Perimeter-based security solutions are considered inadequate to reducing threats in modern, complex and interconnected enterprise cloud architectures. As shown in Figure 10, 62 percent of respondents say perimeter-based security solutions are no longer adequate to mitigate the risk from ransomware, DDoS attacks, insider threats and man-in-the middle incidents and 58 percent of respondents say solutions such as firewalls, VPNs and NACs are not equipped to secure modern, complex and interconnected enterprise cloud architectures.

Fifty-seven percent of respondents cite the remote/hybrid workplace as introducing new risk to organizations and 55 percent of respondents say moving to the cloud brings new security and compliance risks.

Figure 10. Perceptions about cloud security

Strongly agree and agree responses combined



Zero Trust and other solutions to cloud security problems

AT A GLANCE

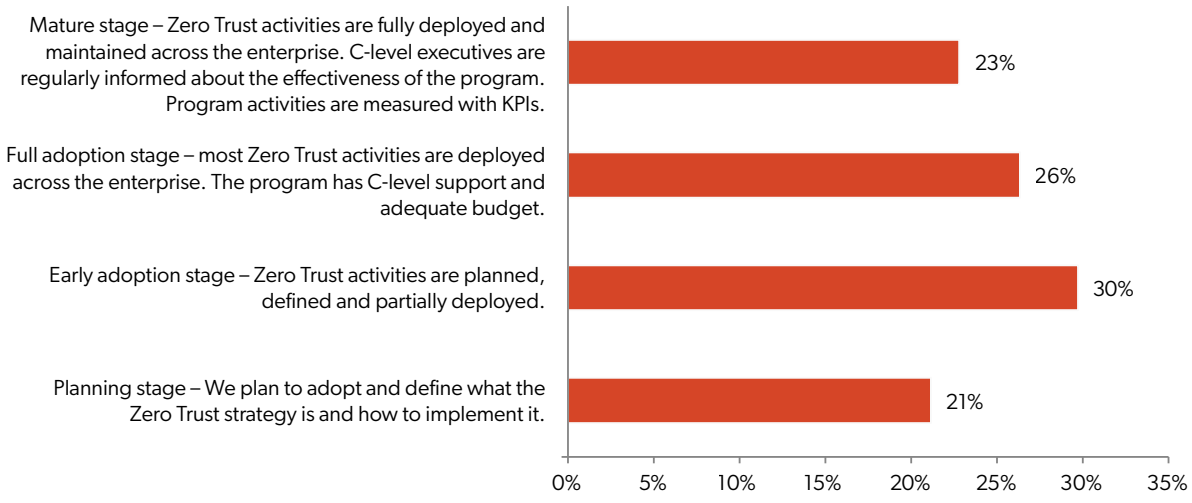
- Adopting and implementing Zero Trust is not a one-and-done activity, but a progressive process. Similarly, securing the cloud is achieved through the interplay of many practices, rather than a "silver bullet" feature or capability.
- Organizations that have adopted Zero Trust report that doing so directly supported their motivations for pursuing cloud transformations in the first place—including increasing efficiency and reducing cost through productivity gains.
- The most common reasons why some organizations have not yet adopted Zero Trust are contradicted by the experiences of those organizations that have already done so.

The lack of Zero Trust maturity is preventing many organizations from realizing its benefits. Forty-nine percent of respondents say their organizations have adopted Zero Trust with different levels of maturity. As shown in Figure 11, 51 percent of respondents say their organizations are in the planning stage (21 percent) or in the early adoption stage (30 percent). Only 23 percent of respondents say their organizations have achieved full maturity.

The different levels of maturity suggests that Zero Trust is not a one-and-done activity. Rather it should be achieved in a step-by-step manner and integrated into other IT and cybersecurity programs.

According to NIST, Zero Trust architecture is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets and resources. A Zero Trust architecture uses Zero Trust principles to plan industrial and enterprise infrastructure and workflows. Zero Trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location or based on asset ownership.

Figure 11. Maturity of organizations' Zero Trust strategy

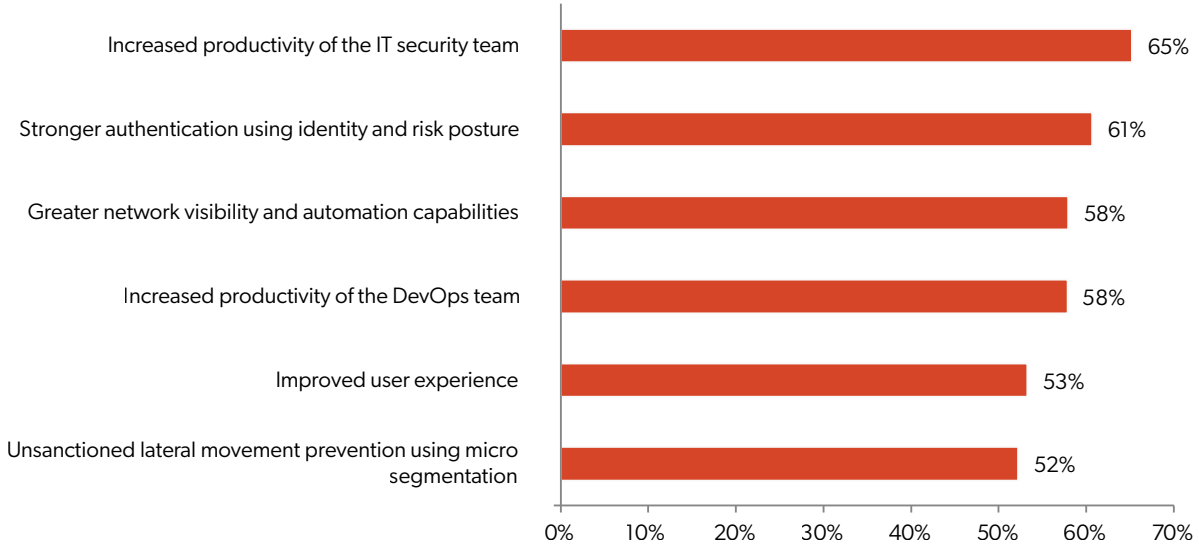


Zero Trust increases the productivity of the IT security team and the ability to ensure accurate authentication. According to Figure 12, 65 percent of respondents say Zero Trust increases the productivity of the IT security team perhaps because of confidence in controls over unauthorized access. Sixty-one percent of respondents say a benefit is stronger authentication using identity and risk posture. Zero Trust also addresses specific challenges highlighted elsewhere in this report such as a lack of visibility into environments and difficulty segmenting resources.

65% of respondents say Zero Trust increases the productivity of the IT security team.

Figure 12. The top six benefits of Zero Trust

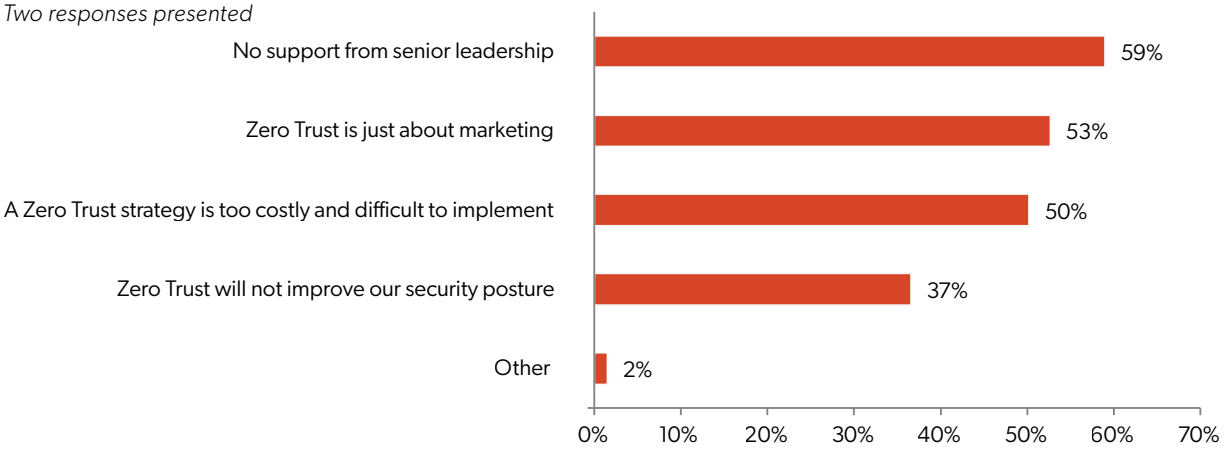
More than one response permitted



Fifty-four percent of organizations have no plan to purchase ZTNA. The reasons are presented in Figure 13. The primary reason is no support from senior leadership (59 percent of respondents) or Zero Trust is just about marketing (53 percent of respondents).

Figure 13. Why would your organization not adopt Zero Trust?

Two responses presented

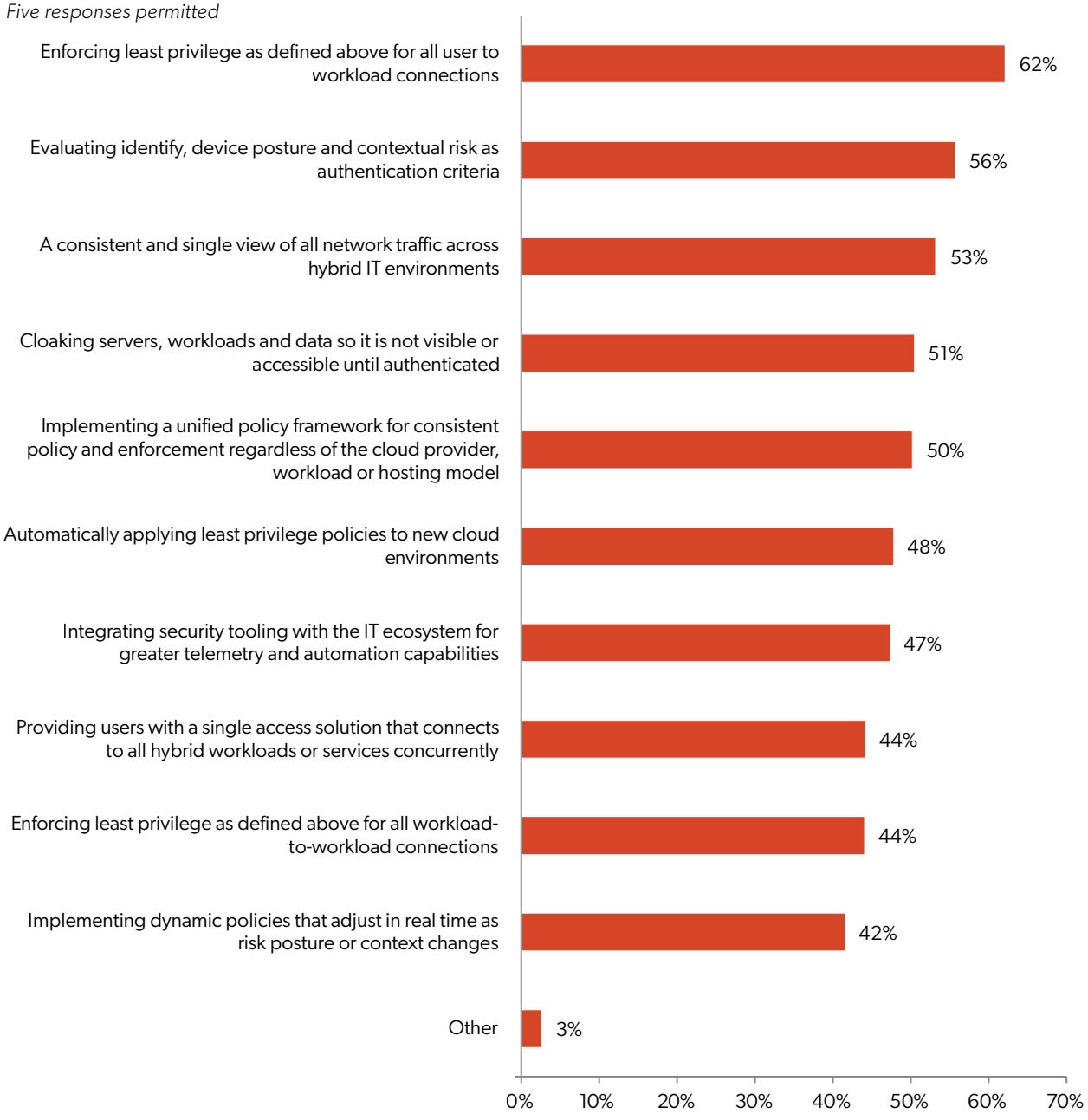


Enforcement of least privilege is the most important practice to achieving secure cloud access. Figure 14 presents a list of practices to achieve secure cloud access. The number one is enforcing least privilege for all user to workload connections (62 percent of respondents) followed by identifying device posture and contextual risk as authentication criteria (56 percent of respondents). Fifty-three percent of respondents say a consistent and single view of all network traffic across hybrid IT environments is important. Many of these practices are core principles of Zero Trust security or features within ZTNA solutions and are considered important to securing the cloud.

Enforcement of least privilege is the most important practice to achieving secure cloud access.

Figure 14. Practices to achieving secure cloud access

Five responses permitted



Organizations are adopting DevOps at a rapid pace, but there is considerable room for improvement in the collaboration between the IT security and DevOps teams. Fifty percent of respondents say their organizations have adopted DevOps and another 40 percent say it will be adopted within the next two to three years.

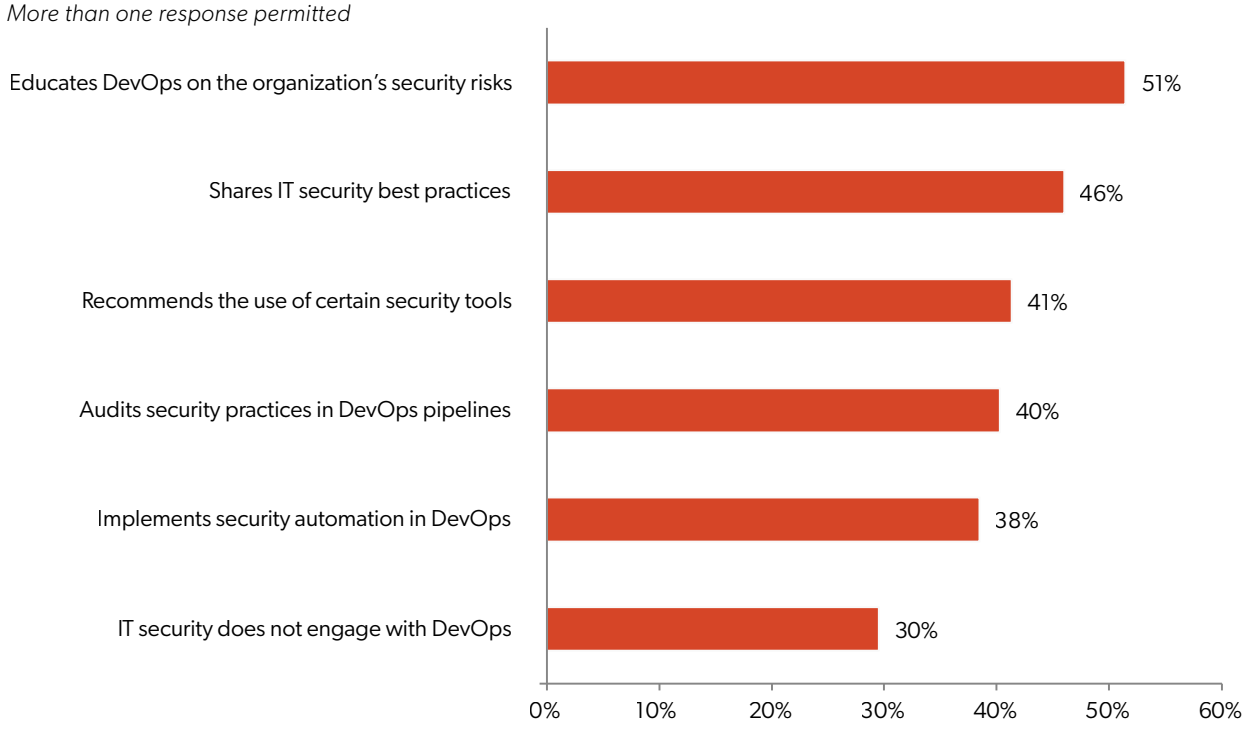
DevOps increases an organization's ability to deliver applications at a faster pace than when using traditional software, development and infrastructure management processes. To ensure security is embedded in the development of applications, IT security should collaborate with DevOps. However, as shown in Figure 15, 30 percent of respondents say their organizations do not engage with DevOps.

50% of respondents say their organizations have adopted DevOps and another 40% say it will be adopted within the next two to three years.

IT security primarily educates DevOps on the organization's security risks (51 percent of respondents) and 46 percent of respondents say IT security shares best practices with DevOps. However, only 40 percent of respondents say IT security audits security practices in DevOps development pipelines. It is surprising that given today's threat landscape only 38 percent of respondents say their organizations implement security automation in DevOps.

Figure 15. How does IT security collaborate with DevOps?

More than one response permitted



Lessons learned from organizations that are very confident in securing access to their cloud environments

AT A GLANCE

- High performers are more likely to point to the limitations of traditional security solutions as a major impediment to securing the cloud environment.
- High performers are more likely to view account takeovers, credential theft and data breaches as more significant threats to their cloud infrastructure.
- High performers are more likely to cite resource cloaking, tooling integration and automation capabilities as important to achieving secure cloud access with much greater frequency than the rest of the respondents.

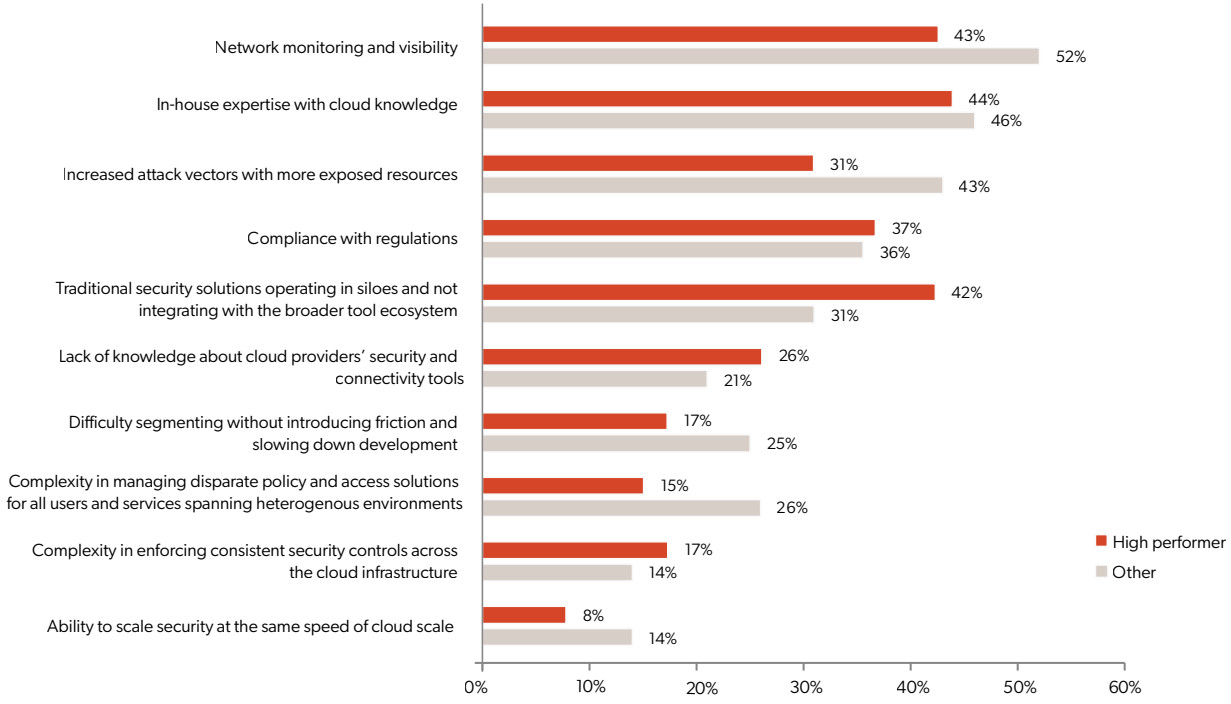
In this section, we provide a special analysis of 582 respondents who rated their organizations' confidence in securing access to the cloud as confident or very confident and compare their perceptions to the 874 respondents who are not as confident.

We refer to the confident respondents as "high performers" and those who are not as confident as "others." We believe the practices of high performing organizations can provide guidance to organizations struggling to achieve a stronger cloud security posture.

High performers have different opinions about the most significant challenges to achieving a secure cloud environment. As shown in Figure 16, high performers are **less likely** to view the following as challenges: an increase in attack vectors with more exposed resources (31 percent vs. 43 percent), complexity in managing disparate policy and access solutions for all users and services spanning heterogenous environments (15 percent vs. 26 percent). High performers are **more likely** to believe traditional security solutions operating in siloes and not being integrated with other tools is a challenge to a stronger cloud security posture.

Figure 16. What are the most significant challenges to having a secure cloud environment?

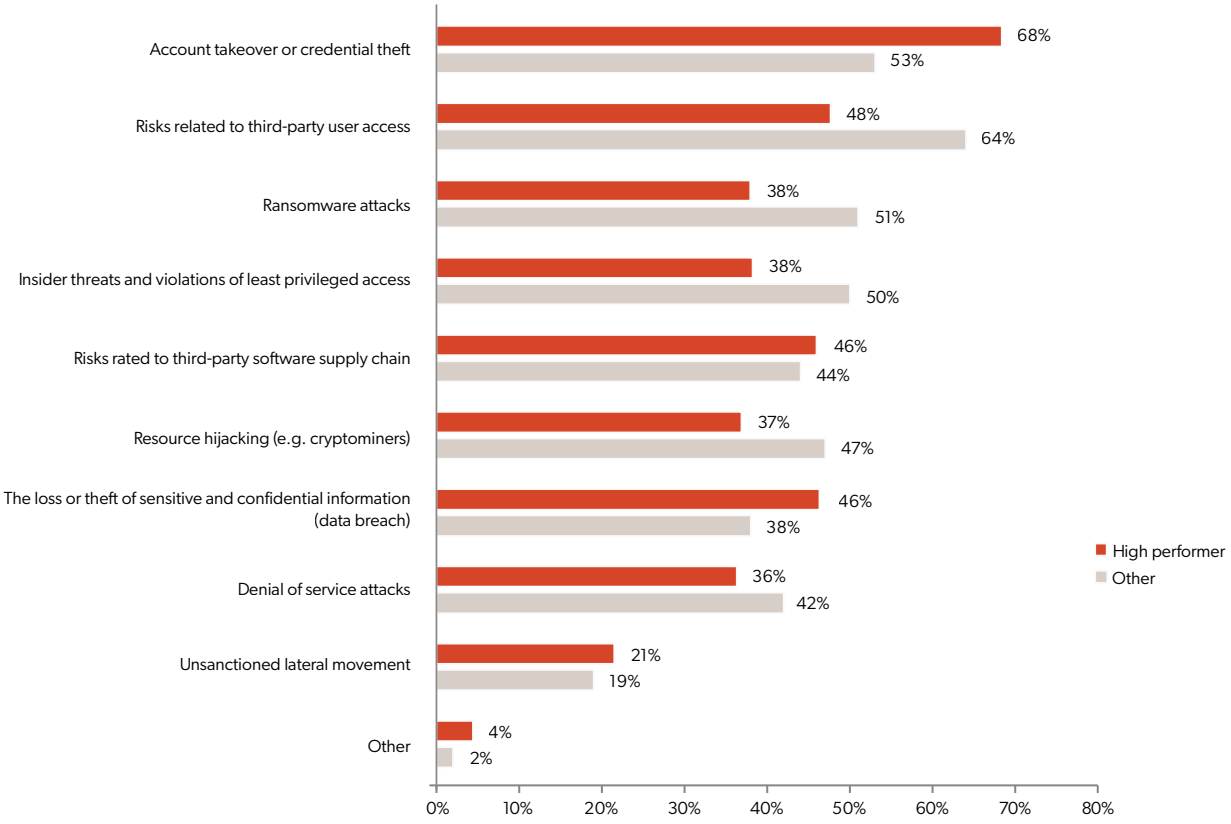
Three responses permitted



High performers see threats differently. In particular, high performers are far more likely to consider account takeovers or credential theft as the top threat to their cloud infrastructures (68 percent vs. 53 percent). The other group of respondents are significantly more concerned about risks related to third-party user access (64 percent vs. 48 percent), ransomware attacks (51 percent vs. 38 percent) and violations of least privileged access (50 percent vs. 38 percent)

Figure 17. What are the top threats to your organization's cloud infrastructure?

Four responses permitted



Confident organizations are more likely to adopt certain security practices. High performer respondents say their organizations are **more likely** to cloak servers, workloads and data so they are not visible or accessible until authenticated (62 percent vs. 43 percent), to integrate security tooling with the IT ecosystem for greater telemetry and automation capabilities (55 percent vs. 42 percent and enforce least privilege for all workload-to workload connections (52 percent vs. 39 percent).

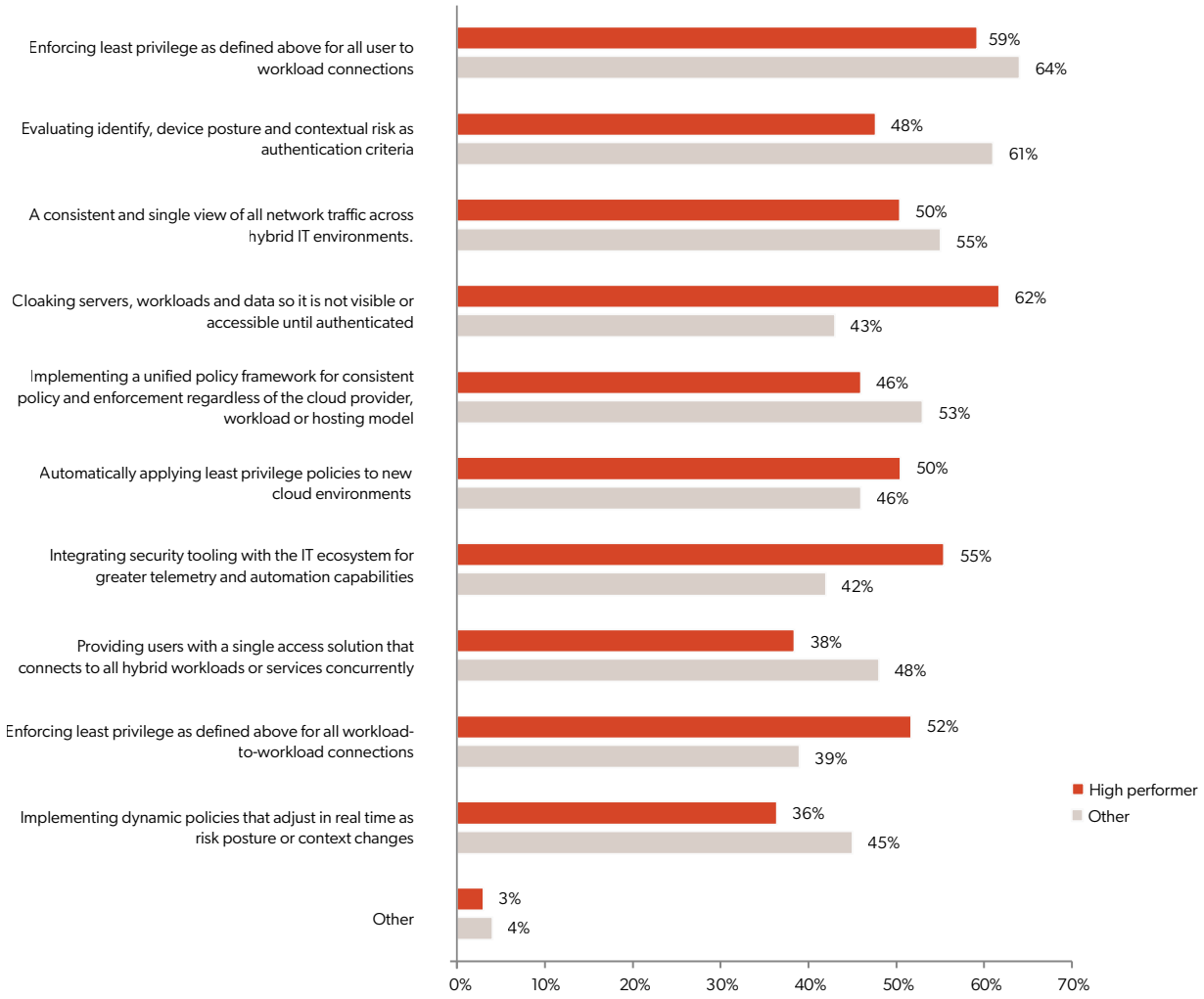
The other respondents are **more likely** to adopt the following practices: identification device posture and contextual risk as authentication criteria (61 percent vs. 48 percent), provide users with a single access solution that connects to all hybrid workloads or services concurrently (48 percent vs. 38 percent) and implement dynamic policies that adjust in real time as risk posture or context changes (45 percent vs. 36 percent).

*High performer respondents say their organizations are **more likely** to cloak servers, workloads and data.*

Permissive workload-to-workload connection policies can help facilitate intrusions and the spread of ransomware.

Figure 18. Which of the following security practices are important to achieving secure cloud access?

Five responses permitted



Conclusion

There are many reasons why organizations pursue cloud transformations, led by increasing efficiency, reducing costs, improving security and shortening deployment timelines.

Architectures leveraging a containerized, microservices-oriented, multi-cloud architecture will be the most common, and within the next two years these cloud environments are expected to handle the majority of total IT and data processing requirements.

However, every enterprise cloud will be unique and on-premises processing will nevertheless remain an important part of enterprise environments for years to come. Traditional perimeter-oriented security tools are poorly equipped for such a diversity of environments and the modern (and continually evolving) threat landscape.

The experiences of organizations that have already adopted and applied Zero Trust principles—particularly from the high-performing organizations—demonstrate Zero Trust's efficacy for securing cloud access.

Based upon this research, we offer five recommendations to help guide business leaders and IT security buyers as they look to achieve their cloud transformation goals:

1. While cloud transformation brings benefits, it also imposes new security requirements. Organizations need to learn the risks associated with cloud environments and CI/CD methodologies, and the processes and security features needed to manage them.
2. Real world experience supports the benefits of Zero Trust. Don't dismiss Zero Trust as being a buzzword simply because of the attention it receives.
3. Recognize that while Zero Trust principles can improve your cloud security posture, respondents say it offers many benefits that extend beyond security, particularly around increasing productivity and efficiency. These benefits should be taken into account when Zero Trust is on the table.
4. Don't treat Zero Trust as an add-on to be explored only as your cloud transformation reaches maturity. Instead, Zero Trust is something that can enable and accelerate the transformation itself.
5. Consider Zero Trust Network Access as a ready-built way to secure cloud access and to directly satisfy both security and operational requirements.

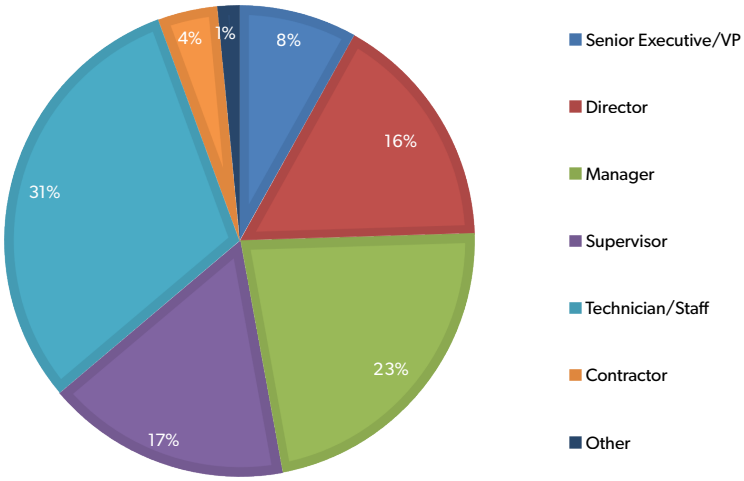
The experiences of organizations that have already adopted and applied Zero Trust principles—particularly from the high-performing organizations—demonstrate Zero Trust's efficacy for securing cloud access.

PART 3.
METHODOLOGY

A sampling frame of 14,365 IT decision makers and security professionals in the U.S., Europe and the Middle East (EMEA) and Latin America were selected as participants to this survey. Table 1 shows 1,626 total returns. Screening and reliability checks required the removal of 170 surveys. Our final sample consisted of 1,456 surveys or a 3.5 percent response.

Figure 19 reports the respondent's organizational level within participating organizations. By design, more than half (64 percent) of respondents are at or above the supervisory levels. The largest category at 31 percent of respondents is technician or staff for security.

Figure 19. Current position within the organization



As shown in Figure 20, 29 percent of respondents report to the chief information officer, 20 percent of respondents report to the chief information security officer, 9 percent of respondents report to the chief technology officer, 8 percent of respondents report to the compliance officer and 8 percent of respondents report to the chief risk officer.

Figure 20. Direct reporting channel

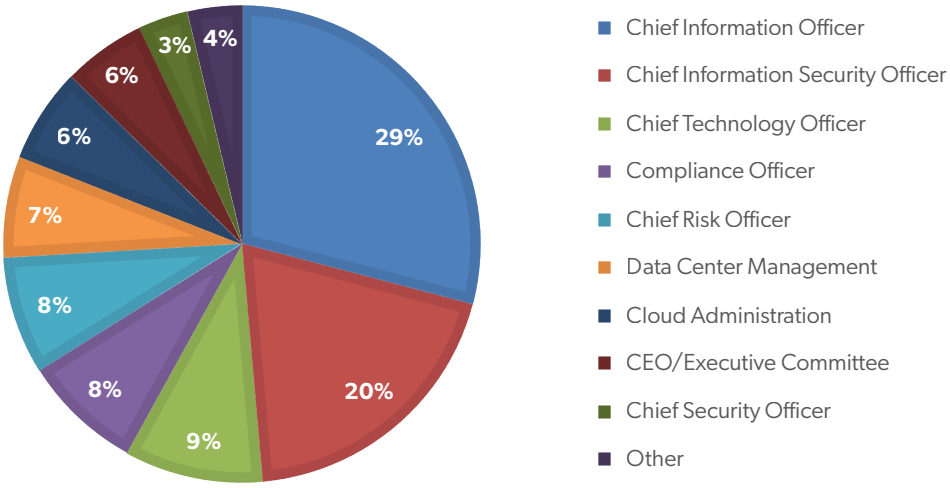
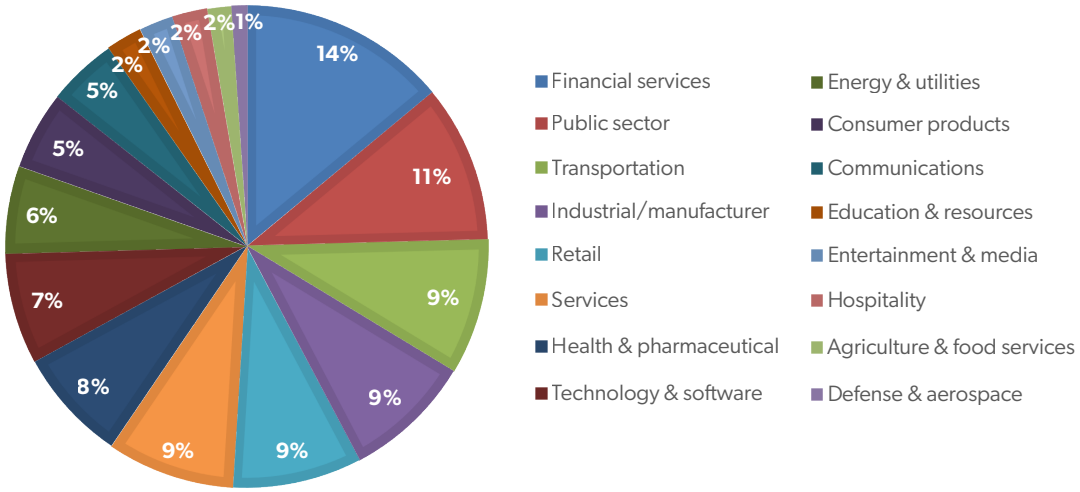
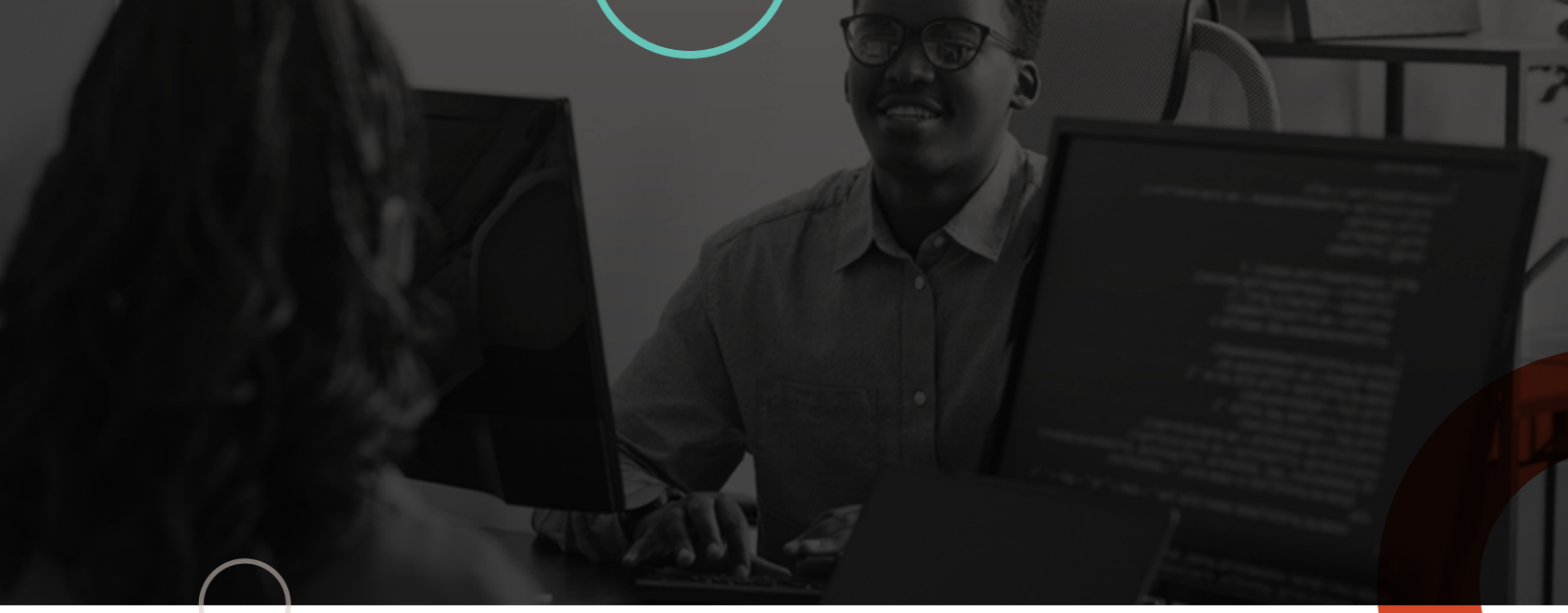


Figure 21 reports the industry focus of respondents' organizations. This chart identifies financial services (14 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by public sector (11 percent of respondents), transportation, industrial/manufacturer, retail and services (each at 9 percent of respondents).

Figure 21. Primary industry focus





PART 4.
CAVEATS TO THIS STUDY

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 decision makers and security professionals. 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.

PART 5. APPENDIX WITH DETAILED AUDITED FINDINGS

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in March 2022.

SURVEY RESPONSE	TOTAL
Total sampling frame	41,365
Total survey returns	1,626
Total rejected responses	170
Final sample	1,456
Response rates	3.5%

Part 1: Screening

S1. WHAT IS THE HEADCOUNT OF YOUR ORGANIZATION?	TOTAL
Less than 500 (stop)	0%
500 to 1,000	35%
1,001 to 10,000	26%
10,001 to 25,000	24%
25,001 to 50,000	6%
50,001 to 75,000	5%
More than 75,000	4%
Total	**100%**
Extrapolated value	*14,104*

S2. WHICH OF THE FOLLOWING BEST DESCRIBES YOUR ROLE IN IT OR IT SECURITY WITHIN YOUR ORGANIZATION? PLEASE SELECT ALL THAT APPLY.	TOTAL
Setting IT security priorities	53%
Managing IT security budgets	49%
Selecting vendors and contractors	42%
Participating in IT security strategies	47%
Evaluating and measuring the effectiveness of security strategies	38%
Managing security risk	49%
Overseeing governance and compliance	32%
None of the above (stop)	0%
Total	**310%**

S3. WHAT PERCENTAGE OF YOUR ORGANIZATION'S IT FUNCTIONS UTILIZE CLOUD TECHNOLOGIES?	TOTAL
Less than 10% (stop)	0%
10% to 25%	37%
26% to 50%	35%
51% to 75%	17%
76% to 100%	10%
Total	**100%**

S4. HOW DO YOU RATE YOUR LEVEL OF INVOLVEMENT IN THE USE OF CLOUD RESOURCES WITHIN YOUR ORGANIZATION?	TOTAL
Very high level of involvement	35%
High level of involvement	40%
Moderate level of involvement	25%
Low level of involvement (stop)	0%
No involvement (stop)	0%
Total	**100%**

S5. HOW FAMILIAR ARE YOU WITH THE PRINCIPLES OF ZERO TRUST SECURITY?	TOTAL
Very familiar	36%
Familiar	36%
Somewhat familiar	28%
Not familiar (stop)	0%
Total	**100%**

Part 2: Cloud Maturity

Q1. WHAT BEST DESCRIBES YOUR CLOUD HOSTING INFRASTRUCTURE? PLEASE SELECT ONLY ONE CHOICE.	TOTAL
All public cloud from a single provider (please skip to Q4)	33%
All public cloud from multiple providers (multi-cloud)	28%
All private cloud (please skip to Q4)	13%
A mixture of public and private (hybrid cloud) (please skip to Q3)	26%
Total	**100%**

Q2. IF YOUR ORGANIZATION DEPLOYS A MULTI-CLOUD ARCHITECTURE OR STRATEGY, HOW MANY DIFFERENT PUBLIC CLOUDS DOES YOUR ORGANIZATION USE?	TOTAL
2	34%
3	29%
4	13%
5	12%
More than 5	13%
Total	**100%**
Extrapolated value	*3.55*

Q3. IF YOUR ORGANIZATION DEPLOYS A MIXTURE OF PUBLIC AND PRIVATE CLOUDS (HYBRID CLOUD) HOW MANY DIFFERENT CLOUDS DOES YOUR ORGANIZATION USE?	TOTAL
2	52%
3	25%
4	12%
5	7%
More than 5	3%
Total	**100%**
Extrapolated value	*2.89*

Q4. IF YOUR ORGANIZATION DOES NOT DEPLOY A MULTI-CLOUD ARCHITECTURE, WILL IT DEPLOY IT IN THE FUTURE?	TOTAL
Yes, within the next six months	24%
Yes, in the next year	16%
Yes, in the next two to three years	14%
No plans to deploy	46%
Total	**100%**

Q5. WHAT ARE THE PRIMARY REASONS CLOUD RESOURCES ARE USED WITHIN YOUR ORGANIZATION? PLEASE SELECT ONLY THREE CHOICES.	TOTAL
Reduce cost	53%
Increase efficiency	62%
Improve security	48%
Faster deployment time	47%
Increase flexibility and choice	36%
Improve customer service	27%
Comply with contractual agreements or policies	25%
Other (please specify)	3%
Total	**300%**

Q6A. HAS YOUR ORGANIZATION ADOPTED DEVOPS AS DEFINED ABOVE?	TOTAL
Yes	50%
No, but plan to adopt in the next six months (please skip to Q7)	14%
No, but plan to adopt in the next year (please skip to Q7)	15%
No, but plan to adopt in the next two to three years (please skip to Q7)	12%
No plan to deploy	10%
Total	**100%**

Q6B. IF YES, HOW DOES IT SECURITY COLLABORATE WITH DEVOPS? PLEASE SELECT ALL THAT APPLY.	TOTAL
Educates DevOps on the organization's security risks	51%
Shares IT security best practices	46%
Recommends the use of certain security tools	41%
Implements security automation in DevOps	38%
Audits security practices in DevOps pipelines	40%
IT security does not engage with DevOps	30%
Total	**250%**

Q7. WHAT PERCENTAGE OF YOUR ORGANIZATION'S APPLICATIONS ARE IN PUBLIC CLOUD ENVIRONMENTS?	TOTAL
0% (none)	13%
1 to 20%	16%
21 to 40%	21%
41 to 60%	10%
61 to 75%	10%
More than 75%	29%
Total	**100%**
Extrapolated value	*46%*

Q8A. HAS YOUR ORGANIZATION ADOPTED THE USE OF CONTAINERS?	TOTAL
Yes	55%
No, but plan to adopt in the next six months (please skip to Q9)	9%
No, but plan to adopt in the next year (please skip to Q9)	8%
No, but plan to adopt in the next two to three years (please skip to Q9)	15%
No plan to adopt	13%
Total	**100%**

Q8B. IF YES, DOES YOUR ORGANIZATION USE CONTAINERS FOR MICROSERVICES ARCHITECTURES?	TOTAL
Yes	55%
No, but plan to adopt in the next six months (Q9)	13%
No, but plan to adopt in the next year (Q9)	13%
No, but plan to adopt in the next two to three years (Q9)	13%
No plan to adopt	7%
Total	**100%**

Q8C. IF YES, WHAT PERCENTAGE OF YOUR ORGANIZATION'S APPLICATIONS ARE BUILT USING CONTAINERS?	TOTAL
0%	0%
1% to 20%	16%
21% to 40%	16%
41% to 60%	19%
60% to 75%	24%
More than 75%	25%
Total	**100%**
Extrapolated value	*55%*

Q9. WHAT PERCENTAGE OF YOUR ORGANIZATION'S APPLICATIONS USE SAAS?	TOTAL
0% (please skip to Q11)	7%
1% to 20%	17%
21% to 40%	23%
41% to 60%	23%
60% to 75%	18%
More than 75%	12%
Total	**100%**
Extrapolated value	*43%*

Q10. APPROXIMATELY HOW MANY SAAS APPLICATIONS DOES YOUR ORGANIZATION USE?	TOTAL
Less than 5	15%
5 to 10	23%
11 to 25	31%
More than 25	32%
Total	**100%**
Extrapolated value	*17.05*

Q11. WHAT PERCENTAGE OF YOUR ORGANIZATION'S RESOURCES UTILIZE PAAS VERSUS ON-PREMISES INFRASTRUCTURE SERVICES?	TOTAL
0% (please skip to Q13)	8%
1% to 20%	21%
21% to 40%	26%
41% to 60%	23%
60% to 75%	11%
More than 75%	11%
Total	**100%**
Extrapolated value	*39%*

Q12. IF YES, APPROXIMATELY HOW MANY PAAS SERVICES DOES YOUR ORGANIZATION USE?	TOTAL
Less than 5	18%
5 to 10	27%
11 to 25	21%
26 to 50	22%
More than 50	12%
Total	**100%**
Extrapolated value	*21.93*

Q13. APPROXIMATELY WHAT PERCENTAGE OF YOUR ORGANIZATION'S TOTAL IT AND DATA PROCESSING REQUIREMENTS ARE MET BY USING CLOUD RESOURCES TODAY (E.G. PUBLIC CLOUD, PRIVATE CLOUD, SAAS, PAAS, CONTAINERS OR SERVERLESS)?	TOTAL
Less than 5%	1%
Between 5% to 10%	6%
Between 11% to 20%	11%
Between 21% to 30%	12%
Between 31% to 40%	15%
Between 41% to 50%	18%
Between 51% to 60%	15%
Between 61% to 75%	11%
More than 75%	12%
Total	**101%**
Extrapolated value	*45.5%*

Q14. APPROXIMATELY WHAT PERCENTAGE OF YOUR ORGANIZATION'S TOTAL IT AND DATA PROCESSING REQUIREMENTS ARE MET BY USING CLOUD RESOURCES TWO YEARS FROM TODAY (E.G. PUBLIC CLOUD, PRIVATE CLOUD, SAAS, PAAS, CONTAINERS OR SERVERLESS)?	TOTAL
Less than 5%	1%
Between 5% to 10%	2%
Between 11% to 20%	6%
Between 21% to 30%	12%
Between 31% to 40%	12%
Between 41% to 50%	19%
Between 51% to 60%	13%
Between 61% to 75%	13%
More than 75%	23%
Total	**100%**
Extrapolated value	*53.0%*

Q15. HAS YOUR ORGANIZATION ADOPTED SERVERLESS ARCHITECTURES?	TOTAL
Yes	36%
No, but plan to adopt in the next six months	16%
No, but plan to adopt in the next year	14%
No, but plan to adopt in the next two to three years	17%
No plan to adopt	18%
Total	**100%**

Part 3. Security Challenges

Q16. WHAT ARE THE MOST SIGNIFICANT CHALLENGES TO HAVING A SECURE CLOUD ENVIRONMENT? PLEASE SELECT THE TOP THREE.	TOTAL
Increased attack vectors with more exposed resources	38%
Complexity in managing disparate policy and access solutions for all users and services spanning heterogenous environments	22%
Ability to scale security at the same speed of cloud scale	12%
Traditional security solutions operating in siloes and not integrating with the broader tool ecosystem	36%
Difficulty segmenting without introducing friction and slowing down development	22%
Lack of knowledge about cloud providers' security and connectivity tools	23%
Network monitoring and visibility	48%
Complexity in enforcing consistent security controls across the cloud infrastructure	15%
Compliance with regulations	36%
In-house expertise with cloud knowledge	45%
Other (please specify)	3%
Total	**300%**

Q17. WHAT ARE THE TOP THREATS TO YOUR ORGANIZATION'S CLOUD INFRASTRUCTURE? PLEASE SELECT THE TOP FOUR.	TOTAL
Account takeover or credential theft	59%
Unsanctioned lateral movement	20%
Risks related to third-party user access	58%
Risks rated to third-party software supply chain	45%
Resource hijacking (e.g. cryptominers)	43%
Insider threats and violations of least privileged access	45%
Denial of service attacks	40%
Ransomware attacks	46%
The loss or theft of sensitive and confidential information (data breach)	41%
Other (please specify)	3%
Total	**400%**

Q18. WHAT ARE THE MOST SIGNIFICANT BARRIERS TO ACHIEVING A SECURE DIGITAL TRANSFORMATION PROCESS AND CLOUD ADOPTION IN YOUR ORGANIZATION TODAY? PLEASE CHOOSE ONLY YOUR FOUR CHOICES.	TOTAL
Insufficient resources or budget	49%
Insufficient visibility of people and business processes	57%
Current vendor lacks support for cloud platforms	46%
Insufficient assessment of cybersecurity risks	58%
Lack of skilled or expert personnel	56%
Lack of leadership	22%
Lack of oversight or governance	23%
Complexity of compliance and regulatory requirements	20%
Other (please specify)	3%
Total	**334%**

Q19. HOW CONFIDENT ARE YOU THAT YOUR ORGANIZATION HAS THE ABILITY TO SEGMENT AND APPLY THE PRINCIPLE OF LEAST PRIVILEGE FROM 1 = NOT CONFIDENT TO 10 = VERY CONFIDENT?	TOTAL
1 or 2	10%
3 or 4	20%
5 or 6	27%
7 or 8	26%
9 or 10	16%
Total	**100%**
Extrapolated value	*5.87*

Q20. HOW CONFIDENT ARE YOU THAT YOUR ORGANIZATION ENSURES SECURE ACCESS TO ITS CLOUD ENVIRONMENTS FROM 1 = NOT CONFIDENT TO 10 = VERY CONFIDENT?	TOTAL
1 or 2	8%
3 or 4	20%
5 or 6	33%
7 or 8	23%
9 or 10	17%
Total	**100%**
Extrapolated value	*5.92*

Q21. HOW CONFIDENT ARE YOU THAT YOUR IT ORGANIZATION KNOWS ALL CLOUD COMPUTING APPLICATIONS, PLATFORMS OR INFRASTRUCTURE SERVICES IN USE TODAY FROM 1 = NOT CONFIDENT TO 10 = VERY CONFIDENT?	TOTAL
1 or 2	16%
3 or 4	26%
5 or 6	25%
7 or 8	17%
9 or 10	16%
Total	**100%**
Extrapolated value	*5.33*

Q22. HOW EFFECTIVE DO YOU BELIEVE YOUR ORGANIZATION IS IN QUICKLY PROVISIONING SECURE ACCESS TO CLOUD ENVIRONMENTS WITHOUT INTRODUCING RISK OR SLOWING PRODUCTIVITY ON A SCALE FROM 1 = NOT EFFECTIVE TO 10 = HIGHLY EFFECTIVE?	TOTAL
1 or 2	10%
3 or 4	19%
5 or 6	28%
7 or 8	26%
9 or 10	17%
Total	**100%**
Extrapolated value	*5.93*

Q23. HOW DIFFICULT DO YOU BELIEVE IT IS FOR YOUR ORGANIZATION TO SEGMENT THE NETWORK AND RESOURCES TO FURTHER RESTRICT LATERAL MOVEMENT AND CONTAIN RANSOMWARE ON A SCALE FROM 1 = NOT DIFFICULT TO 10 = VERY DIFFICULT?	TOTAL
1 or 2	11%
3 or 4	20%
5 or 6	23%
7 or 8	28%
9 or 10	18%
Total	**100%**
Extrapolated value	*5.91*

PLEASE USE THE AGREEMENT SCALE TO RATE EACH STATEMENT LISTED BELOW: STRONGLY AGREE AND AGREE RESPONSES COMBINED.	TOTAL
Q24. Cloud adoption has brought new security and compliance risks to my organization.	55%
Q25. Current network security controls affect the productivity of DevOps or introduce vulnerabilities because those controls cannot scale fast enough.	52%
Q26. Perimeter-based solutions like firewalls, VPNs and NACs are ill-equipped to secure modern, complex and interconnected enterprise cloud architectures.	58%
Q27. Perimeter-based security solutions are no longer adequate to mitigate the risk from ransomware, DDoS attacks, insider threats and man-in-the-middle incidents.	62%
Q28. Remote working and the emerging hybrid workforce has further complicated cloud security and introduced new risk to the enterprise.	57%

Part 4. Solutions

Q29. WHICH OF THE FOLLOWING SECURITY PRACTICES ARE IMPORTANT TO ACHIEVING SECURE CLOUD ACCESS? PLEASE SELECT THE TOP FOUR CHOICES.	TOTAL
Cloaking servers, workloads and data so it is not visible or accessible until authenticated	51%
Identifying device posture and contextual risk as authentication criteria	56%
Enforcing least privilege as defined above for all user to workload connections	62%
Enforcing least privilege as defined above for all workload-to-workload connections	44%
Implementing dynamic policies that adjust in real time as risk posture or context changes	42%
Implementing a unified policy framework for consistent policy and enforcement regardless of the cloud provider, workload or hosting model	50%
Providing users with a single access solution that connects to all hybrid workloads or services concurrently	44%
Automatically applying least privilege policies to new cloud environments	48%
Integrating security tooling with the IT ecosystem for greater telemetry and automation capabilities	47%
A consistent and single view of all network traffic across hybrid IT environments.	53%
Other (please specify)	3%
Total	**500%**

Q30. HAS YOUR ORGANIZATION ADOPTED A ZERO TRUST STRATEGY AS DESCRIBED ABOVE?	TOTAL
Yes	49%
No (please skip to Q34)	51%
Total	**100%**

Q31. IF YES, WHAT BEST DESCRIBES THE MATURITY OF YOUR ORGANIZATION'S ZERO TRUST STRATEGY?	TOTAL
Planning stage – We plan to adopt and define what the Zero Trust strategy is and how to implement it.	21%
Early adoption stage – Zero Trust activities are planned, defined and partially deployed.	30%
Full adoption stage – most zero-trust activities are deployed across the enterprise. The program has C-level support and adequate budget.	26%
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.	23%
Total	**100%**

Q32. WHAT ARE THE MOST SIGNIFICANT BENEFITS OF ZERO TRUST? PLEASE SELECT THE TOP SIX BENEFITS.	TOTAL
Attack surface reduction (i.e. cloaked servers, workloads and/or data)	50%
Stronger authentication using identity and risk posture	61%
Unsanctioned lateral movement prevention using micro segmentation	52%
Reduced complexity in securing access to heterogenous environments	44%
Improved user experience	53%
Increased productivity of the IT security team	65%
Increased productivity of the DevOps team	58%
Reduction in help desk tickets	45%
Reduction in policy management issues	42%
Focus security and IT teams on transformation efforts	36%
Greater network visibility and automation capabilities	58%
Ability to integrate Zero Trust into DevOps	37%
Total	**600%**

Q33. HAS YOUR ORGANIZATION PURCHASED OR PLAN TO PURCHASE ZERO TRUST NETWORK ACCESS (ZTNA)?	TOTAL
Yes	46%
No	54%
Total	**100%**

Q34. IF NO PLANS TO ADOPT, WHAT ARE THE REASONS FOR NOT ADOPTING? PLEASE SELECT THE TOP TWO REASONS.	TOTAL
Zero Trust is just about marketing	53%
No support from senior leadership	59%
A Zero Trust strategy is too costly and difficult to implement	50%
Zero Trust will not improve our security posture	37%
Other (please specify)	2%
Total	**200%**

Part 5. Budget and Investment

Q35. WHAT SECURITY TOOLS HAS YOUR ORGANIZATION PURCHASED TO SECURE CLOUD ACCESS? PLEASE SELECT ALL THAT APPLY.	TOTAL
VPNs	52%
Cloud Native Firewall	60%
Service Mesh	46%
Next Generation Firewall (NGFW)	44%
Web Application Firewall (WAF)	58%
Cloud Access Security Broker (CASB)	60%
Cloud workload protection platform	41%
Cloud workload segmentation	43%
Multi-factor authentication	46%
Other (please specify)	3%
Total	**454%**

Q36. WHAT SECURITY TOOLS DOES YOUR ORGANIZATION PLAN TO PURCHASE TO SECURE CLOUD ACCESS? PLEASE SELECT ALL THAT APPLY.	TOTAL
VPNs	60%
Cloud Native Firewall	62%
Service Mesh	52%
Next Generation Firewall (NGFW)	45%
Web Application Firewall (WAF)	61%
Cloud Access Security Broker (CASB)	64%
Cloud workload protection platform	45%
Cloud workload segmentation	51%
Multi-factor authentication	60%
Other (please specify)	2%
Total	**503%**

Q37. WHAT RANGE BEST DESCRIBES YOUR ORGANIZATION'S ANNUAL IT BUDGET IN THE CURRENT FISCAL YEAR?	TOTAL
Less than $1 million	0%
$1 to $10 million	3%
$11 to $25 million	10%
$26 to $50 million	13%
$51 to $100 million	14%
$101 to $250 million	24%
$251 to $500 million	29%
More than $500 million	7%
Total	**100%**
Extrapolated value	*$ 153,774*

Q38. WHAT PERCENTAGE OF YOUR COMPANY'S ANNUAL IT BUDGET IS DEDICATED TO SECURING CLOUD-BASED RESOURCES?	TOTAL
None	0%
Less than 5%	3%
5% to 10%	6%
11% to 15%	18%
16% to 20%	23%
21% to 30%	27%
31% to 50%	17%
More than 50%	6%
Total	**100%**
Extrapolated value	*24%*

Part 6. Your Role and Organization

D1. WHAT ORGANIZATIONAL LEVEL BEST DESCRIBES YOUR CURRENT POSITION?	TOTAL
Senior Executive/VP	8%
Director	16%
Manager	23%
Supervisor	17%
Technician/Staff	31%
Contractor	4%
Other (please specify)	1%
Total	**100%**

D2. CHECK THE PRIMARY PERSON YOU OR YOUR IT SECURITY LEADER REPORTS TO WITHIN THE ORGANIZATION.	TOTAL
CEO/Executive Committee	6%
Chief Information Officer	29%
Chief Information Security Officer	20%
Chief Risk Officer	8%
Chief Security Officer	3%
Chief Technology Officer	9%
Compliance Officer	8%
Data Center Management	7%
Cloud Administration	6%
Other (please specify)	4%
Total	**100%**

D3. WHAT BEST DESCRIBES YOUR ORGANIZATION'S PRIMARY INDUSTRY CLASSIFICATION?	TOTAL
Agriculture & food services	2%
Communications	5%
Consumer products	5%
Defense & aerospace	1%
Education & resources	2%
Energy & utilities	6%
Entertainment & media	2%
Financial services	14%
Health & pharmaceutical	8%
Hospitality	2%
Industrial/manufacturer	9%
Public sector	11%
Retail	9%
Services	9%
Technology & software	7%
Transportation	9%
Total	**100%**

GLOBAL STUDY ON ZERO TRUST SECURITY **FOR THE CLOUD**

Ponemon INSTITUTE

Please contact research@ponemon.org or call us at 800.887.3118 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 high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict 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.

appgate

Appgate is the secure access company. We empower how people work and connect by providing solutions purpose-built on Zero Trust security principles. This people-defined security approach enables fast, simple and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises and hybrid environments. Appgate helps organizations and government agencies worldwide start where they are, accelerate their Zero Trust journey and plan for their future. Learn more at appgate.com.

©2022 Appgate. All Rights Reserved. The Appgate logo and certain product names are the property of Appgate.
All other marks are the property of their respective owners.