April 2024

Organizations tackling multi-cloud security amidst misconfigurations and poor visibility

CRA | Business Intelligence
A CRA Resource

Contents

ALSO IN THIS REPORT

"It is better to have your head in the clouds, and know where you are... than to breathe the clearer atmosphere below them, and think that you are in paradise."

– HENRY DAVID THOREAU

Foreword

If the cloud is essential to competing in the digital economy, then why is its security so often an afterthought?

It's a frustration many of our survey respondents voiced in this report.

Whether it was Legion's **abuse** of AWS and PayPal, TeamTNT's **credential theft** of major cloud platforms, or the most recent and devastating attack on **Change Healthcare** that saw its cloud-based lab interface tools go offline, respondents were more than validated by what we saw in the last year and a half. The takeaway? Cloud security is never, ever a given.

This year, new stressors entered the fray. Many organizations expanded cloud partnerships and platforms to satisfy business requirements, inadvertently creating more blind spots and misconfiguration errors for IT security teams to track. Limited visibility into cloud-based inventory and lack of familiarity with multiple platforms have raised the stakes as well. Security personnel are desperate for solutions that can identify vulnerabilities before adversaries can, but they lack the budget, skill sets, or manpower to get it done.

"We're not mature enough that we're able to easily see what's not set up properly," says one respondent. "I worry it's all being done so quickly, that it's possible it's being done incorrectly."

This is not the first year our team has conducted this survey, but it is the first time we've asked how new technologies (like AI, SASE, ZTNA, and IaC) could augment cloud security capabilities. We found many enthusiastic and optimistic for what these products could deliver, but there were also concerns about potential misuse, their costs, and whether they can be integrated with existing tools.

We hope that this report provides you with a candid look at how security decision-makers are planning their next steps in the cloud journey. Though hazards abound and trials may lie ahead, we believe awareness of these factors can help organizations prioritize cloud security with the care and rigor it deserves.

Cloud Security 101

Cloud computing enables organizations to reach more customers, speed up service delivery, and introduce more efficient business processes through automation and orchestration. However, it can also expose organizations to greater risk if not managed appropriately.

- **Shared responsibility.** Cloud services entail a shared service agreement between the provider and the customer. Depending on the type of service offered (e.g., IaaS, PaaS, SaaS), the provider will carry primary responsibility for securing cloud infrastructure and native services, while the customer will be primarily responsible for ensuring protection of data, applications, and configurations in the cloud.

- **Defense-in-depth.** Organizations are encouraged to secure the cloud through a multi-layered defense strategy. By diversifying their cloud security portfolio, they're much more likely to weather incidents where one or more defenses go offline. Comprehensive cloud security should be able to enforce protection across multiple levels of the organization — within policies and processes, to physical security and perimeter defenses, to internal network, application and data layers.

- **Visibility = command and confidence**. There are plenty of ways cloud security can drop the ball. Basic misconfigurations, insecure APIs, unauthorized access, lax permissions, and cyber attacks are some of the most common offenders. And in most of these cases, poor visibility is to blame. In recent years, there's been a push for businesses to adopt cloud security tools (such as a CNAPP, CWPP or CSPM) that consolidate cloud functionality in a single pane of glass, giving security and operations shared visibility into how cloud assets are performing and what's entering/exiting the network.

"The road to security is paved with good configurations."

– CLIFFORD STOLL, ASTRONOMER, AUTHOR, AND TEACHER

Four key findings from the survey:

1.

Cloud-first shift is driving security requirements.

The cloud-first shift has been a business boon, but more deployments and platform dependencies put pressure on IT to eliminate security blind spots.

2.

Next-gen cloud security solutions are still nascent.

Cloud security initiatives prioritize IAM, encryption and employee awareness, while next-gen security solutions and practices (like SASE, ZTNA, and IaC) have yet to find widespread adoption.

3.

Misconfigurations and limited visibility are top cloud security challenges.

The threat of misconfigurations and limited visibility into cloud assets keep IT security up at night.

4.

AI optimism is widespread, but not without concerns.

There is widespread optimism that AI could dramatically enhance cloud security functions, but there are also concerns over data privacy, longevity of vendor tools, and abuse of LLMs for adversarial purposes.

1

THE STATE OF CLOUD SECURITY

Organizations under pressure to secure multiple cloud platforms

This year, we see many companies continue their march into the cloud, increasing their cloud providers and expanding deployments to satisfy consumer demands. In the past 12 months, 93% of respondents saw some portion of their workloads migrate to the cloud. Four in ten respondents say at least a quarter of their workloads crossed the cloud threshold.

While it's most common for organizations to use one or two cloud providers, a growing contingent (43%) now partner with anywhere between three to six providers — a seven-point percentage bump since we asked the same question last year.

While expanding cloud services can help organizations meet high demands, they create more pressure for IT teams to ensure such deployments are secure and not susceptible to misuse.

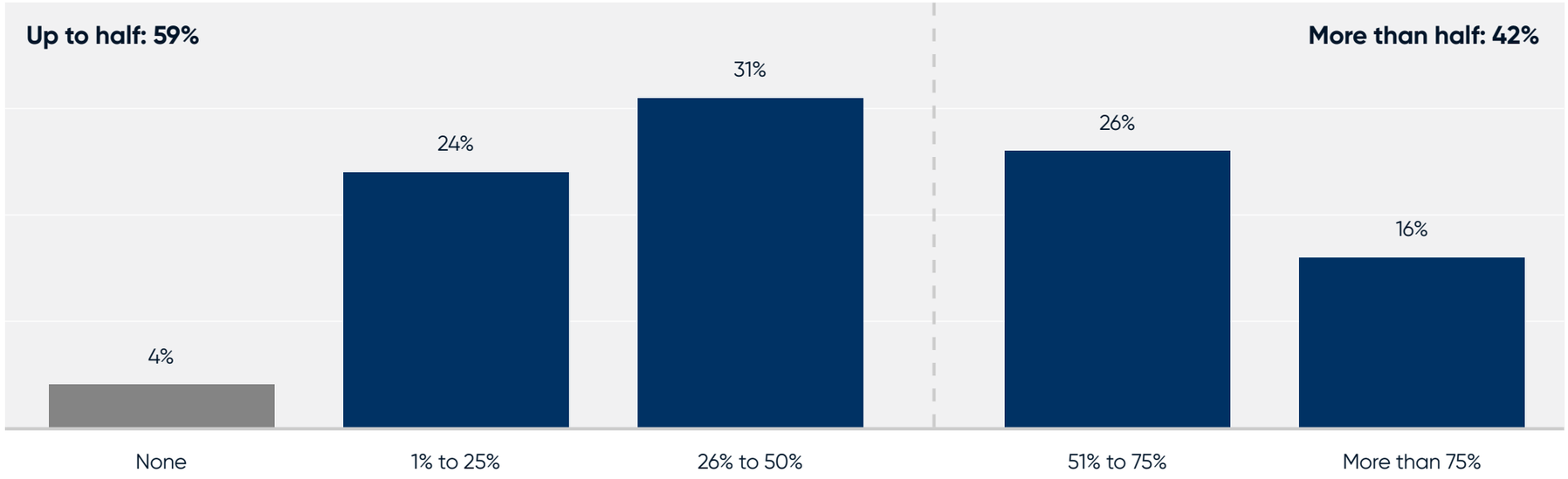
"We weren't able to address our constituents' needs with just one [cloud] platform," according to one respondent. "But now I have three different solutions to deploy technology in those areas, and that just makes it three times as hard."

93%

migrated some share of their workloads to the cloud in the past 12 months

About 4 in 10 respondents say their organization has more than half of its workloads in the cloud.

Q: What percentage of your workloads are in the cloud?



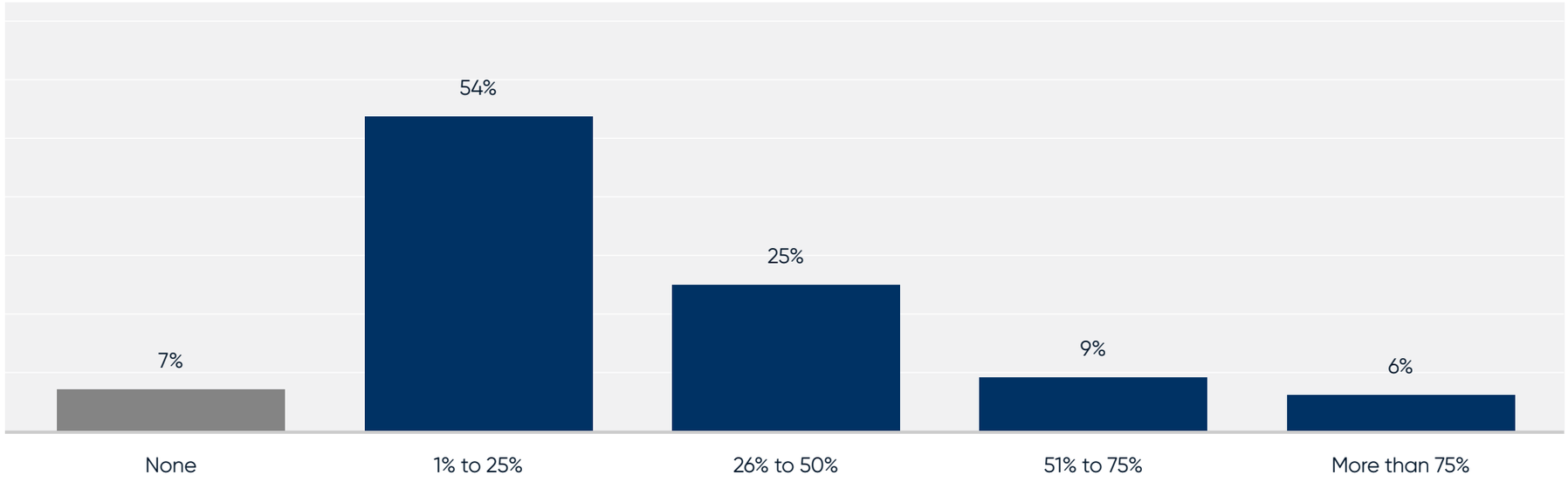
Base: All respondents (n=202).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Cloud Security Survey, January 2024.

"The cloud gives us scalability. If we need a new server, we can spin that up in minutes rather than waiting on equipment purchase for on-prem. It lets us focus more on application support — solving clinician issues and solving patient issues – rather than focusing on worrying about infrastructure."

– SURVEY RESPONDENT

Virtually all respondents (93%) report their organization moved some share of its workloads to the cloud in the past 12 months.

Q: In the last 12 months, what percent of your organization's workloads were moved to the cloud?



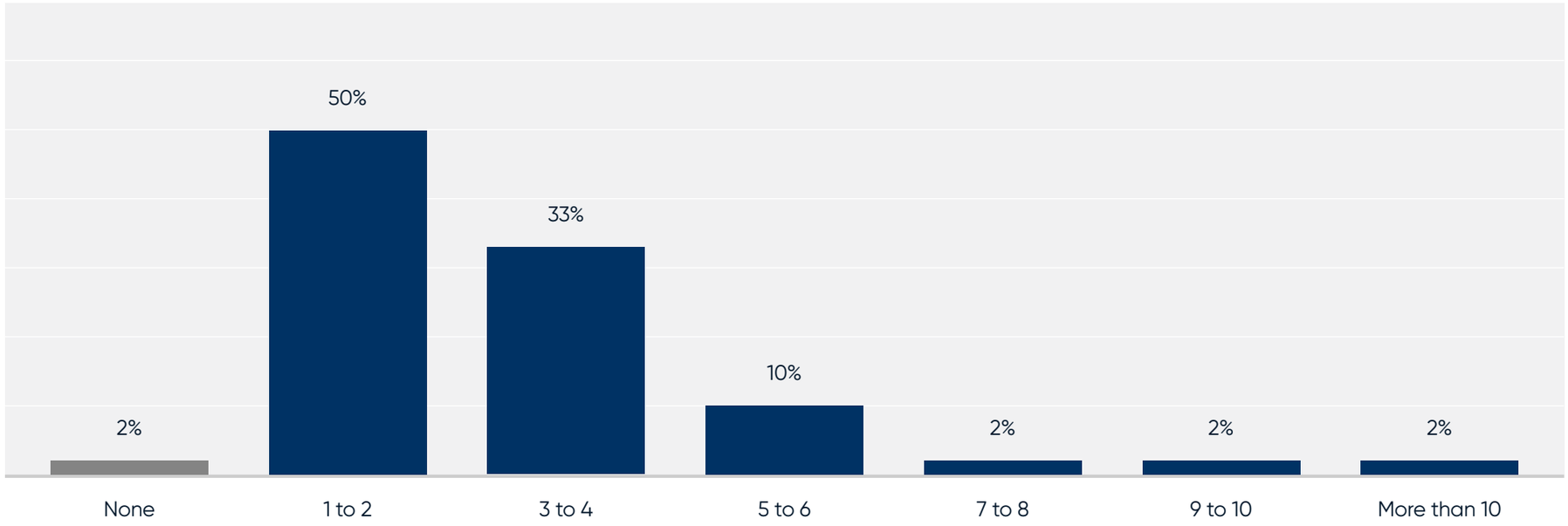
Base: Respondents whose organizations have workloads in the cloud (n=194).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Cloud Security Survey, January 2024.

"We're cloud-first, not cloud-only. It's faster to deploy, easier to deploy, and certainly has the potential to be cheaper to deploy."

– SURVEY RESPONDENT

The largest segment of respondents (50%) report their organization uses one or two public or private cloud providers.

Q: How many public and private cloud providers does your organization currently use?



Base: Respondents whose organizations have workloads in the cloud (n=194).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Cloud Security Survey, January 2024.

"We've got a lot of different constituents with different needs — mostly on the faculty and research side. They have specific needs we weren't able to address with just one platform. So that's really why we're expanding."

– SURVEY RESPONDENT

2

CLOUD SECURITY STRATEGY AND TACTICS

Cloud deployments are managed in a variety of ways

Moving to the cloud is one thing, but managing it well and securing it from potential adversaries is no less daunting. Fifty-three percent of respondents consider their organization to have competent, advanced or expert proficiency at managing cloud security. Another 46% see themselves as less than competent in this regard.

Organizations manage cloud deployments in a variety of ways. Sixty-four percent adopt a hybrid arrangement where their cloud provider assists them with upkeep, 27% manage the cloud independently, and another 8% fully outsource to a provider.

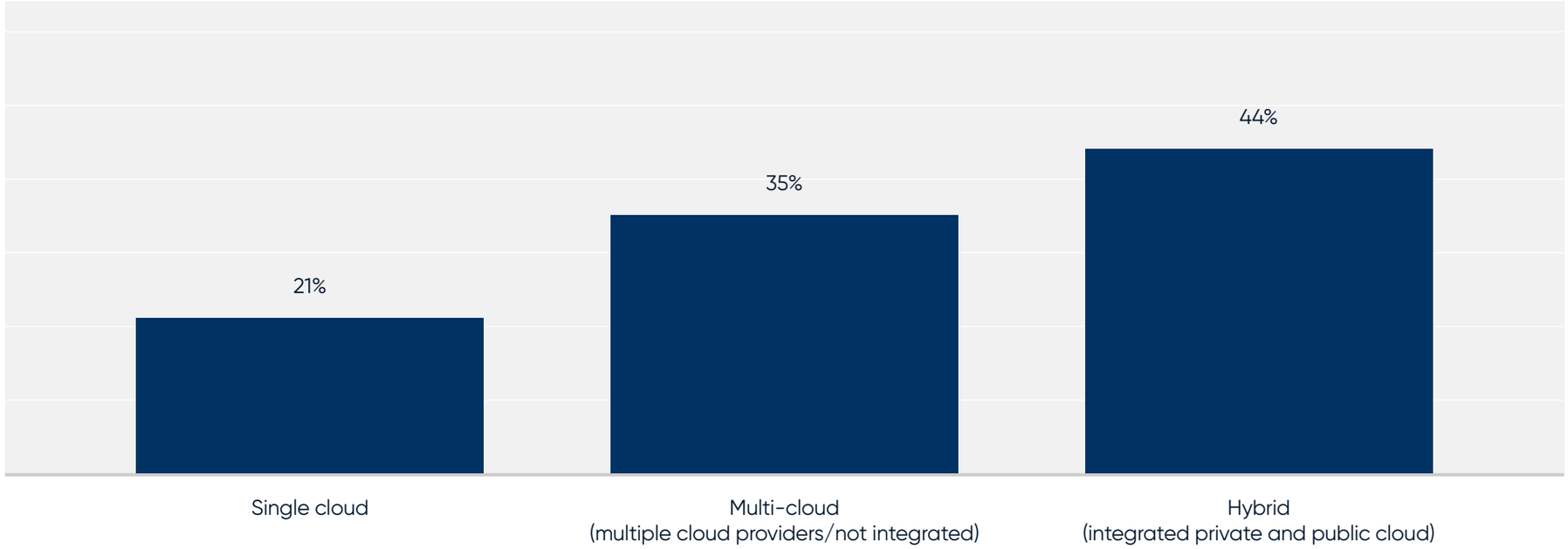
Identity and access management, encryption, and employee awareness initiatives are the most common practices used to secure the cloud. Meanwhile, some of the least popular practices and solutions include SASE, Infrastructure as Code, Zero Trust Network Access, and Software Composition Analysis.

46%

describe their organization's cloud security proficiency as non-existent, beginner, or developing

About 8 in 10 respondents indicate their organization has either a multi-cloud or a hybrid cloud strategy.

Q: What is your organization's primary cloud deployment strategy?



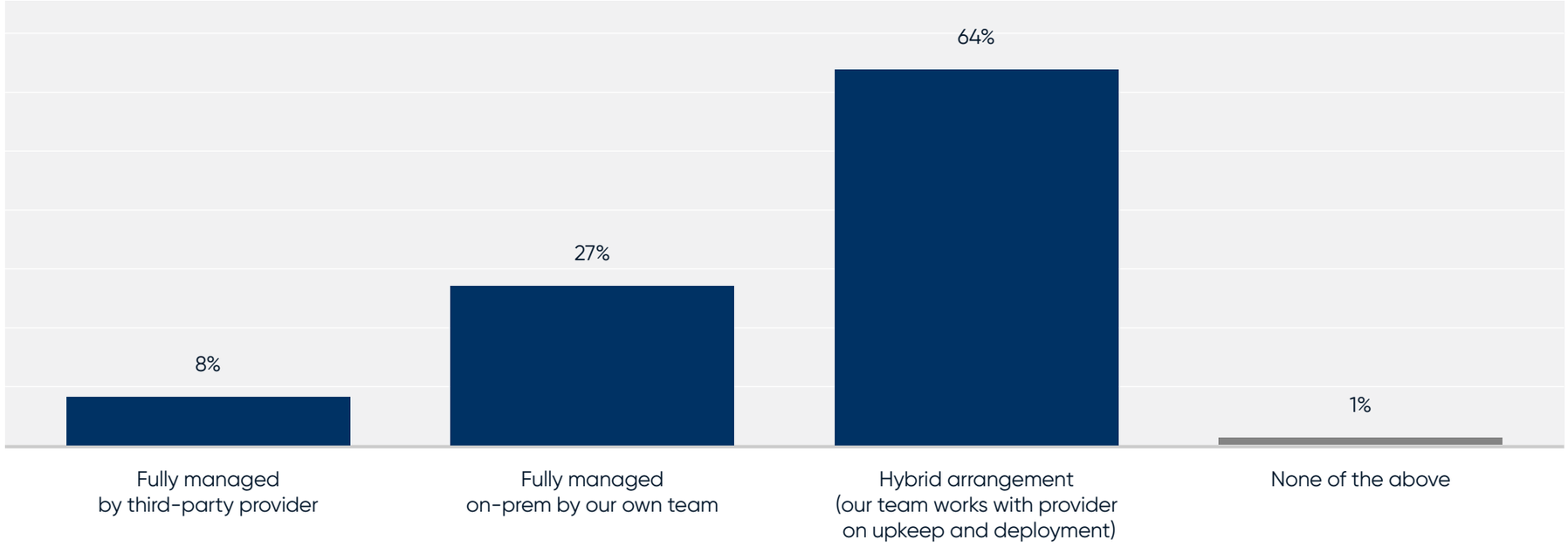
Base: Respondents whose organizations have workloads in the cloud (n=194).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Cloud Security Survey, January 2024.

"I'd say we are 90% to 100% in the cloud. So, we used to have some on-prem workloads, but we've migrated all of these to the cloud and the rest of the things we have are SaaS."

– SURVEY RESPONDENT

About 2 in 3 respondents indicate their organization has a hybrid arrangement to manage its cloud security.

Q: Which of the following best describes how your organization manages cloud security?



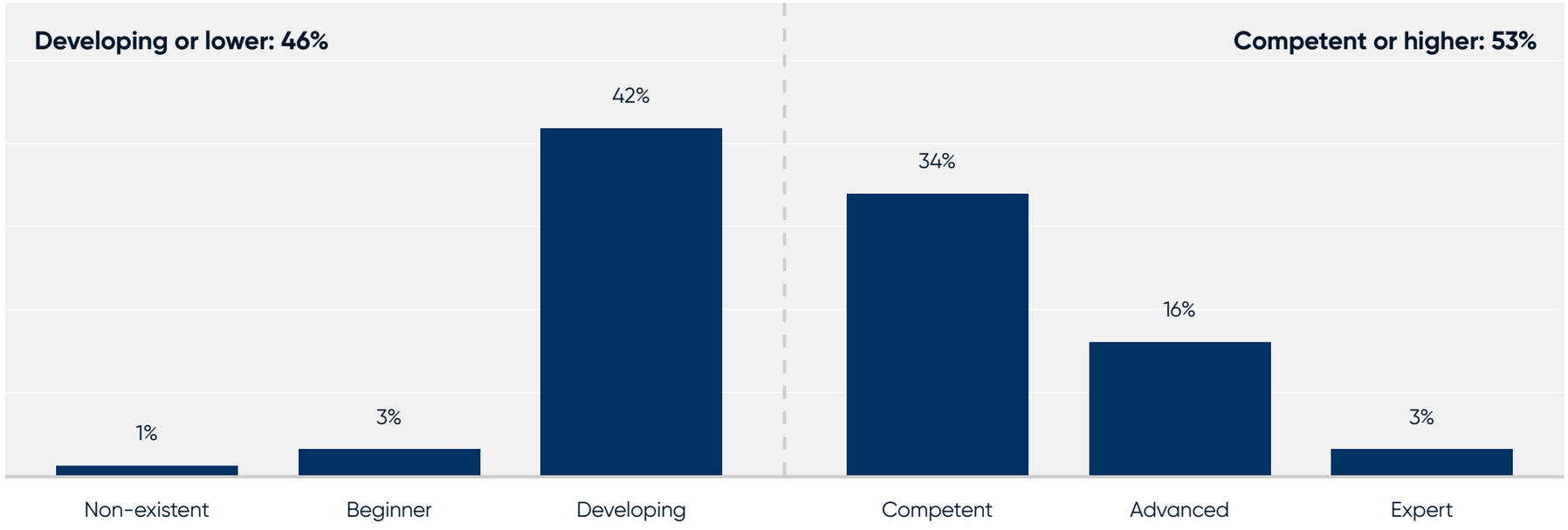
Base: Respondents whose organizations have workloads in the cloud (n=194).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Cloud Security Survey, January 2024.

"Everything about our infrastructure could change because it's Microsoft, Amazon, and Google that are changing and creating these designs. We're sort of going along for the ride, just trying to stay on top of what they require at the speed in which it's being deployed."

– SURVEY RESPONDENT

The largest segment of respondents (42%) describe their organization's cloud security proficiency as "developing."

Q: How would you describe your organization's overall proficiency in managing cloud security?



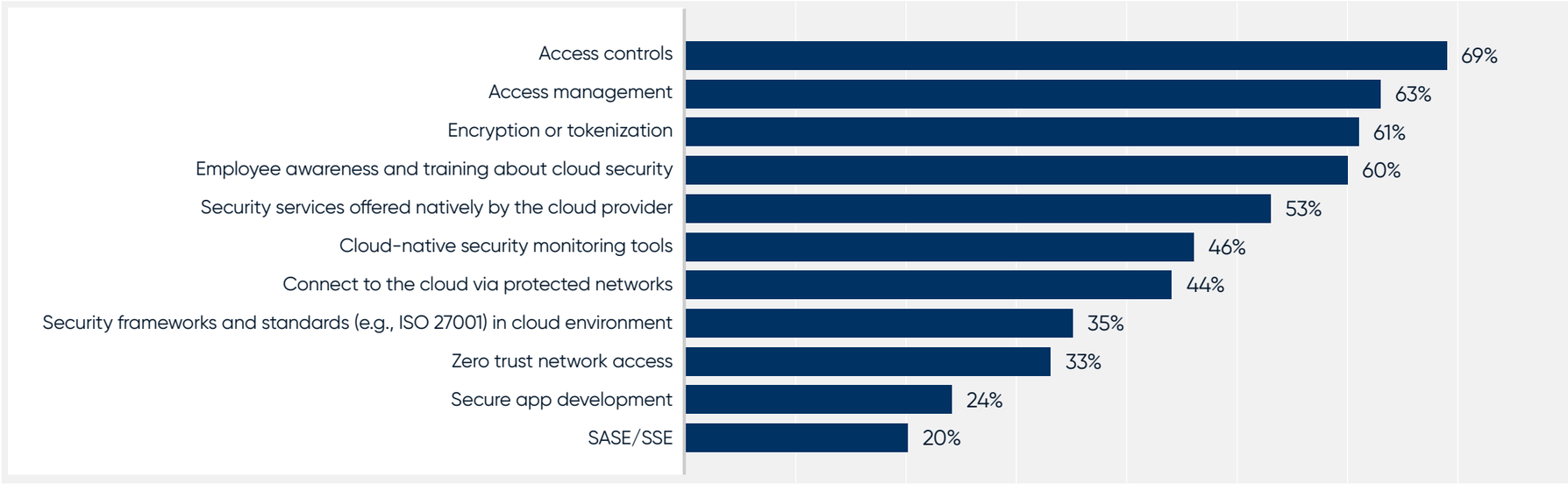
Base: Respondents whose organizations fully manage cloud security on prem or have a third-party hybrid arrangement (n=177).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Cloud Security Survey, January 2024.

"I have a dedicated team for cloud deployments, but I don't have a dedicated team for cloud monitoring and cloud security. So, there's a big gap there. They wear a security hat and operate in a security-minded way, but I don't feel we're as mature as we can be given the complexity and growth and the speed of that growth."

– SURVEY RESPONDENT

Access controls and access management are the top cloud security practices used by organizations.

Q: Which of the following cloud security practices and solutions are used by your organization?



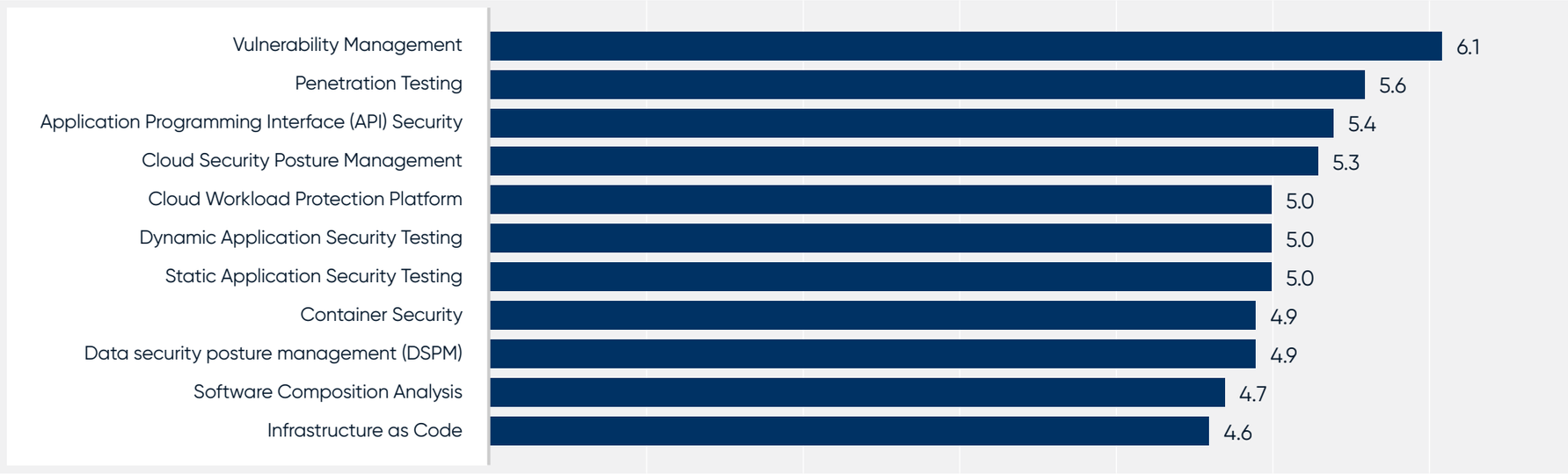
Respondents were asked to select all that apply.
Base: Respondents whose organizations have workloads in the cloud (n=194).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Cloud Security Survey, January 2024.

"Identity is usually the entry point for hackers to get into your system. They send out phishing or social engineering attempts to get identity, and if they do then they can get away with pretty much whatever they want. So we're looking hard at identity and access management tools right now."

– SURVEY RESPONDENT

On average, vulnerability management is the highest-priority approach for protecting organizations against cloud-related threats.

Q: How much does your organization prioritize each of the following in securing your organization against cloud-related threats?



Respondents were asked to rate each on a 7-point scale where 1 is "Not at all a priority" and 7 is "Critical priority."
Chart shows mean scores (out of 7).
Base: Respondents whose organizations have workloads in the cloud (n=194).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Cloud Security Survey, January 2024.

"Look, there's no magic bullet out there. You have to look at cloud security holistically – from user education, to phishing, to email protection, network protection, your API and IAM protection – you have to worry about every component in the security landscape."

– SURVEY RESPONDENT

3

CLOUD SECURITY CHALLENGES

Security teams losing sleep over cloud misconfigurations

Without proper configuration and multi-layered protections in place, one organization's cloud is just another threat actor's bounty.

In the last year, the most common cloud security-related incidents that afflicted respondents were misconfiguration vulnerabilities (35%), lack of visibility (29%), and unauthorized access leading to account compromise (23%).

After budgetary constraints (48%), cloud misconfigurations are the most most cited challenge (40%), followed by multi-cloud security (34%) and third-party risk (31%).

"The thing that really makes me lose sleep at night is the misconfiguration," says one respondent. "We're not mature enough to be able to easily see what's not set up properly. What makes me lose sleep is the fact that this is being done so quickly, and that it's being done both quickly and incorrectly."

Some respondents mentioned how recent attacks (such as the Change Healthcare breach) were a wake-up call to take third-party risk seriously.

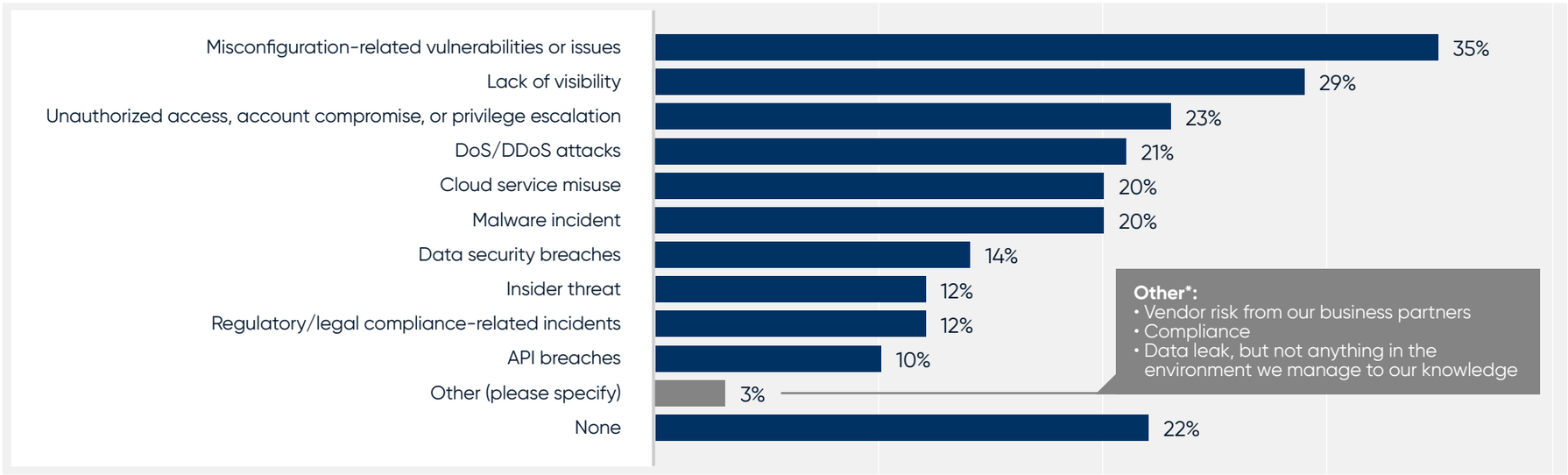
"You can have perfect protection of everything on your turf, but if your third-party vendors don't have a backup plan or their backups are on the same network as their primary servers, then you still won't be spared."

40%

believe misconfigurations are a top challenge to cloud security at their organization

Misconfiguration vulnerabilities are the top cloud-related security incidents, experienced by more than one-third of organizations.

Q: Which of the following types of cloud-related security incidents, if any, has your organization experienced in the last 12 months?



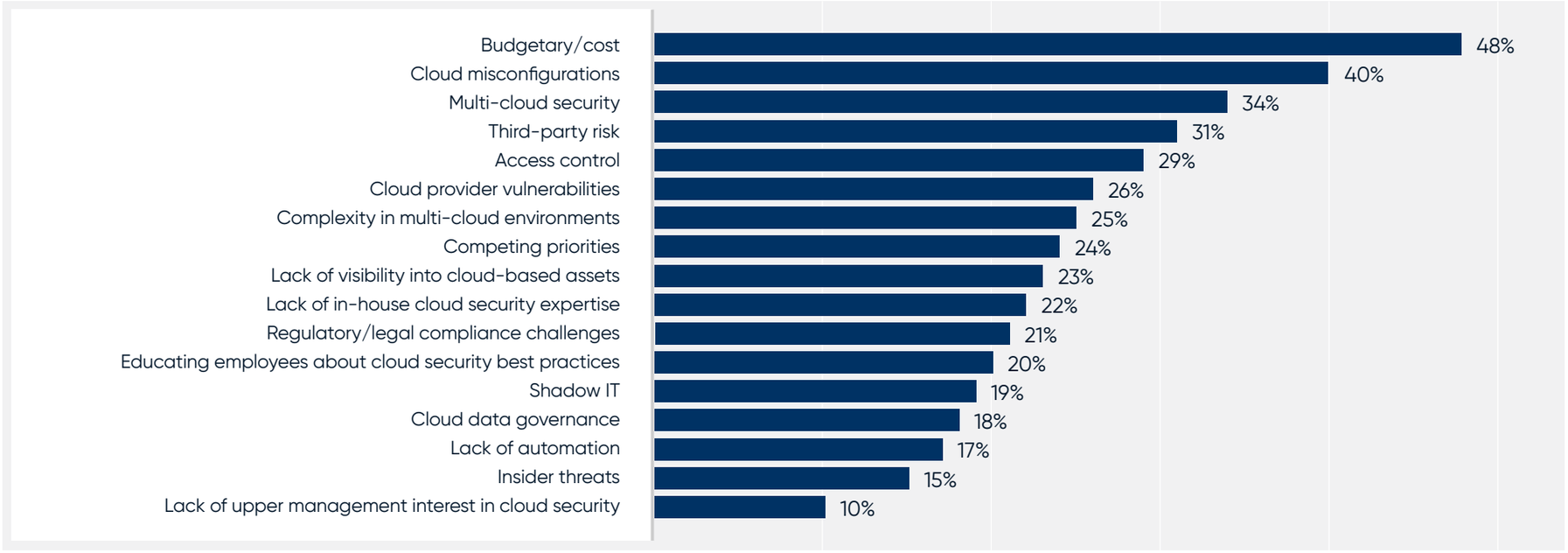
Respondents were asked to select all that apply.
Base: Respondents whose organizations have workloads in the cloud (n=194).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Cloud Security Survey, January 2024.

"Change Healthcare has had a profound business impact [on us]. It impacted our lab interfaces so we were not able to get lab results in real time from our lab providers. We had a workaround, fortunately, where we could login and download the results. But if we did not have that access to the native systems, it could've had significant consequences on the level of care we provide."

– SURVEY RESPONDENT

After budgetary/costs (48%), misconfigurations in the cloud are the most commonly cited security challenge, cited by 40% of respondents.

Q: What are your top concerns or challenges related to cloud security at your organization?



Respondents were asked to select up to 5 choices.
Base: Respondents whose organizations have workloads in the cloud (n=194).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Cloud Security Survey, January 2024.

"The thing that really makes me lose sleep at night is the misconfiguration possibility. We're not mature enough that we're able to easily see what's not set up properly. I mean, it could be something as simple as not installing a particular agent that we have – whether it's EDR or a vulnerability management tool. I worry it's all being done so quickly, that it's possible it's being done incorrectly."

– SURVEY RESPONDENT

Recommendations

We asked a few respondents to provide their recommendations and advice for achieving cloud security maturity. These are their responses.

Governance

"Having a good governance model is important. Understand what it is you're trying to protect and how you're going to go about protecting that. You have to have that framework."

Board Communications

"Talk to the board often about security. When there's a security incident that happens, use that opportunity to make sure they know the impact of the things you're trying to do."

Multi-Faceted Approach

"Take a multi-faceted approach. You need to make this as tight as can be across all areas – from user education, from phishing, to your email, your network, your APIs, and everything. You can't just focus on one piece and ignore the rest of it because you're going to have holes in your security umbrella."

Third-Party Risk

"Do not ignore third-party vendor risk. You can have the perfect protection on everything you have, but if you don't understand your third-party vendors then you are just as exposed."

Team Alignment

"Make sure you partner well. Make sure your infrastructure team, your platform team, and your security team have a good working relationship with each other. Because if one doesn't know what the other is doing, you're going to be disconnected. Go too fast and you may get ahead of the operations folks who can't monitor it, or you may get ahead of the security team where it's not configured properly. So, make sure your teams are aligned and have a common goal."

CyberRisk Alliance Business Intelligence (CRA BI), Cloud Security Survey, January 2024.

4

THE FUTURE OF CLOUD SECURITY

Respondents are cautiously optimistic about AI enhancements to cloud security

Many respondents have an optimistic view of how artificial intelligence could be used to enhance cloud security. Sixty-two percent believe AI will have a positive impact in securing the cloud, compared to 29% who are neutral and 8% who have a negative outlook.

On the one hand, AI could be used to increase automation of common functions, identify trends faster, help analysts use their time more productively, and improve proactive detection of threats to the cloud.

"I think AI can and already has taken user behavior analysis to the next level, and I think we are just scratching the surface on what it will be able to do in the end," writes one respondent.

On the other hand, some are wary of putting too much faith in AI too early.

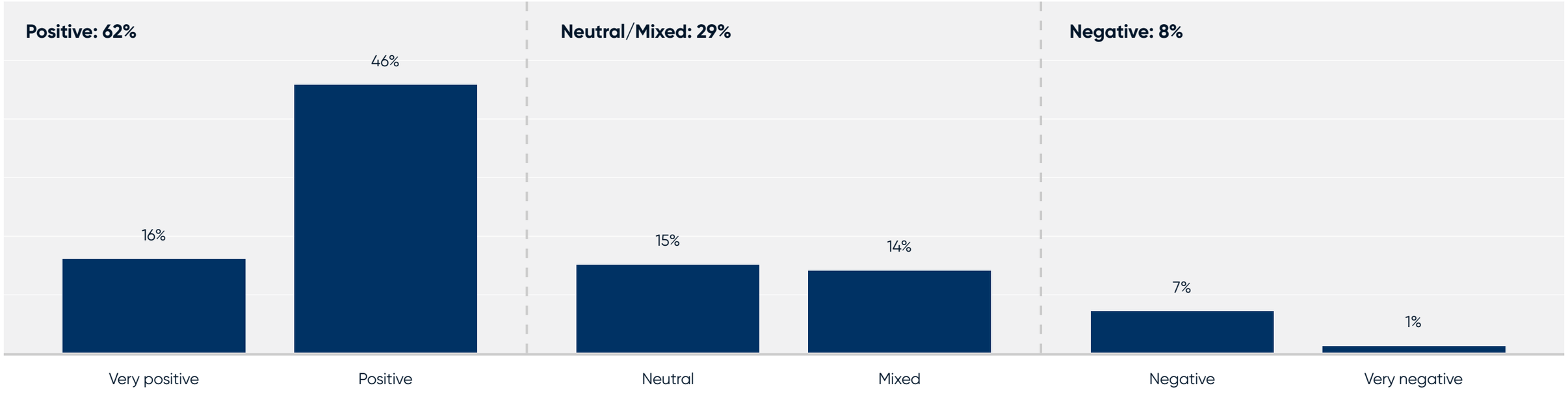
"Since this is the Wild West right now, longevity is important. We don't want to invest in an [AI] product that won't be around in one to three years because the company went out of business."

62%

have an overall positive sentiment about the potential benefits of AI/ML in cloud security

About 6 in 10 respondents have a positive sentiment about the potential for AI/ML to enhance cloud security in the near future.

Q: In your opinion, what impact do you think AI and ML will have in enhancing cloud security in the near future?



Note: Chart is a depiction of sentiment based on open-ended responses.
CyberRisk Alliance Business Intelligence (CRA BI), Cloud Security Survey, January 2024.

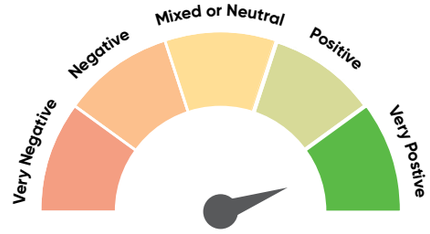
Positive sentiment about AI/ML enhancing cloud security tends to focus on reducing mundane work, automation, and learning from historical data to predict behavioral patterns.

Q: In your opinion, what impact do you think AI and ML will have in enhancing cloud security in the near future?

"I think it will reduce quite of bit of 'noise' and mundane work."

"AI may provide capability to detect and respond to threats in real time and anticipate potential threats. May also help us automate security processes which minimizes human error and improves our security posture."

"Hopefully (and ideally) AI and ML will learn from historical data and will be able to predict new threats based on past behavioral patterns."



"Huge... the ability to see complex data patterns will create more buy-in for the need for change."

"Predictions, analysis, and rapid responses will be night and day beyond what is currently available through traditional means."

"It has a huge impact on the regulatory and compliance and legal perspective."

"Big impact on log review/SIEM to detect low noise/signals and long-term anomalies."

CyberRisk Alliance Business Intelligence (CRA BI), Cloud Security Survey, January 2024.

Some respondents worry about AI/ML providing a false sense of security and concerns about data privacy, employee attrition, the malicious intent of AI, and the lack of human-led security.

Q: In your opinion, what impact do you think AI and ML will have in enhancing cloud security in the near future?

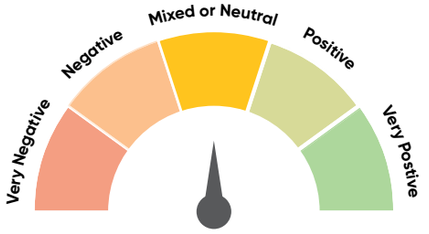
"They will build in lots of assumptions that are not necessary. They will give a false sense of security. They'll get just enough right to be of promise, reduce budgets, and leave gaping holes where you least expect them."

"With these technologies we have an existential threat to security. I worry greatly that without oversight we will have issues."

"The primary concern is the PII or customer data that is sent to third-parties."

"Financial issues with losing employees and work overload for the remaining employees."

"I am unconvinced that AI/ML will do more than some generative tooling."



"It could improve automation, but also has the potential to be used maliciously."

"Huge improvements in productivity, reactivity, and security.... or it is how humans will end up answering to robots."

"Will be a benefit if used to supplement human-led security. Will be a detriment if people think it can do everything."

CyberRisk Alliance Business Intelligence (CRA BI), Cloud Security Survey, January 2024.

Survey methodology

The data and insights in this report are based on an online survey conducted in January 2024 among 202 security and IT leaders and executives, practitioners, administrators, and compliance professionals in North America from CRA's Business Intelligence research panel.

Further insights from follow-up phone interviews with several respondents are also included.

The objective of this study was to explore various issues and topics related to organizations' cloud security strategy, efforts, challenges, AI, and related opinions.

Notes:

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

The respondent profile is as follows:

IT or IT security roles/titles:

- CISOs/CROs/CIOs/CTOs (10%)
- VPs/SVPs/EVPs (8%)
- Directors (31%)
- Managers (29%)
- IT/security admins (18%)
- Analysts/consultants (4%)

Organization sizes:

- Small (1 to 99 employees) (11%)
- Medium (100 to 999 employees) (24%)
- Large (1,000 to 9,999) (42%)
- Enterprise (10,000 or more) (23%)

Top industries:

- High-tech, IT software, or telecom (19%)
- Education (17%)
- Manufacturing (14%)
- Healthcare (11%)
- Financial services (9%)
- Professional services (consulting, legal, etc.) (6%)
- Retail, trade, or eCommerce (5%)

Other CRA Business Intelligence reports

2024

1. Navigating the identity security minefield (March 2024)
2. Threat Intelligence: Organizations seek expertise and guidance to help build their threat intelligence programs (February 2024)
3. The zero-trust dilemma: Ensuring a positive user experience and getting leadership buy-in (January 2024)

2023

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

2022

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

CRA Business Intelligence contacts

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

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

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

About CyberRisk Alliance

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