Cloud Security Report 2023

CYBER SECURITY HUB

THE FUTURE OF CLOUD SECURITY

Insight from cyber security professionals on visibility, misconfigurations and threat detection and response in the cloud

INSIDE:

- The primary cloud security concerns of security professionals
- Where investments are being made in cloud security controls
- Making the business case for cloud security

Brought to you in association with

eSENTIRE

Introduction

As organizations around the world prioritize digitization, the focus on cloud security is rapidly growing.

Security flaws such as limited visibility, lack of threat detection and response capabilities, and the inability to detect unknown threats or misconfigurations within cloud environments, can all have devastating consequences. Misconfigured cloud resources can cause unintentional data leaks, and an inability to detect and respond to threats can allow malicious actors to wreak havoc, with organizations only discovering the damage when it is far too late.

With this in mind, *Cyber Security Hub* has conducted a survey of more than 700 cybersecurity professionals from a range of regions, industries and job roles to gain key insights into the current trends, challenges and investment opportunities in the world of cloud security.

The report contains an analysis of the data collected in addition to insights from cybersecurity practitioners at eSentire, Lacework, Voices.AI and *Cyber Security Hub*'s Advisory Board.

Contents

Olivia Powell
Editor
Cyber Security Hub

About the respondents

This section explores the job roles, regions, industry and company and budget size of the 708 cybersecurity professionals surveyed for this report.

Figure 1

What is your job role?

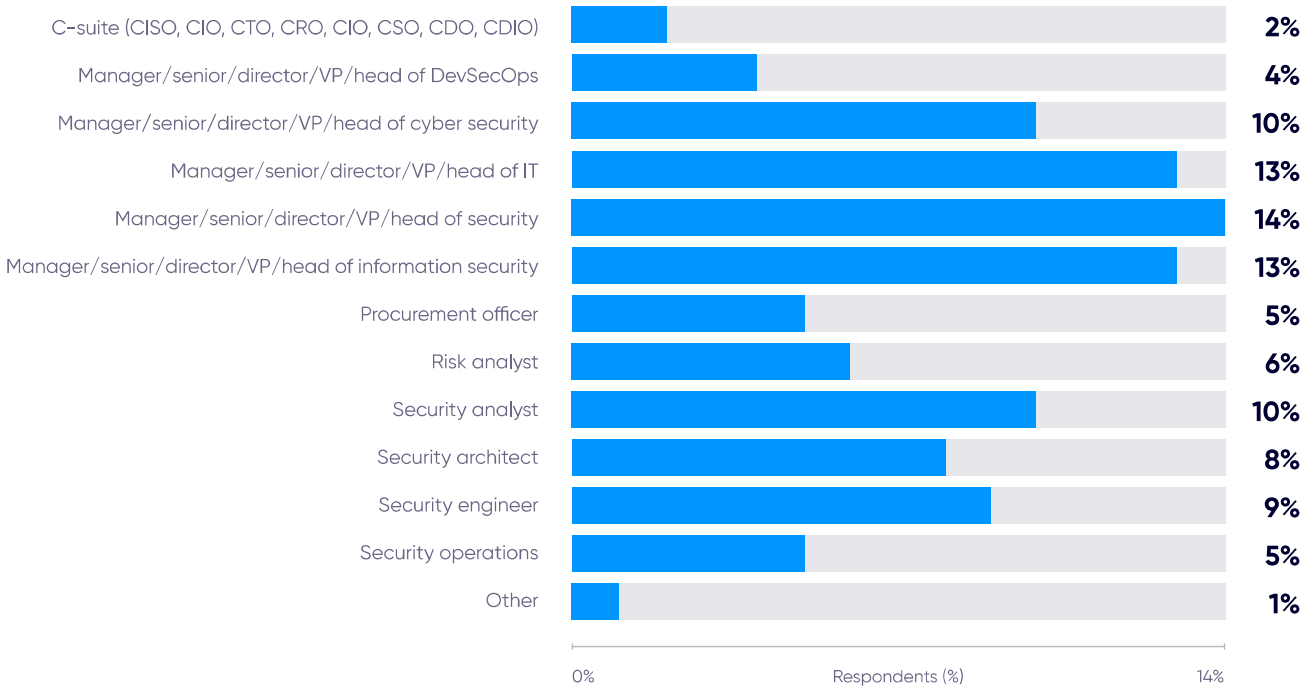
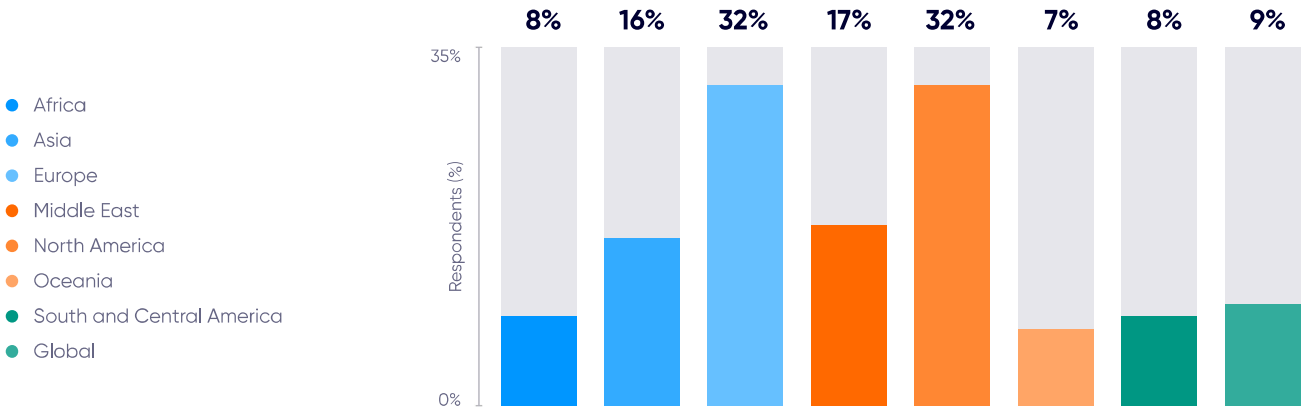


Figure 2

What region(s) do you/your company provide services for?



Source: *Cyber Security Hub's Future of Cloud Security survey, April–May 2023*

About the respondents

Figure 3

Which industry vertical best describes where your organization sits?

11% Manufacturing	10% Communications	9% Energy	7% Construction	7% Healthcare
6% Education	6% Government	6% Leisure/hospitality	5% Software vendor	5% Insurance
4% Oil and gas	4% Banking/finance	4% Military	4% Minerals/mining	3% Pharmaceuticals/life sciences
3% Legal	3% Transportation	1% Communications	1% Retail/wholesale	1% Utilities

"The emergence of dynamic and transient environments in the cloud has enhanced complexity and generated unexpected interactions."

Charles Denyer
Cyber Security Hub **Advisory Board member and cyber security consultant**

About the respondents

Figure 4

What is your company size?

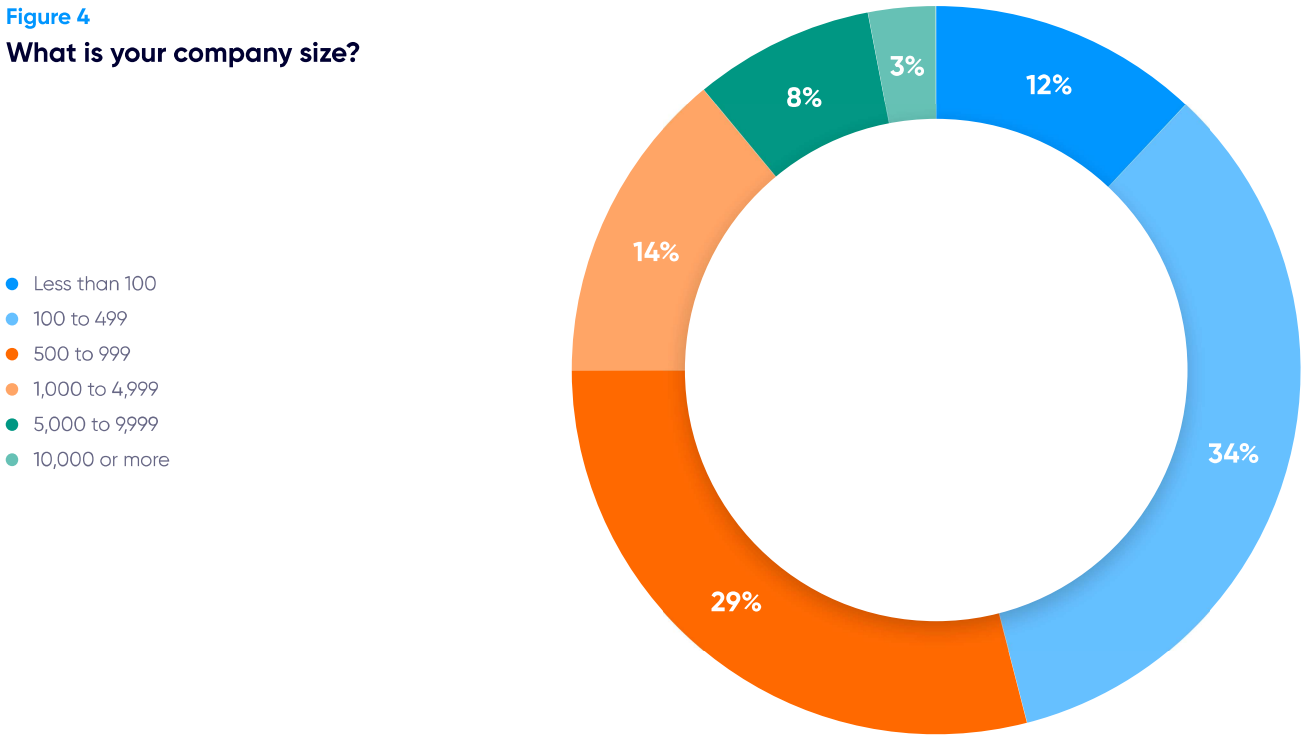
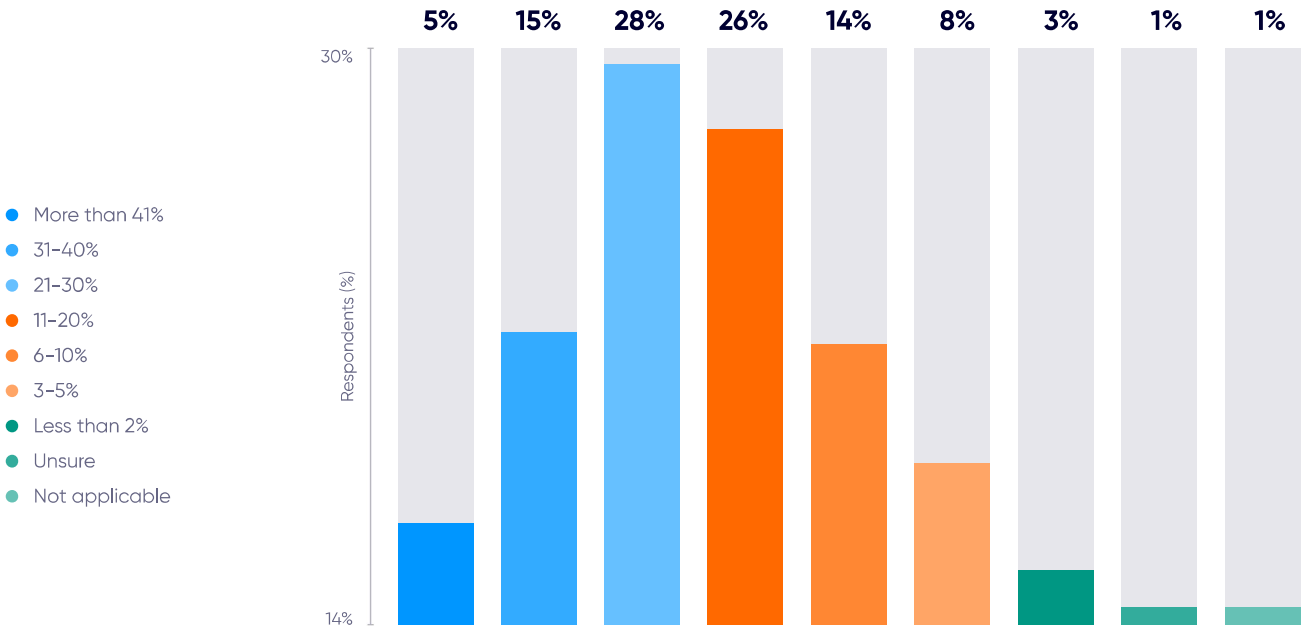


Figure 5

How much of your security budget is currently allocated to cloud security?



Source: *Cyber Security Hub's Future of Cloud Security survey, April–May 2023*

eSENTIRE | CYBER SECURITY HUB

The current state of cloud security

Figure 6

What are the top cloud threat detection challenges you face?

Note: respondents could select three answers

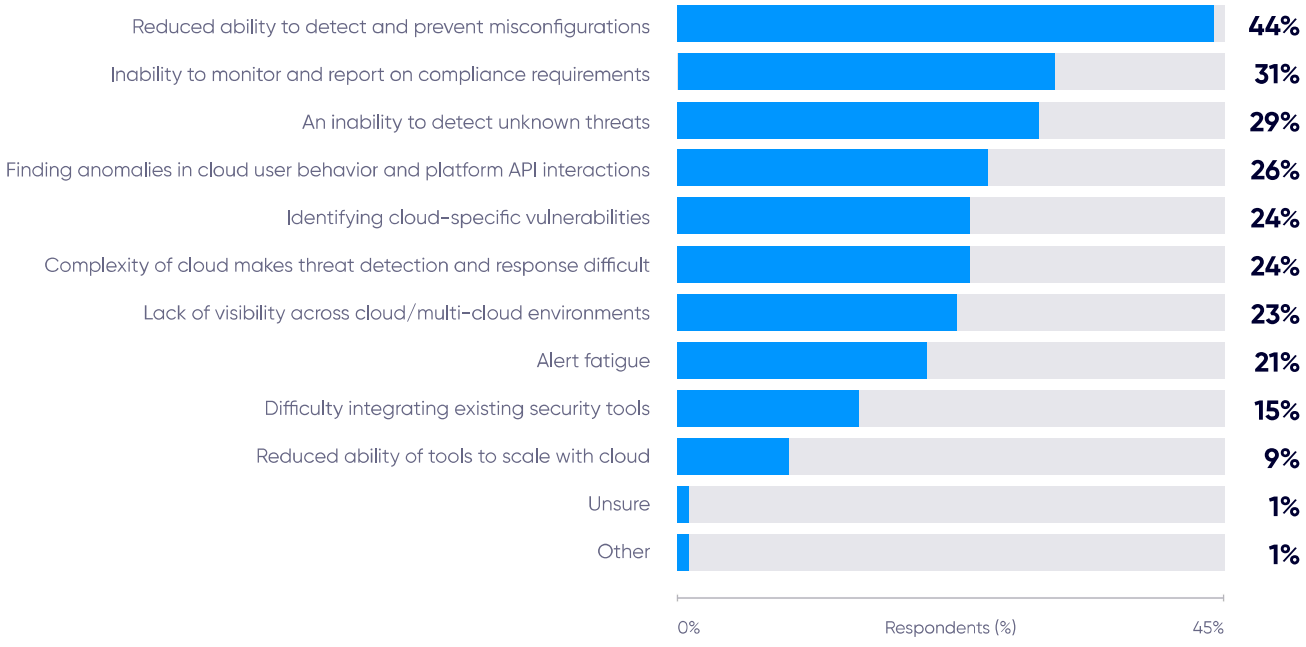
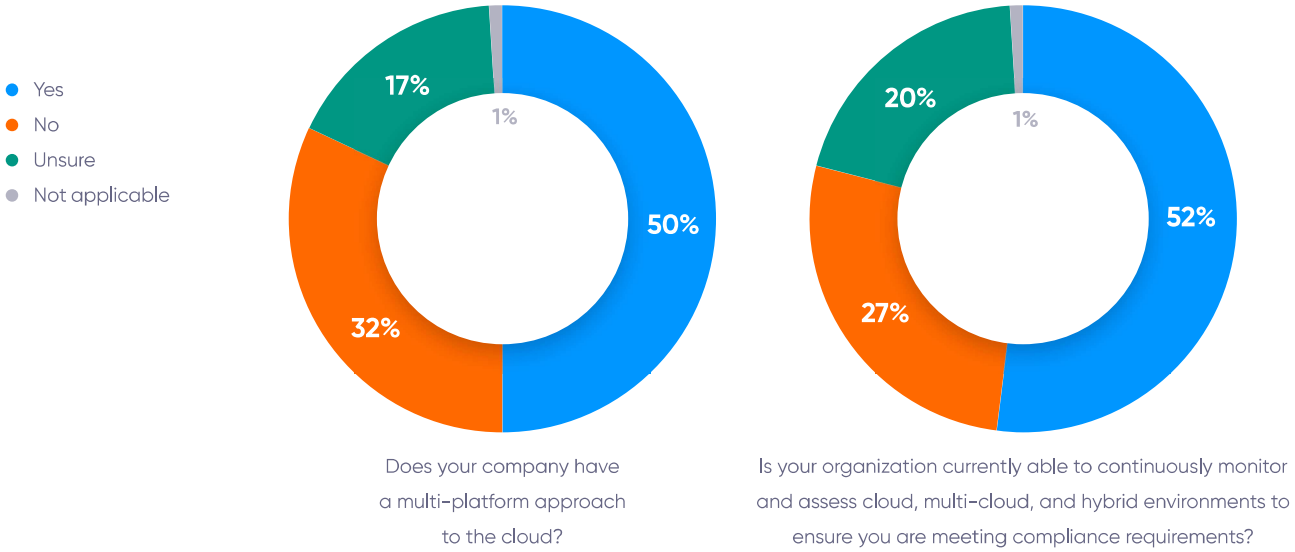


Figure 7

Respondents were asked to answer the following questions about their company's cyber security offering:



Does your company have a multi-platform approach to the cloud?

Is your organization currently able to continuously monitor and assess cloud, multi-cloud, and hybrid environments to ensure you are meeting compliance requirements?

Source: *Cyber Security Hub's Future of Cloud Security survey, April–May 2023*

eSENTIRE | CYBER SECURITY HUB

The current state of cloud security

With the advent of digitalization, more companies are migrating their data to the cloud than ever before. Cloud storage and compute resources may offer benefits for organizations such as increased efficiency for both operations and cost and improved data security, but it also opens a larger attack surface for malicious actors.

Cyber Security Hub Advisory Board member and cyber security consultant Charles Denyer explains: "New security concerns of all shapes and sizes have been introduced by the move to the cloud. The emergence of dynamic and transient environments in the cloud has enhanced complexity and generated unexpected interactions.

"Critical data is now housed on the cloud, where a single misconfiguration can have significant repercussions, as opposed to the past when all data was protected on-premises with physical barriers and controls."

The expanded attack surface and added security needs can cause issues for cyber security teams. This was corroborated by almost half of respondents (44 percent) as they said their number one challenge to cloud security was a reduced ability to detect and prevent cloud misconfigurations (see figure 6). Misconfigurations in the cloud, which occur because of improper settings being used when architecting and deploying services within cloud platforms, can cause data breaches that have a business-wide impact. For example, the American Bar Association reported a breach in April 2023 caused by a misconfigured cloud server that **exposed the data of 1.4 million members.**

Likewise, almost a third of respondents (31 percent) reported an inability to monitor and report on compliance requirements as their biggest challenge when it comes to cloud security. If cyber security teams are unable to meet these regulatory requirements, it can have severe consequences for their organization. James Hastings, senior cloud product manager at eSentire, notes that when dealing with compliance requirements, it is important that cyber security teams understand the underlying motivations.

Hastings notes: "Some compliance leaders are truly interested in security, while others are simply looking to check a box. Regardless of their motivations, the desired outcomes of compliance buyers are often the same, such as logging, vulnerability scanning and attestation scans."

This lack of visibility across cloud and multi-cloud environments can cause challenges when monitoring and detecting cyber threats that can allow attackers to gain initial access. More than a quarter of respondents (26 percent) cited an inability to detect unknown threats as their top cloud security challenge. Poor visibility highlights a critical need for multi-signal coverage which collects data and telemetry across multiple sources within an environment including endpoint, network, log, and cloud resources. As malicious actors expand their attack vectors and new threats emerge, shortcomings in cloud security coverage and multi-signal visibility may lead to successful cyber attacks, data breaches and data leaks if not properly addressed.

When considering how to increase visibility in cloud environments, cloud security and DevOps consultant Youssef El Achab notes that cloud security solutions themselves can be used to help mitigate this threat by providing continuous monitoring and analysis of user behavior and resource access patterns.

How to make the case for cloud security

When considering their ability to roll out cloud security business-wide, it is important for cyber security professionals to make sure they are in the optimal position not only to roll out cloud but to make its business case to stakeholders.

The current state of cloud security

Only about half (52 percent) of respondents say their organization is currently able to continuously monitor and assess cloud, multi-cloud and hybrid environments to ensure it is meeting compliance requirements. More than a quarter (27 percent) say that their organization does not monitor their environments to ensure they are meeting regulatory requirements and one in five (20 percent) say they are unsure of their company's ability to do this.

Considering 31 percent of respondents reported an inability to monitor and report on their organization's ability to meet compliance requirements as a top challenge to cloud security, uncertainty regarding compliance remains an ongoing issue in cloud environments.

Tim Chase, global field CISO at Lacework, explains that this uncertainty may be because companies are failing to recognize the tools needed to ensure proper cloud security "the[se companies] still think about firewalls and wonder how they can fit their existing tools into the cloud," Chase remarks. "When they try that, they get overwhelmed by the failure of the tools to perform well and provide meaningful results. They end up putting everything into security information and event management (SIEM) and then being underwhelmed by the visibility it provides."

This insight from Chase may explain why the top three cloud security challenges faced by respondents all relate to their threat detection, network monitoring and response capabilities. This also may be because, according to Chase, the switch to a cloud operating model "requires a new way of thinking", which can lead to expertise problems on the security team when trying to implement cloud security.

As a result, it is critical that cyber security teams have the right tools and infrastructure to detect potential threats and respond quickly to minimize threat actor dwell time. Investing in security automation and 24/7 managed detection and response can help organizations create a more effective and efficient security posture while reducing costs.

The respondents were split on multi-platform approaches to the cloud, with half saying their organization does have a multi-platform approach to the cloud, around a third (32 percent) saying they do not and 17 percent saying they are unsure of their organization's approach to the cloud. Chase notes that a multi-platform approach to the cloud can be beneficial as there is so much data involved in cloud security.

David Ciccarelli, founder and CEO of artificial intelligence platform Voices.AI, shares that when it comes to having a multi-platform approach to cloud security, there are benefits and drawbacks that must be evaluated on a case-by-case basis.

Ciccarelli says: "On one hand, you get the best features and tools from different providers, which can boost your overall security. On the flip side, managing multiple platforms can be tricky and might make your security architecture more complex. It is all about finding that sweet spot between flexibility and control."

Hastings adds that while multi-cloud environments can provide disaster recovery or fault tolerance in case one cloud provider has an issue, they can also make it harder to have a complete view of what is happening across said environments. This can mean that it can be easier to compromise a company's security posture and increase the

The current state of cloud security

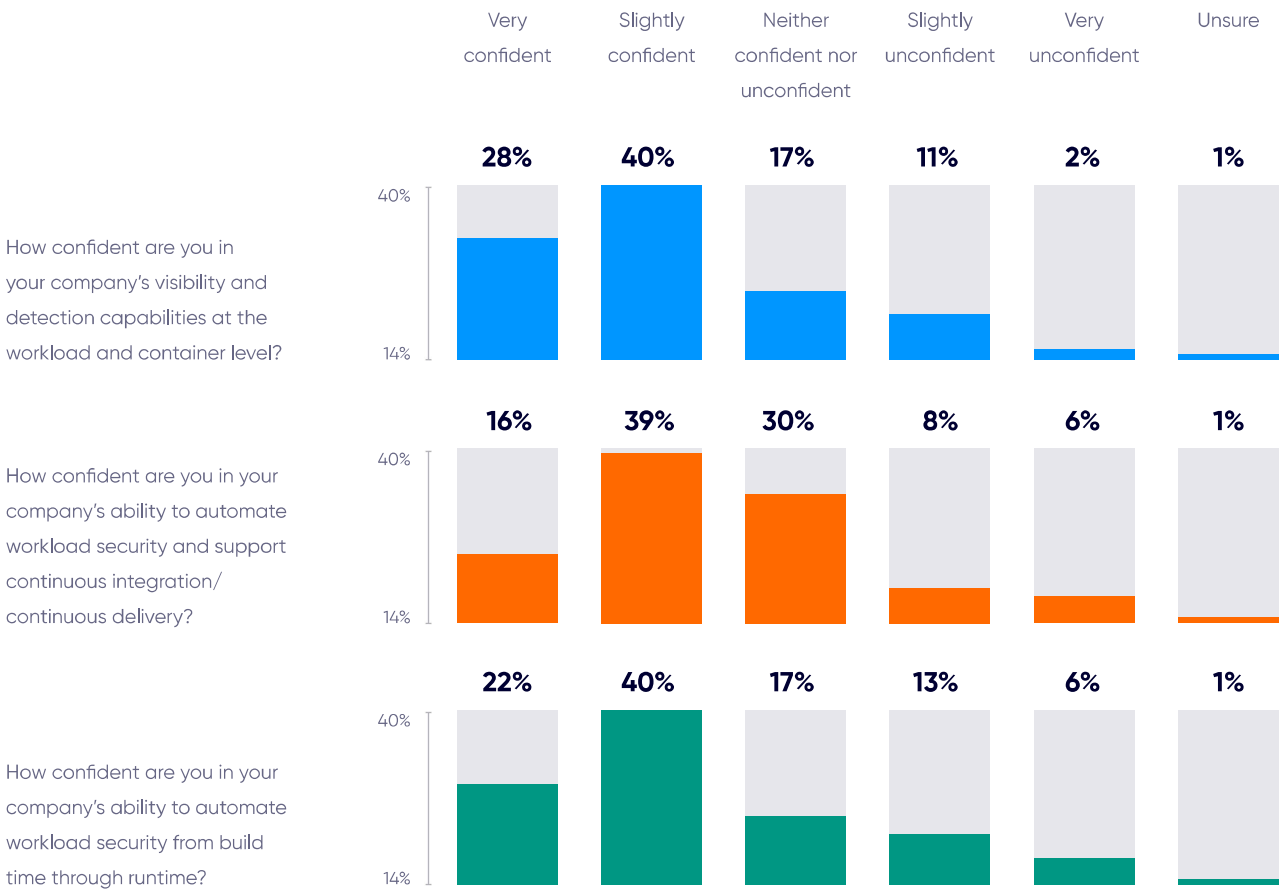
number of entry points malicious actors can exploit. With visibility compromised, this can further benefit hackers as their malicious activity may go unnoticed until it is too late.

To reduce confusion when it comes to what data is being stored in cloud environments and, therefore, reduce the likelihood of cyber security teams not meeting regulatory requirements, Anthony Lim, fellow of cyber security and governance at Singapore University of Social Sciences, says cyber security teams need to have a central policy and clear visibility on what data from which department are being placed in cloud services. This also includes which person in each department oversees and authorizes this process.

Additionally, Lim suggests that organizations use a centrally managed and enforced data classification system that decides what data sets are allowed to be stored in cloud services to ensure that regulatory compliance is then baked into the security of these cloud services.

Figure 8

How confident are you in your company's cyber security abilities?



Source: *Cyber Security Hub's Future of Cloud Security survey, April–May 2023*

The current state of cloud security

How to increase confidence in cyber security capabilities

Considering the range of cyber security professionals that responded to the survey, the fact that the leading survey responses were only 'slightly confident' shows cyber security teams are slightly lacking confidence in their company's cyber security capabilities is an industry-wide issue.

Only 28 percent of respondents report being 'very confident' in their company's visibility and detection capabilities at the workload and container level. Likewise, less than one in five (16 percent) said they were 'very confident' in their company's ability to automate workload security and support continuous integration/continuous delivery. Additionally, 22 percent reported being 'very confident' in their company's ability to automate workload security from build time through runtime.

When asked for more information on why they had this level of confidence in their company's cyber security abilities, survey respondents cited internal issues as the reason for their confidence being lower than it could be. One respondent explained that within their organization, "knowingly or unknowingly, insiders leak, destroy network systems or alter recorded information [which can lead to] the unauthorized use of network resources, including illegal operations on the system, illegal users entering the network or unauthorized operations by legitimate users".

These issues with illegitimate access and insider threats can be exacerbated by cloud security issues. While mature organizations can implement policies and processes around who can create the workloads, how to deploy them and ensure they are monitored continuously, smaller organizations may have smaller cyber security teams that are unable to ensure this level of monitoring. As noted previously, respondents to the survey said their top issues with cloud security included an inability to detect and respond to unknown threats and monitor compliance. This increases the likelihood of cyber security incidents, data breaches and leaks.

To decrease the likelihood of insider threats and malicious unauthorized access, Youssef Al Echab says that organizations should employ cloud security solutions that also use machine-learning algorithms to detect anomalies in user behavior and identify potential insider threats. These solutions can also enforce access controls and apply policies to prevent unauthorized access or activity.

Investing in cloud security

Figure 9

How far along in its cloud adoption journey/maturity is your company?

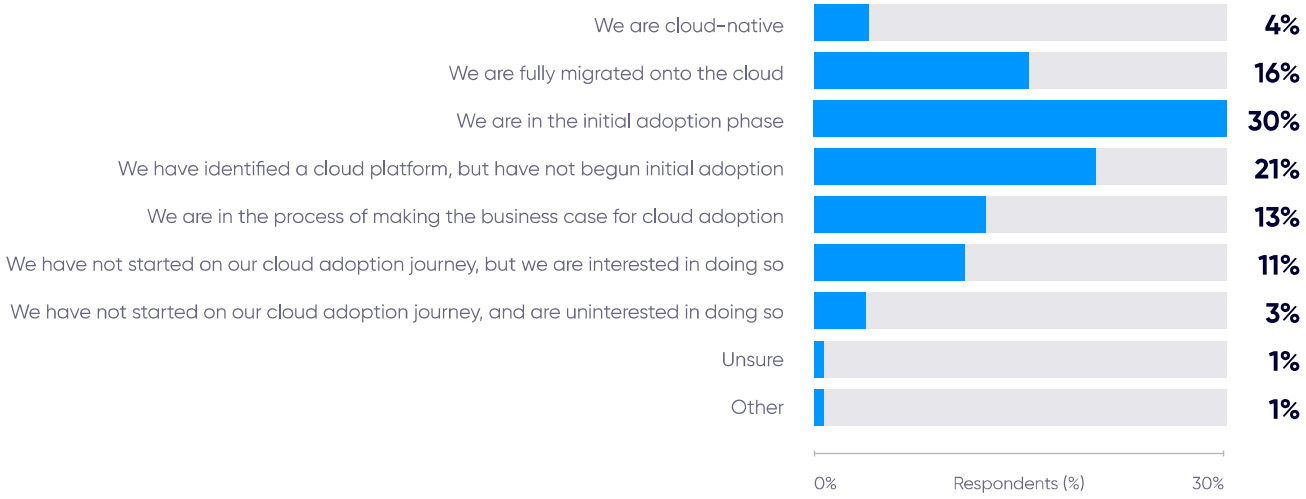
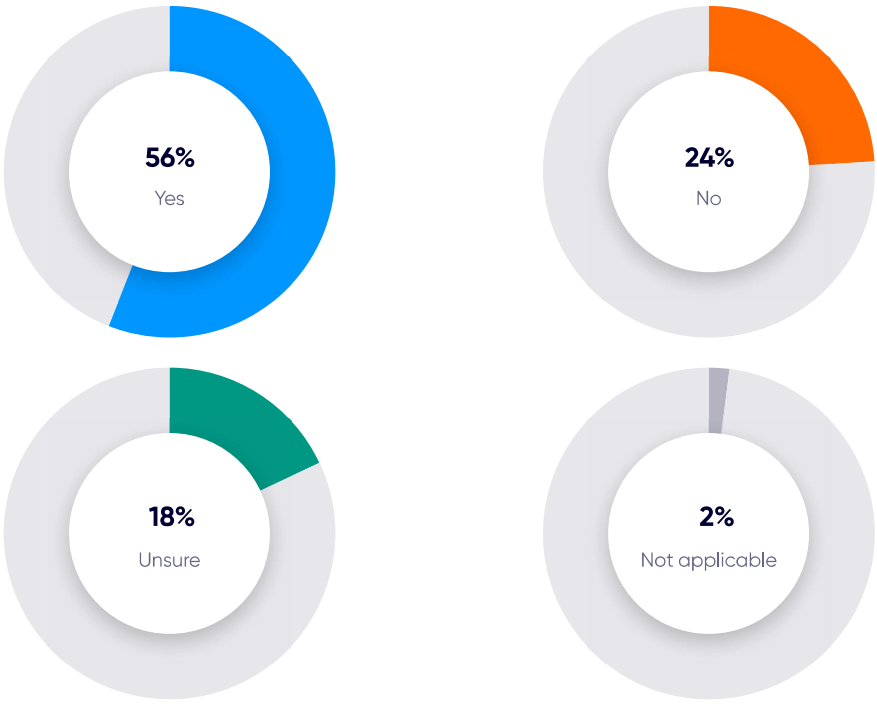


Figure 10

Do you look for the use of terms like CSPM, CWPP, CIEM and CNAPP when searching for security technology?

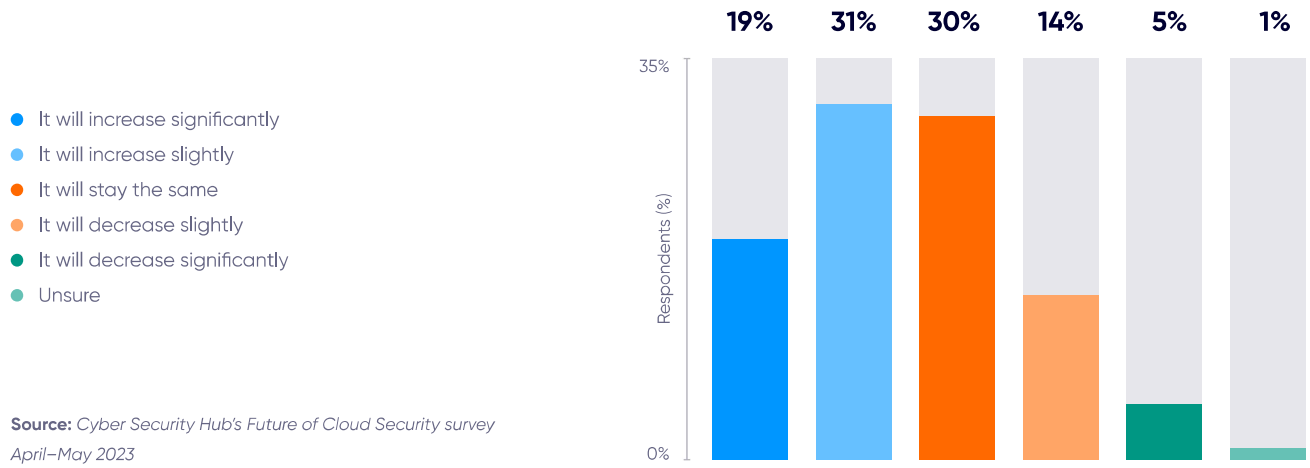


Source: *Cyber Security Hub's Future of Cloud Security survey, April–May 2023*

Investing in cloud security

Figure 11

How do you think your company's investment in cloud security will change over the next 12 months?



Source: *Cyber Security Hub's Future of Cloud Security survey April–May 2023*

While cloud security is undoubtedly a top priority for those both within and outside the cyber security industry, 64 percent (figure 10) are just beginning of their cloud security journey.

When surveyed by *Cyber Security Hub*, most respondents (51 percent) said they were just starting their cloud adoption journey, with 21 percent identifying a cloud platform but not yet beginning cloud adoption and 30 percent in the initial adoption phase. Additionally, only four percent of respondents said their organization is fully cloud-native. This shows that while cloud security itself is definitely a growing field, it is still in its infancy for the majority of cyber security teams.

When considering how to best roll out cloud security business-wide, eSentire's Hastings advises that organizations make stakeholders part of the process.

"To gain stakeholder buy-in and investment, cyber security professionals need to focus on the desired outcomes of the organization and tailor their approach to address those needs. This involves understanding the motivations and priorities of stakeholders, mapping compliance requirements to individual services, and being prescriptive in terms of proposing solutions that can help achieve desired outcomes," he explains.

How and why cloud security investment will increase

With cloud security an increasing priority, investment in it is already high and is only set to increase. This can be seen through *Cyber Security Hub*'s research, which saw 26 percent of respondents say 11–20 percent of their cyber security budget is allocated to cloud security and 28 percent of respondents say that 21-30 percent of their budget is allocated to cloud security.

Additionally, 61 percent of those surveyed said they predict that their company's investment in cloud security will either slightly or significantly increase over the next 12 months.

When investing in cloud security, respondents said they are looking for enhanced threat detection and response capabilities, as well as increased network visibility and the ability to protect private information. This is in-keeping with the internal security issues already flagged by respondents earlier in the survey, showing that cyber

Investing in cloud security

security professionals are keen to overcome the cloud security challenges they are facing, not by moving away from cloud security but by investing more in it.

This is also shown by more than half of the respondents (56 percent) noting that they look for the use of specialist terms like cloud security posture management (CSPM), cloud workload protection platform (CWPP), cloud infrastructure entitlement management (CIEM) and cloud-native application protection platform (CNAPP) when searching for security technology to invest in. One respondent, however, did note that they dislike when companies use these acronyms as "buzzwords" when advertising their cloud security offerings as it means that it can become confusing or unclear as to what the company's actual offering is.

In conclusion, when looking for cloud security services to invest in, cyber security professionals want to ensure the services address any issues they are already struggling with in their current cloud security offering. Additionally, cyber security professionals want the offering to be easy to roll out and to not be too confusing.

Final remarks

Cloud security is becoming a need-to-have for organizations around the world and it is important to balance a comprehensive posture management with 24/7 high-touch response no matter the cloud environment. With the majority of respondents just starting their cloud adoption and migration journey, this can lead to security flaws and vulnerabilities as companies roll out a cloud security solution across the business.

To address the top three cloud security challenges highlighted in this report – a reduced ability to detect and prevent cloud misconfigurations, an inability to monitor and report on compliance requirements, and an inability to detect unknown threats – cyber security professionals can look to implement solutions with Cloud Security Posture Management (CSPM) and Cloud Workload Protection (CWPP) capabilities. These tools can help address these issues by providing 24/7 visibility, monitoring, scanning and control over cloud environments and applications

Additionally, combining 24/7 managed detection and response (MDR) with CSPM and CWPP platforms can help to ensure that critical security policy violations are proactively identified, prioritized and resolved. This is because MDR providers can remediate cyber security flaws that may lead to data breaches or leaks, for example critical cloud misconfigurations, behavioral anomalies, and policy and compliance violations. An MDR provider's 24/7 security operations center (SOC) cyber analysts will continuously monitor and assess your environment for compliance with policies, automatically detecting anomalies and providing remediation and prioritization guidance.

Cyber security leaders should also consider working with an MDR provider that can ingest and correlate signals across cloud and on-prem environments. A multi-signal approach can help security operations teams prevent attackers from gaining an initial foothold and initiate manual containment at multiple levels of the attack surface. This can also help build cyber resilience even in the face of advanced cyber threats.

eSENTIRE | LACEWORK

You're in the cloud. We're all in to protect you.

Whatever the cloud brings to your business, we're all-into keep you ahead of disruption.

Our experts provide seamless monitoring, scanning and control over your cloud environments and applications, delivering unmatched visibility, multi-signal correlation and complete protection from cloud-specific threats.

Start building comprehensive cloud security that scales and prevents business disruption with eSentire 24/7 Managed Detection and Response, Cloud Security Posture Management (CSPM), and Cloud Workload Protection (CWPP).

Learn More

ON-DEMAND WEBINAR

The Security Leader's Guide to Detecting and Responding to Threats in the Cloud

with James Hastings, Sr. Cloud Product Manager, eSentire and Tim Chase, Global Field CISO at Lacework

Learn about the top cloud security challenges leaders face and how you can achieve full visibility and complete protection from cloud-specific threats.

Watch Now

Cyber Security Hub Calendar 2023

	Focus Topic	
JAN	Network Security	**ONLINE EVENT** New Event *(TBC)* **INDUSTRY REPORT** Government and Critical Infrastructure EMEA and US **EXPERT INSIGHTS EBOOK** Detection and Response **WEBINAR** CS Hub Presents *(Topic TBC)*
FEB	Threat Defense	**ONLINE EVENT** **CS Summit:** Detection and Response 2023 **INDUSTRY REPORT** Government and Critical Infrastructure APAC
MAR	Ransomware	**ONLINE EVENT** **CS Summit:** Third Party Risk Management 2023
APR	Incident Response	**ONLINE EVENT** **CS Summit:** Cloud Security APAC 2022 **INDUSTRY REPORT** Data Loss and Prevention EMEA and US **WEBINAR** CS Hub Presents *(Topic TBC)*
MAY	Data Centre Cyber Security	**ONLINE EVENT** **CS Summit:** Global 2023 **INDUSTRY REPORT** Data Loss and Prevention APAC
JUN	Cloud Security	**EXPERT INSIGHTS EBOOK** Third-party Risk Management
JUL	Security Architecture	**ONLINE EVENT** **CS Summit:** APAC 2023 **INDUSTRY REPORT** Mid-Year State of Cyber Security report EMEA and US **WEBINAR** CS Hub Presents *(Topic TBC)*
AUG	Malware	**ONLINE EVENT** **CS Summit:** Threat Intelligence 2023 **INDUSTRY REPORT** Mid-Year State of Cyber Security report APAC
SEPT	XDR and EDR	**ONLINE EVENT** **CS Summit:** Gov & Critical Infrastructure APAC 2023 **MARKET UPDATE** Threat Intelligence
OCT	Security Strategy	**ONLINE EVENT** **CS Summit:** EMEA 2023 **INDUSTRY REPORT** Annual Outlook on Cyber Security US and EMEA **WEBINAR** CS Hub Presents *(Topic TBC)*
NOV	Internet of Things Security	**ONLINE EVENT** **CS Summit:** Detection and Response APAC 2023 **INDUSTRY REPORT** Annual Outlook on Cyber Security APAC
DEC	Mobile	**ONLINE EVENT** **CS Summit:** North America 2023 **MARKET UPDATE** Detection and Response APAC

If you are interested in **becoming a CS Hub contributor**, please get in touch with our editor Olivia Powell: **olivia.powell@cshub.com**

If you would like to be **positioned as a thought leader, promoting your offering to CS Hub's extensive community** of cyber security experts and professionals through reports published throughout the year, please get in touch with our director of sales Imran Shafi: **imran.shafi@cshub.com**

eSENTIRE | CYBER SECURITY HUB