aqua

Evolution of Cloud Security
From CSPM to CNAPP

Cloud Security Survey Results

Table of contents

Cloud Security Posture Management (CSPM) is an important component of a holistic Cloud Native Application Protection Platform (CNAPP). Initially seen as distinct or even as a replacement for a CNAPP, CSPM focused primarily on identifying and managing security risks across cloud configurations, aiming to ensure compliance and governance in cloud environments. This infrastructure layer security made CSPM a significant tool for organizations navigating the complex, dynamic nature of cloud native applications.

However, as the cybersecurity landscape evolved, so has the integration of security technologies. CNAPP emerged as a holistic solution designed to secure cloud native applications across their entire lifecycle, from development to build to runtime. While CSPM and CNAPP are not the same, the role of CSPM within a CNAPP is an important piece. It serves not just as a mechanism for configuration management and compliance monitoring but enhances visibility, manages vulnerabilities, and strengthens the overall security posture within cloud native ecosystems.

This convergence of capabilities within CNAPP solutions mark a significant shift in the cloud native landscape, offering comprehensive protection for both the infrastructure and the application under a single umbrella. To gain deeper insights into this evolving landscape, we conducted a survey targeting security leaders at the forefront of the industry.

The survey results depict an industry in flux. Cloud environments and teams are advancing in their cloud journeys, resulting in heightened complexity, alongside the emergence of sophisticated and elusive attacks that defy traditional security measures. Consequently, CISOs are grappling with the question: Does our security stack align with this new-world view of CSPM as an integrated part of CNAPP?

> **The distinctive feature of CNAPP solutions currently offered by vendors is the integration of several capabilities that were previously offered as standalone products. These most often include Cloud Security Posture Management (CSPM) for identifying vulnerabilities and misconfigurations in cloud infrastructures, Cloud Workload Protection Platforms (CWPP) that deal with runtime protection of workloads deployed in the cloud (such as virtual machines, containers, and Kubernetes, as well as databases and APIs), and Cloud Infrastructure Entitlement Management (CIEM) for centralized management of rights and permissions across (multi-)cloud environments.**
>
> **- 2024 KuppingerCole Leadership Compass**

Understanding the Role of CSPM: A Multifaceted Approach to Security

Question 1

What are the top 3 common buying triggers, events or conditions that set you in search of a CSPM solution?

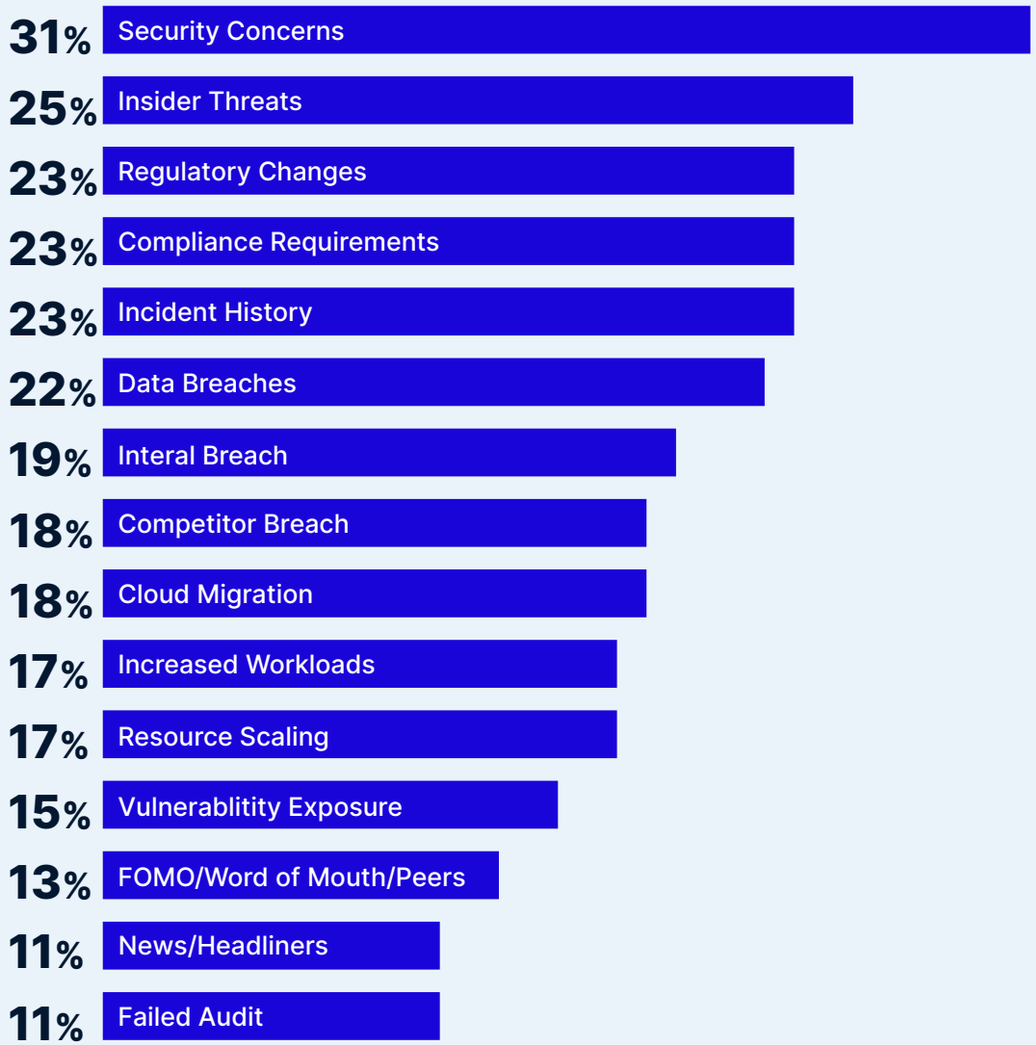
There are many reasons why security teams adopt a CSPM solution. Top of the list here is Security concerns (31%) followed by Insider threats (25%), and Regulatory changes (23%). This aligns with what CSPM was created to do, as CSPM traditionally works to identify misconfigurations and compliance risks, monitor infrastructure for gaps in security policy and show compliance to industry regulations.

In the past CSPM solutions were perceived as complete CNAPP solutions due to their ability to identify and address “security issues” across cloud environments such as CVE’s and misconfigurations. However, as regulatory requirements have become more stringent, infrastructures more complex, and threats more covert organizations that rely solely on CSPM leave themselves susceptible to attacks, especially those that cannot be detected by agentless scans.

This helps to explain why we can see no clear leader in terms of organizational motivation as to the trigger for purchasing a CSPM solution. It's also important to consider that initial motivation doesn’t always follow through into value. Some companies may onboard a CSPM solution for a specific reason, only to find different benefits or realize their CSPM solution doesn’t check all the boxes they need.

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Triggers, Events or Conditions that Launched the Search for a CSPM Solution



1% Didn't Search

1% I don't know/Not sure

Expanding Cloud Usage: Amplifying Security Challenges

Question 2

How many public, hybrid or private cloud accounts does your company manage?

Today many enterprises are in the middle of their digital transformation. They are moving to the cloud, and most companies have embraced a multi-cloud approach, this often involves a diverse mix of cloud platforms like AWS, Google Cloud, and Azure.

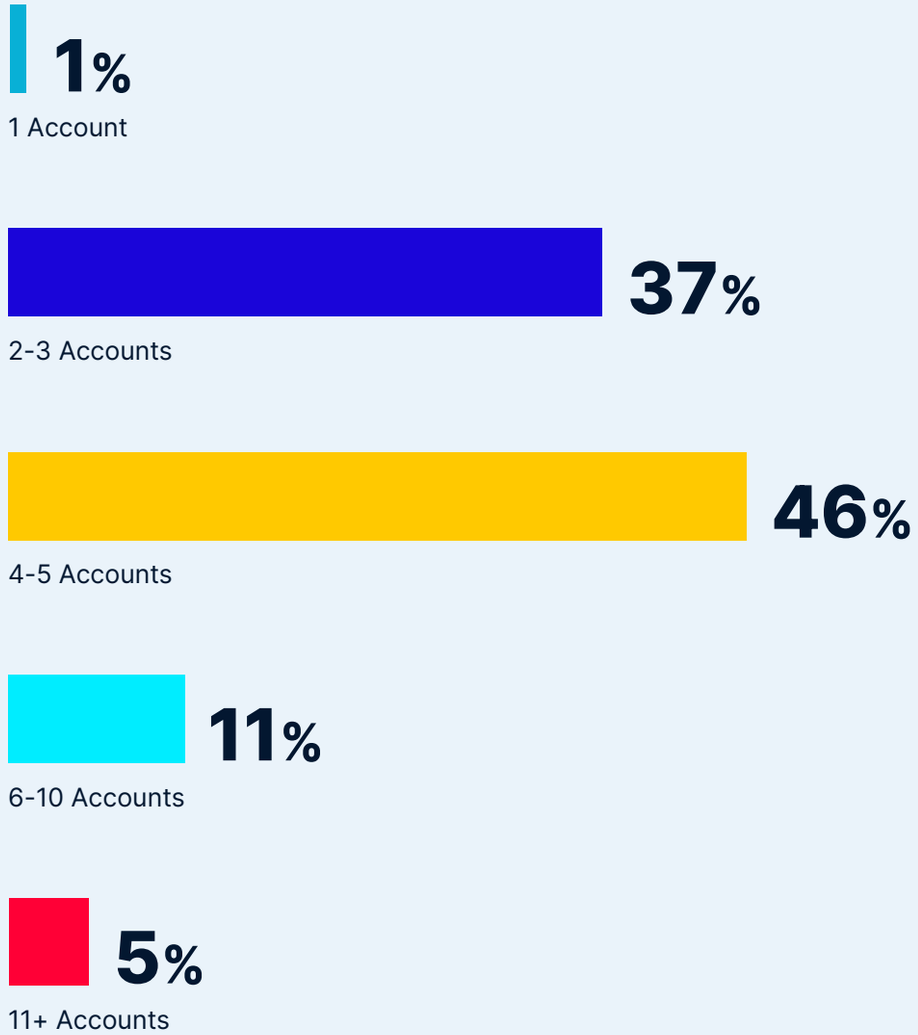
This transformation is evident in the growing number of cloud accounts organizations now manage. The survey showed that **62%** of companies have four or more cloud accounts to monitor, manage and maintain. The breakdown being 46% of respondents claiming 4-5 cloud accounts, 11% with 6-10 accounts, and 5% with 11 or more. As companies increasingly embrace multi-cloud environments, maintaining security throughout the journey is paramount.

More cloud accounts, disparate cloud services in use, and multiple providers equate to more complexity, which makes it harder to manage and secure the environment. In such a diverse and complex reality, with four or more accounts in place, an organization is less likely to know what is happening at any given moment, and therefore more likely to be susceptible to an attack. Especially if these accounts are managed on different platforms, security teams may likely miss something and open themselves up to risk.

This highlights the problem of siloed dev and security teams and the disparate tools within which they operate. If there is no integration, no connection from development to build to runtime, then time and resources are spent chasing alerts, managing false positives, all while an adversary could be silently executing an attack.

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Number of Private, Hybrid or Public Cloud Accounts



Top Factors When Comparing CSPM Solutions

Question 3

What are the 3 most important factors when considering CSPM adoption?

Many people have mistakenly embraced Cloud Security Posture Management (CSPM) as their Cloud Native Application Protection Platform (CNAPP) solution, primarily drawn by the promise of enhanced visibility as a magic solution for all security concerns. However, as the market matures, it's becoming evident that relying solely on CSPM as an "easy" security fix falls short.

Our research looked at the CSPM solutions available today, to what holds the utmost importance for buyers. Our findings revealed that 38% of respondents prioritize "ease of use" in their CSPM solution, a commonly sought-after feature. Following closely behind is the need for speed and agility, 24%, reflecting the ongoing transition of business environments to the cloud.

However, what truly stands out is the equal emphasis placed on visibility and security, each highlighted by 20% of respondents. You cannot stop what you cannot see therefore visibility and security go hand and hand, a connection that requires more than the partial visibility a CSPM solution can provide.

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

The Significance of Visibility in Cloud Environments

Question 4

What are the key components of your CSPM solution (main use cases)?

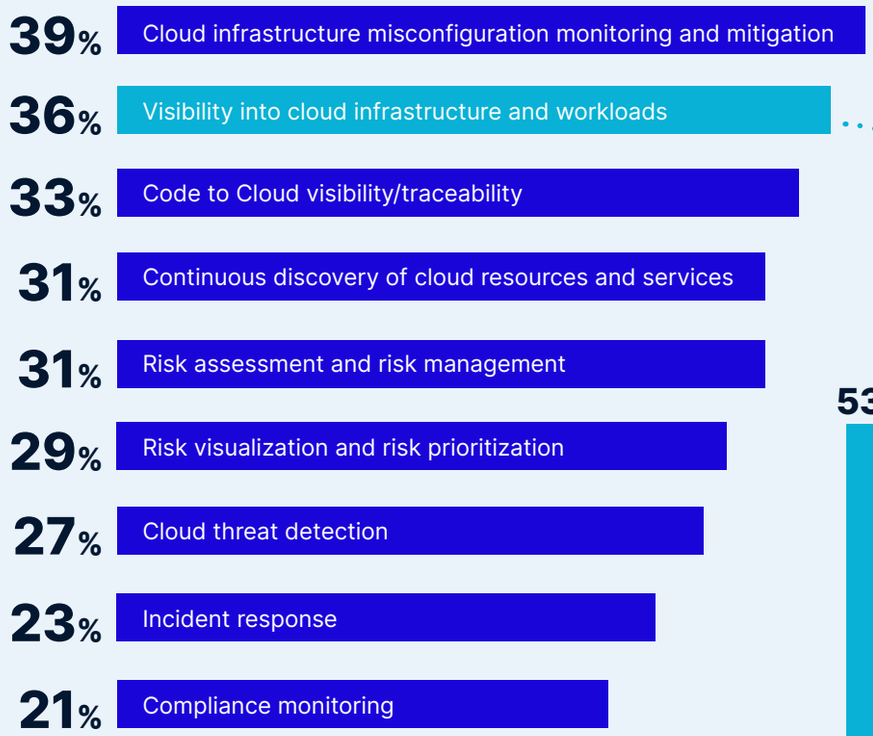
As it is the origin of CSPM, it's easy to see why cloud infrastructure misconfiguration monitoring and mitigation are the most common use cases for existing CSPM solutions today. What was more interesting to see in the survey results was the importance placed on visibility. The second most common use case is visibility into cloud workloads and infrastructure (36%), followed by connecting that visibility to code (33%).

Visibility plays a crucial role in navigating today's intricate cloud environments. However, traditional CSPM solutions focus solely on disk snapshots, leaving blind spots vulnerable to CPU and memory-targeted attacks. Gartner's acknowledgment of the convergence between CWPP and CSPM underscores the evolving landscape of cloud security, stressing the necessity of comprehensive strategies under CNAPP. While CSPM solutions offer visibility into static configurations, they frequently neglect threats in runtime environments, necessitating an extension of visibility to counter dynamic hazards effectively.

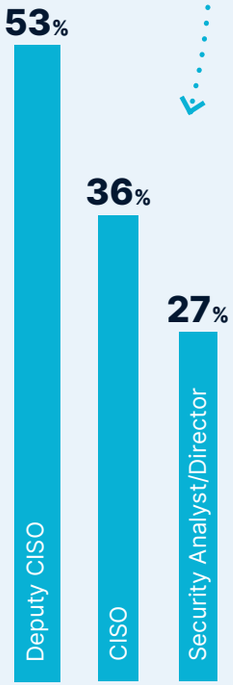
The use of CSPM for visibility by role within the organization also uncovered interesting insights and only highlights the importance of this convergence as more than half of deputy CISOs (53%) use their CSPM solutions for gaining visibility. This makes sense, as the deputy CISO has a practical role, and holds responsibility for setting and executing the strategy, and making sure everything happens according to plan. This relies on visibility as a crucial first step, but if you can't see everything, then you can't accurately prioritize what is critical to your organization.

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

The Main Use Cases of Existing CSPM Solutions



Visibility into cloud infrastructure and workloads, by Role



Cloud Security Must-Haves:
Active Protection & Real-Time Visibility

Question 5

From the following list, which is the most important feature you wish your CSPM solution will provide?

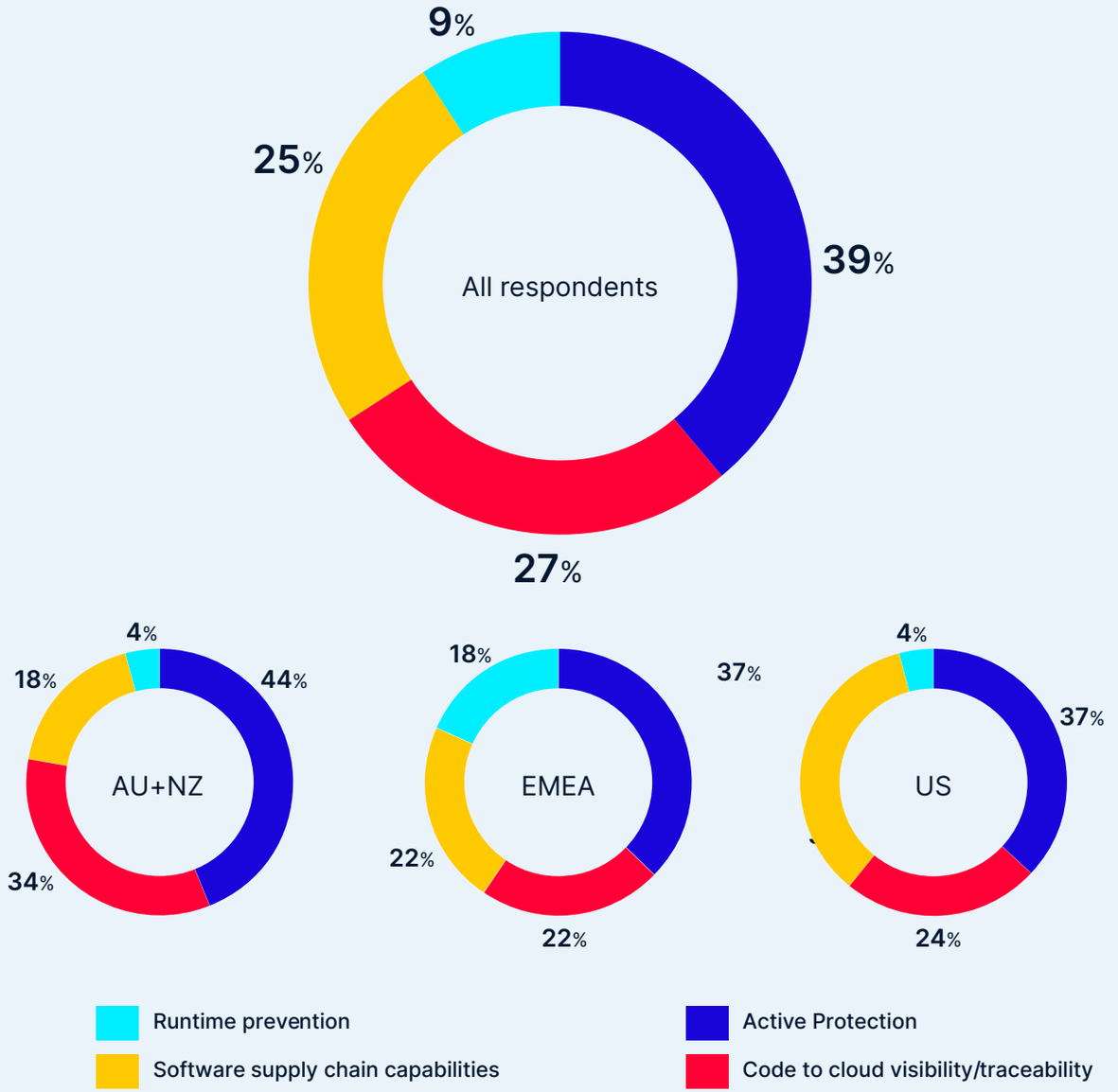
It is here we see this evolution – as organizations seek capabilities beyond CSPM, particularly in the realm of runtime security.

39% of those surveyed said that active protection is critical for cloud native security coming in at the top position, followed by code to cloud visibility or traceability (26%), and software supply chain capabilities (25%). The market demands more than point-in-time visibility and misconfiguration checks, thus making CSPM an insufficient standalone solution for cloud native security. Only an integrated CNAPP can provide active protection and effectively connect the issues found in the cloud back to the line of code. These responses show us that security professionals alike are realizing the importance of shifting left with software supply chain security and further right into proactive runtime protection to stop attacks before they begin.

By breaking down responses between regions, we also uncover significant differences. In the US for example, software supply chain capabilities (US-35%) are almost equal to active protection (US- 37%) as a required feature. This we attribute to the recent focus on the software supply chain because of the SolarWinds and Kaseya attacks and the presidential order 14028 which has placed a heavy focus on strengthening the software supply chain through secure software development practices. As additional compliance mandates are enacted across regions, such as DORA and NIS2 compliance in the EU, we will continue to see the capabilities of CSPM-only solutions as inadequate to meet these mandates.

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Most Important Feature for CSPM Solution to Provide



The Challenges with CSPM (Cloud Security Posture Management)

Question 6

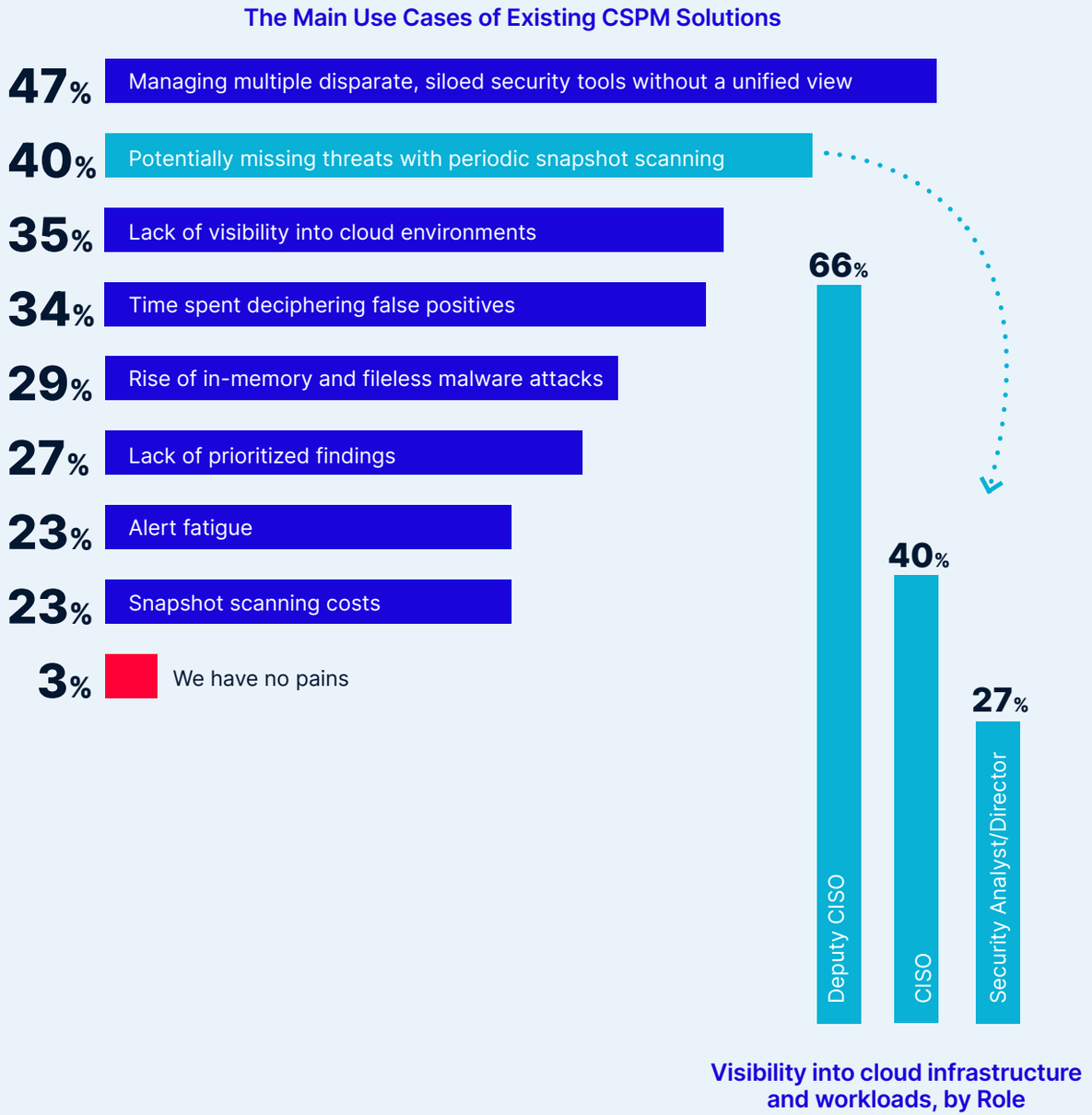
What are your top 3 cloud security risk management pains you would like to solve?

The top three pain points cited by leaders in search of their CSPM solution remain consistent across the survey: managing multiple disparate and siloed security tools without a unified view (47%), potentially missing threats with periodic snapshots (40%), and lack of visibility into cloud environments (35%). However, as cloud infrastructure evolves, once again, visibility stands out as the primary focus for these leaders as they address the security challenges associated with cloud native applications.

Furthermore, with the increasing adoption of hybrid and multi-cloud solutions, another critical pain point emerges – the concern around missing threats due to a lack of real-time visibility across workloads and environments. With 52% of attacks now designed to evade periodic scanning solutions, it's evident why these rank as the second-largest pain point for today's leaders, particularly for those in practical roles such as deputy CISOs.

In this dynamic landscape, having a unified solution that offers real-time visibility across hybrid and multi-cloud environments becomes imperative. Leaders recognize the necessity of consolidating their security tools into a comprehensive CNAPP.

*Question allowed more than one answer and as a result, percentages will add up to more than 100%



Future Focus:
Moving Toward a CNAPP Solution

Question 7

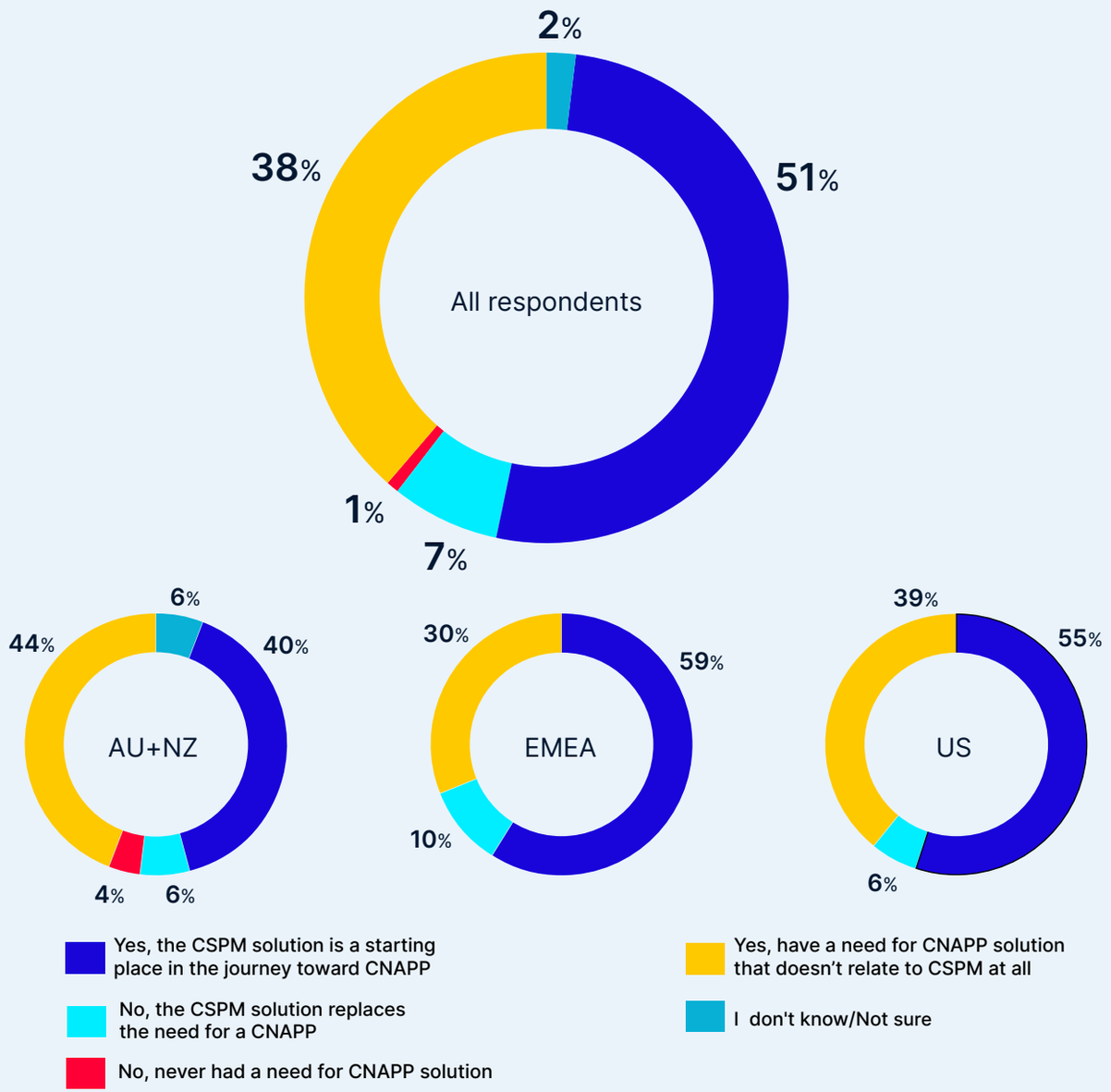
Does your company have a need or plans for moving toward a CNAPP solution?

More than half of security leaders, 51%, view their CSPM solution as a starting point in the journey toward adopting a CNAPP. This sentiment is consistent across different regions and roles, with a slightly higher emphasis in EMEA (59%) and the US (55%). This validates the evolution of the CSPM market. Buyers demand more functionality than a CSPM solution alone in order to meet regulatory compliance and adequately protect their cloud native environments from sophisticated attacks.

The only true way to do this is by integrating CSPM as part of a CNAPP. But buyers beware! While many vendors claim to offer a full CNAPP solution, it's important to make sure that when looking at a CNAPP, it offers an integrated, unified platform that checks all your specific boxes for visibility, monitoring, and prevention, including connecting across all phases of the Software Development Lifecycle (SDLC).

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Future Focus: Moving Toward a CNAPP Solution



CSPM to CNAPP:
Elevating Cloud Security Visibility

The KuppingerCole 2024 Leadership Compass on CNAPP stated, “The distinctive feature of CNAPP solutions is the integration of multiple capabilities that were previously offered as standalone products to address various risks and challenges.” Considering our data and analyst insights, it's evident that CSPM as a standalone strategy falls short in effectively addressing the evolving landscape of cloud native. Rather, the future lies in embracing a more holistic approach encapsulated in CNAPP. CNAPP represents a paradigm shift towards a fully integrated solution that intertwines application security with risk management and fortified cloud infrastructure.

Visibility holds significant importance in cloud security, particularly within CSPM, it plays a role in ensuring the overall security and compliance of cloud infrastructures. Our survey highlights the significant reliance placed by senior managers on CSPM tools to furnish comprehensive insights into an organization's cloud setup enabling real-time monitoring, analysis, and evaluation of security status. These tools facilitate continuous scrutiny of cloud resources, configurations, and activities, shedding light on potential vulnerabilities, misconfigurations, compliance shortfalls, and looming threats within the cloud framework.

Cross-environment visibility proves indispensable for consistently identifying and mitigating security risks across all cloud deployments. It empowers organizations to uphold a unified security stance and swiftly respond to emerging threats or vulnerabilities, regardless of their origins within the cloud structure. The heightened visibility offered by CSPM solutions aids in swiftly pinpointing, prioritizing, and resolving security concerns, thereby bolstering the overall security stance of cloud-based systems. By leveraging detailed visibility, CSPM empowers organizations to maintain vigilant oversight and control over their cloud environments, thus curtailing risks and ensuring adherence to security protocols and compliance standards.

Moreover, the capability to observe across environments facilitates comprehensive risk management, ensuring uniform and thorough application of security measures throughout the entire cloud ecosystem. Comprehensive security, encompassing CSPM, runtime security, image scanning, Infrastructure as Code (IaC) security, supply chain security, and more, is deemed essential for ensuring the full lifecycle security of cloud infrastructures.

In summary, while CSPM has played a crucial role, its efficacy as a standalone strategy is waning. Embracing CNAPP, with its integrated approach and emphasis on visibility and comprehensive security measures, represents the future direction for safeguarding cloud environments effectively.

Methodology

To get insight into the state of cloud native security solutions vs CSPM solutions today, we commissioned a survey of 150 cybersecurity leaders at director level or higher, with respondents split equally between the United States, the United Kingdom/EMEA, and Australia and New Zealand. All respondents work at companies with 35,000 employees or more, across all major industries. We screened for those who influence decisions regarding cloud security budgets.

This report was administered online by Global Surveyz Research, a global research firm. The respondents were recruited through a global B2B research panel, invited via email to complete the survey, with all responses collected during September 2023. The average amount of time spent on the survey was 6 minutes and 59 seconds. The answers to most of the non-numerical questions were randomized to prevent order bias in the answers.

aqua

Aqua Security sees and stops attacks across the entire cloud native application lifecycle in a single, integrated Cloud Native Application Protection Platform (CNAPP). From software supply chain security for developers to cloud security and runtime protection for security teams, Aqua helps customers reduce risk while building the future of their businesses. Founded in 2015, Aqua is headquartered in Boston, MA and Ramat Gan, IL protecting over 500 of the world's largest enterprises. For more information, visit https://www.aquasec.com.

Schedule a demo ›