Cybersecurity
INSIDERS

2024

Cloud Security Report

CHECK POINT™

Introduction

With businesses increasingly reliant on cloud technologies, the security of cloud platforms has escalated into a significant concern that highlights their potential and susceptibility. Traditional security measures often fall short in addressing the dynamic and sophisticated nature of threats faced in cloud settings, making it imperative to shift from a reactive to a preventative stance in security strategies.

This 2024 Cloud Security Report uncovers the pressing concerns and evolving priorities in cloud security. By gathering insights from over 800 cloud and cybersecurity professionals, the survey explores the current state of cloud security, the effectiveness of existing security measures, and the adoption of advanced security solutions, providing a comprehensive view of the challenges and advancements in this critical area.

Key Survey Findings Include:

- **Escalating Security Incidents:** Cloud security incidents are alarmingly on the rise, with 61% of organizations reporting breaches within the last year, marking a significant increase from 24% the year before. This trend underscores the escalating risk landscape in cloud environments.
- **Evolving Breach Types:** Data security breaches have emerged as the most common cloud security incident, reported by 21% of organizations. This shift highlights the evolving nature of threats and the critical need to safeguard sensitive data.
- **Addressing Zero-Day Threats:** Navigating zero-day threats remains a top concern, with 91% of respondents worried about their systems' ability to handle such unknown risks. The survey underscores the need for predictive and immediate defense mechanisms against these sophisticated attacks.
- **Shifting Security Focus:** Despite the rise in incidents, only 21% of organizations prioritize preventive measures aimed at halting attacks before they occur. This indicates a significant prevention gap in current cloud security strategies.
- **Accelerating CNAPP Adoption:** The adoption of Cloud Native Application Protection Platforms (CNAPP) is growing, with 25% of organizations having already implemented CNAPP solutions. This trend reflects a strategic move towards integrating comprehensive security measures that combine prevention, detection, and response capabilities.

We would like to extend our gratitude to Check Point Software Technologies Ltd. for their invaluable contribution to this survey. Their expertise and support have been instrumental in shedding light on the complexities and necessities of modern cloud security.

We hope that the insights derived from this survey will serve as a vital resource for organizations working to enhance the security of your cloud environments.

Thank you,

Holger Schulze

Founder, Cybersecurity Insiders

Cybersecurity INSIDERS

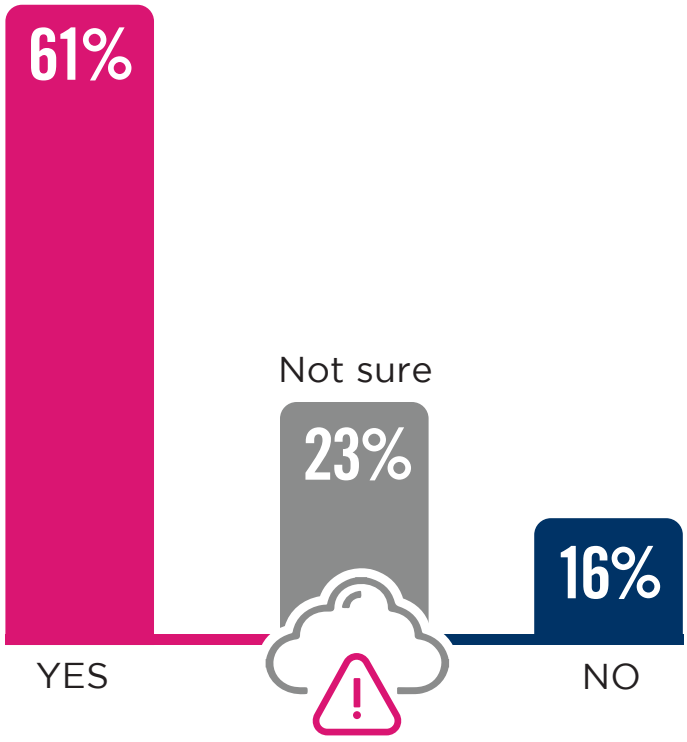
Cloud Security Incidents on the Rise

Understanding the frequency and nature of cloud security incidents is important for grasping the vulnerabilities that persist in cloud environments.

An alarming **61%** of organizations reported experiencing cloud security incidents over the past 12 months, a significant increase from 24% in the previous year. This sharp rise underscores the risks associated with cloud environments and emphasizes the urgent need for enhanced security frameworks that prioritize comprehensive visibility and proactive threat management.

Additionally, the fact that **23%** of respondents were either unsure or unable to disclose details about these incidents suggests a concerning lack of visibility and control over cloud security, which could exacerbate the risk of undetected breaches.

Has your organization experienced any security incidents related to public cloud usage in the last 12 months?



KEY INSIGHTS:

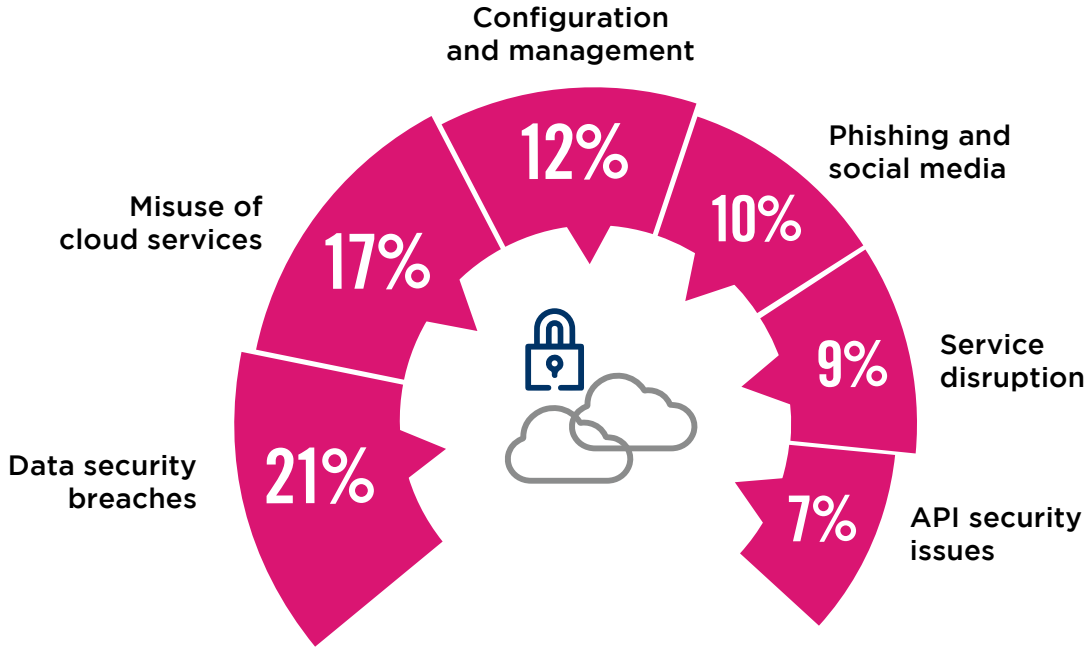
To address these increased incidents and blind spots, organizations should adopt a prevention-first approach, ensuring security measures are proactive rather than reactive. Leveraging advanced, Artificial Intelligence (AI)-supported security solutions can aid in anticipating and mitigating potential threats before they result in significant damage, aligning with an industry-wide shift towards more preemptive security strategies.

Most Common Cloud Security Incidents

Tailoring cybersecurity strategies to the specific types of incidents encountered in cloud environments is critical for effectively addressing prevalent threats, and this is particularly relevant for 2024 and beyond.

In previous years, misconfigurations has been the leading enabler for security incidents and the focus for most organizations. However, this year, we see that data security breaches have taken the number one spot with **21%**. Misuse of cloud services, noted by **17%** of respondents, indicates significant exploitation of cloud resources for malicious purposes, and configuration and management errors, reported by **12%**, moves down a couple of places.

If your organization experienced any security incidents related to public cloud usage in the last 12 months, what type of incident occured?



Additional responses include: Supply chain attacks 6% | Malware-related incidents 5% | User activitiy related 3% | Compliance violations 3% Software vulnerabilities 3% | Other 4%

KEY INSIGHTS:

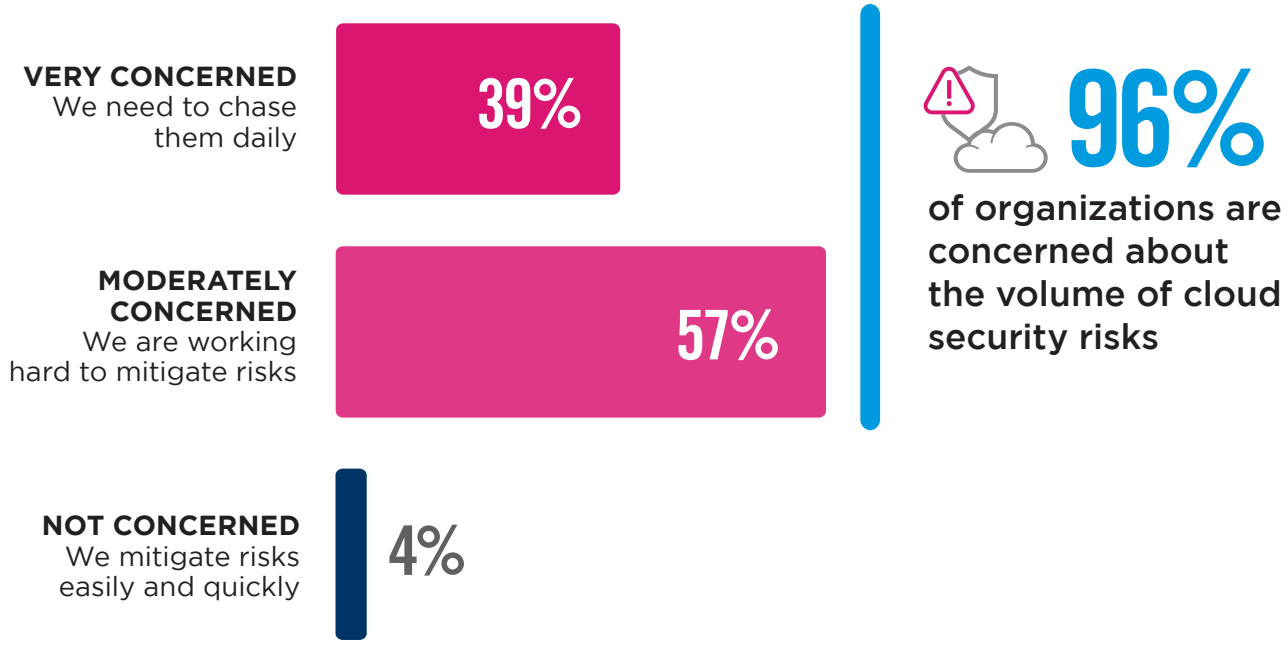
Although Cloud Security Posture Management (CSPM) has become a common security practice for many organizations, aimed at ensuring the implementation of appropriate policies and controls to identify misconfigurations, the rising number of data breaches highlights the necessity of prioritizing the protection of cloud assets that contain sensitive data. Adding security components like Data Security Posture Management (DSPM) offers security teams added visibility as to where sensitive data lives, who has access to it, and how it is being used.

Cloud Security Concerns

Understanding the degree of IT professionals' concerns about cloud security risks helps in assessing the efficacy of current security measures.

An overwhelming **96%** of survey respondents are concerned about their capacity to manage these risks, with **39%** being very concerned, highlighting the significant pressure on scarce resources and underscoring the need for more proactive security solutions.

How concerned are you with the volume of cloud security risks that require mitigation?



KEY INSIGHTS:

Continuous cloud innovation and complexity has taken us to a place where cloud security is managed and implemented by DevOps and developer teams. Over time, many CISO organizations have ceded control over to DevOps, losing visibility and oversight.

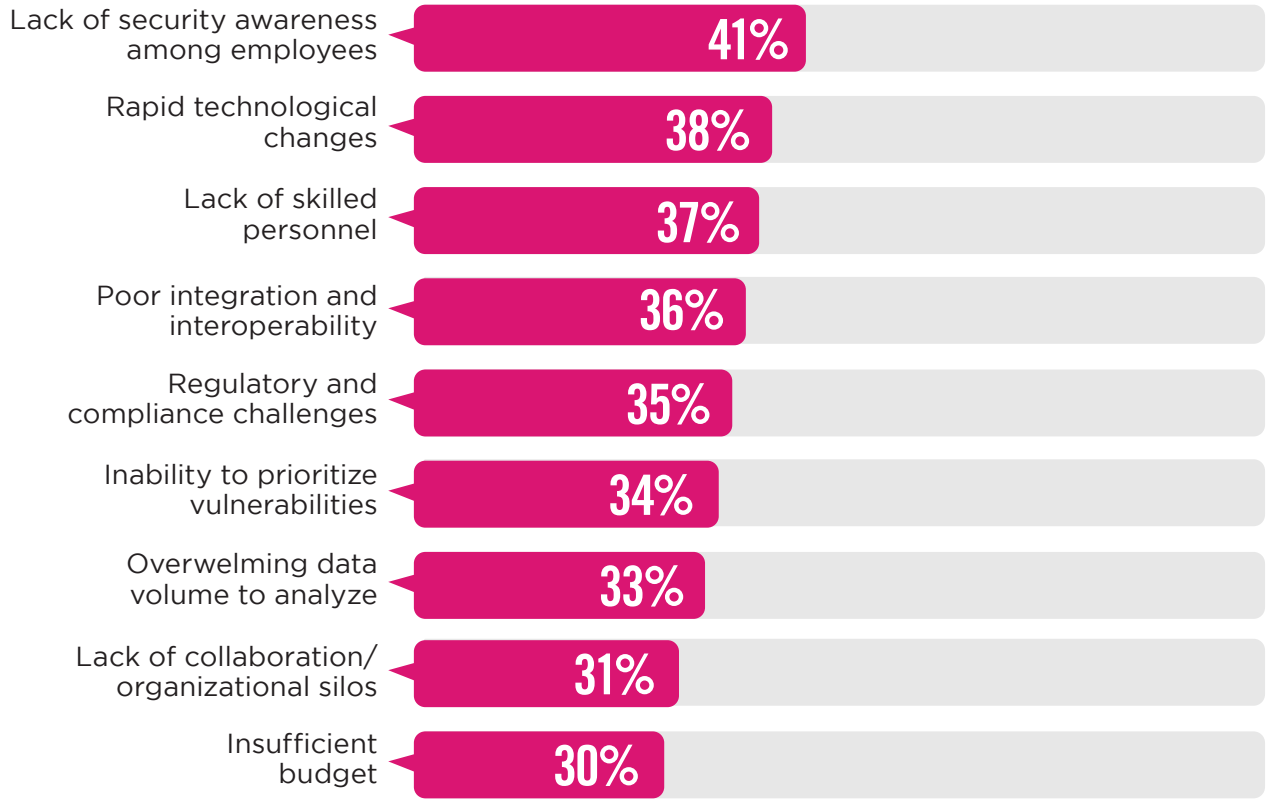
It is time for a paradigm shift that transcends the traditional cycle of detection and remediation so organizations can secure cloud environments without offloading security operations to developers alone.

Barriers to Effective Cyber Defense

Knowing the key obstacles organizations face in defending against cyberthreats is necessary for refining cybersecurity strategies and resource allocation. The most significant barrier, reported by **41%** of respondents, is the lack of security awareness among current employees, emphasizing the need for comprehensive training programs that enhance security knowledge across all organizational levels. Rapid technological changes and the lack of skilled personnel, noted by **38%** and **37%** respectively, underscore the difficulty in keeping pace with evolving threats and the technology designed to combat them.

Additionally, **36%** of participants identified poor integration and interoperability between security solutions as a major challenge, indicating that a cohesive security environment could significantly enhance defensive capabilities.

Which of the following barriers inhibit your organization from adequately defending against cyberthreats?



Additional responses include: Difficulty justiying additional investment 29% | Inadequate contextual information from security tools 28% | Supply chain vulnerabilities 26% | Lack of management support 24% | Underinvestment in effective solutions 23% | Not sure/other 13%

KEY INSIGHTS:

To overcome these barriers, organizations should consider advanced training and development of existing staff to close the skills gap. In addition consulting services can also further assist with integrating security solutions across their various tools and platforms and free up constrained resources.

Cybersecurity Talent Shortage

Digging deeper on employee resource constraints, we find that not only are organizations struggling with keeping current cybersecurity skills sharpened, but the survey findings highlight the challenge many organizations face in recruiting new cybersecurity expertise with a significant **76%** of respondents reporting a shortage of skilled cybersecurity professionals.

This substantial figure underscores the widespread issue in the industry where the demand for cybersecurity talent far exceeds the supply for years to come, potentially leaving critical security functions understaffed and vulnerabilities unaddressed.

Is your organization currently facing a shortage of cybersecurity talent?

KEY INSIGHTS:

Organizations can supplement these deficiencies and grow their team's expertise by investing in a Managed Cloud Native Application Protection Platform (CNAPP). This approach helps offset shortages and fill knowledge gaps by providing seamless integration with an organization's IT and InfoSec operations for better monitoring, configurations, policy tuning, incident management, troubleshooting, and more.

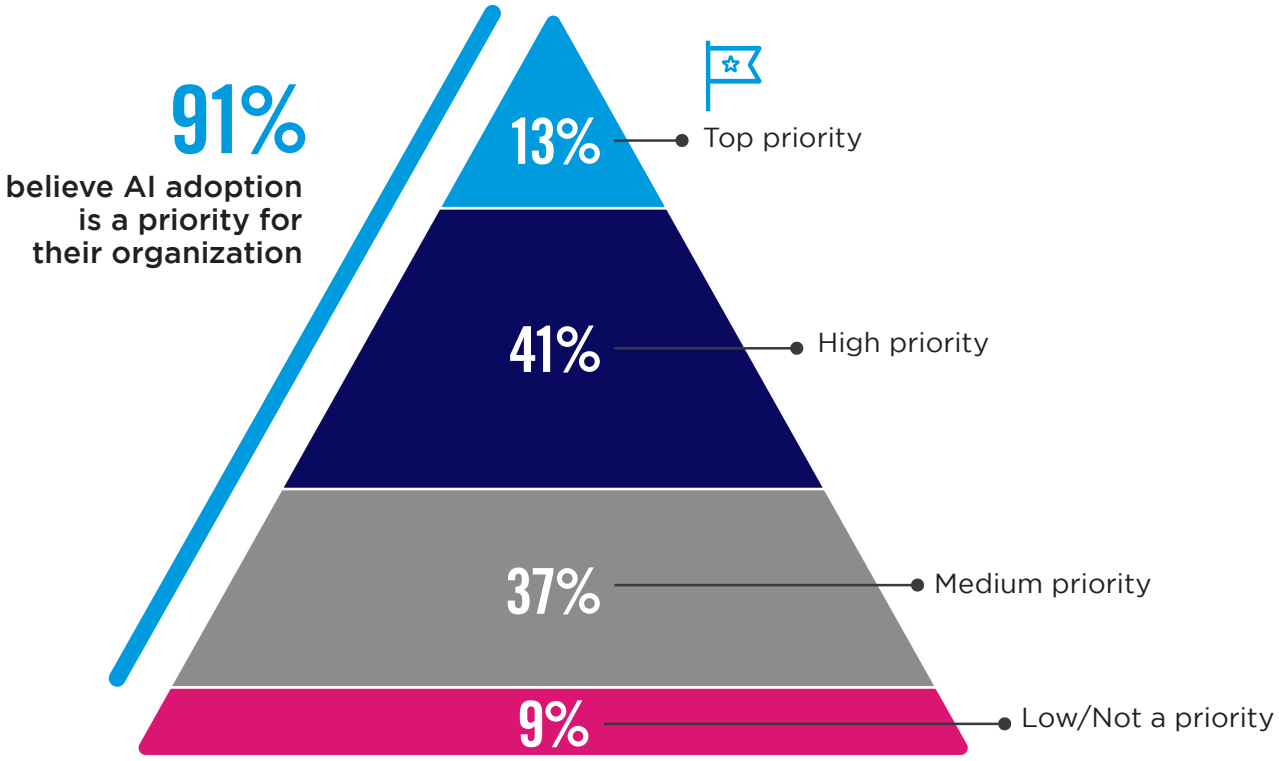
Additionally, integrating advanced security solutions that leverage AI and automation can compensate for the shortage of human resources. These technologies can perform routine security tasks and analyze large volumes of security data more efficiently than human teams, allowing existing staff to focus on more strategic, high-impact security initiatives.

AI Priority in Cybersecurity

The integration of artificial intelligence (AI) into cybersecurity strategies is a telling indicator of how organizations perceive the role of advanced technologies in enhancing their security posture.

A majority of respondents **(91%)** consider AI a priority, illustrating a significant lean towards adopting AI-driven solutions within their cybersecurity strategies. This substantial focus underscores the growing reliance on AI to augment security measures, driven by AI's capability to analyze large data sets rapidly, detect anomalies, and predict potential threats with a level of precision and speed unattainable by human analysts alone.

How does AI adoption rank among your organization's cybersecurity priorities?



KEY INSIGHTS:

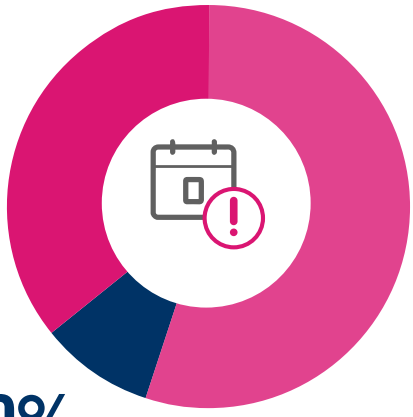
Organizations should consider elevating AI's role within their cybersecurity strategies, particularly by leveraging AI-powered tools like proactive web application firewalls and advanced network security systems. These AI-enhanced tools can dramatically improve the detection and prevention of sophisticated cyber threats, especially zero-day attacks, by continuously learning and adapting to new threats.

Navigating Zero-Day Threats

Rapid technological advancements have increased cybercriminals' capabilities to create more sophisticated attacks.

Almost all respondents (**91%**) are concerned about their security systems' ability to manage zero-day attacks and unknown risks, pointing to a significant gap in current security measures that do not adequately prevent or mitigate these attacks before they cause harm.

How concerned are you about unknown risks and zero-day attacks such as Log4j / Log4Shell?



36%
VERY CONCERNED
We don't believe that our security measures will be able to handle these attacks

55%
MODERATELY CONCERNED
We have the right security measures in place

9%
NOT CONCERNED
We have strong security capabilities in place that have prevented previous attacks

KEY INSIGHTS:

A modern WAF, especially one that utilizes AI to provide immediate and predictive protections without reliance on signatures, can serve as a critical first line of defense at the cloud's 'front door', blocking malicious attempts before they penetrate deeper into the network. Coupling this with an advanced network security solution that offers deep packet inspection and real-time threat detection across all access points can greatly reduce the vulnerability of cloud environments to zero-day exploits.

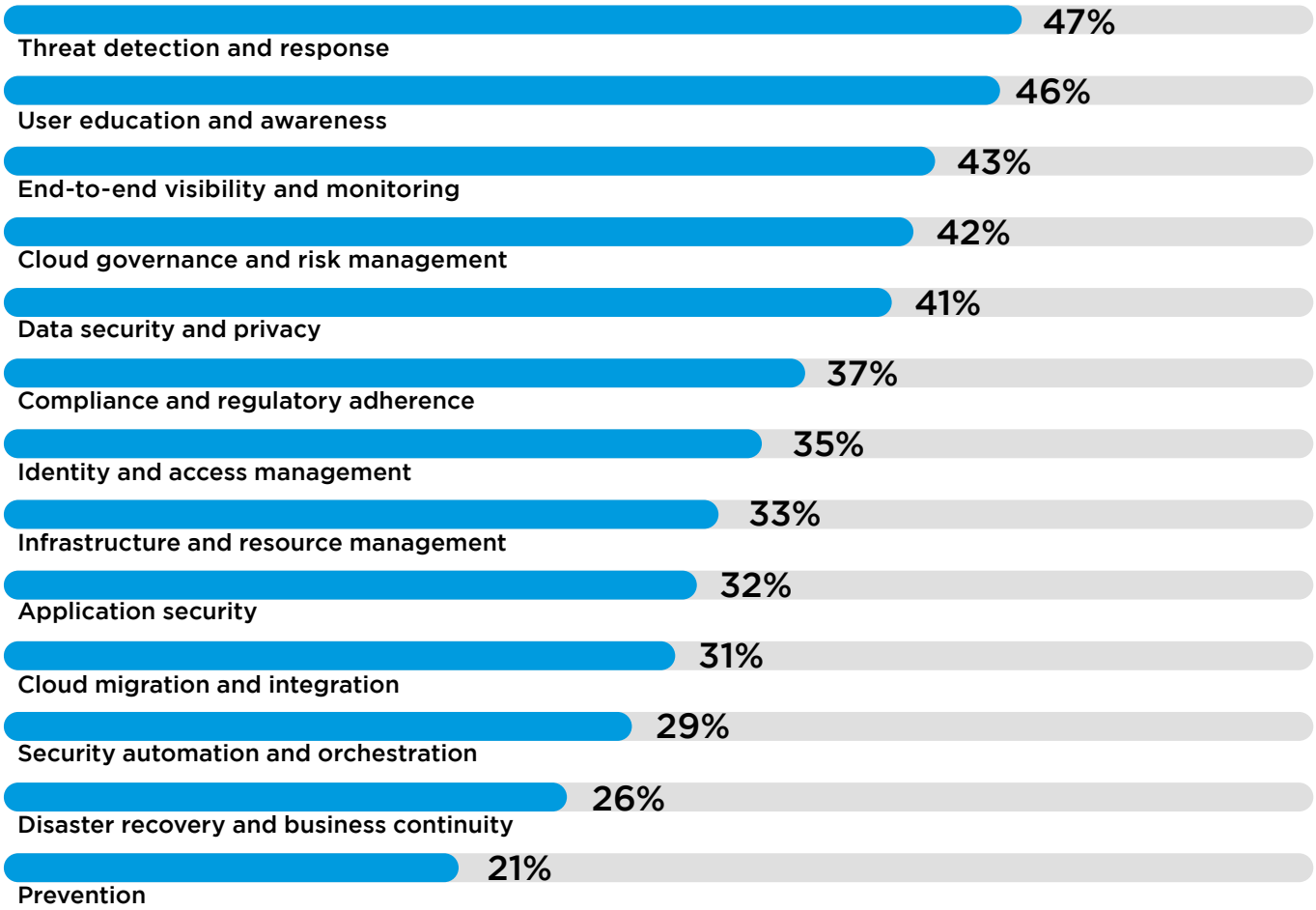
These technologies, when integrated within a seamless security architecture, ensure a robust defense mechanism that not only detects but also prevents attacks, maintaining the integrity and resilience of cloud infrastructures against the most unpredictable threats.

Evolving Priorities in Cloud Security

As organizations navigate the complexities of cloud security amidst rising security incidents and data breaches, the survey reveals a concentrated focus on threat detection and response, with **47%** of respondents emphasizing this as a priority. This approach reflects a traditional, reactive stance that rests solely on identifying and mitigating threats as they occur.

Interestingly, despite the increasing sophistication of cyber threats, only **21%** of organizations prioritize prevention strategies aimed at stopping attacks before they happen.

What are your top cloud security priorities?



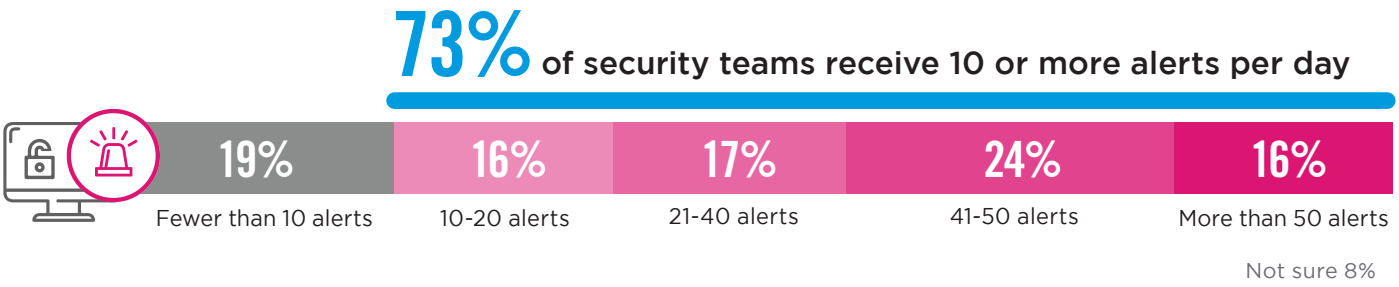
KEY INSIGHTS:

This prevention gap highlights a critical and common oversight in current security efforts—while threat detection and monitoring are essential, they often rely on recognizing known vulnerabilities and patterns of malicious behavior. Such methods fall short against novel threats, particularly zero-day attacks, which exploit previously unknown vulnerabilities, and therefore cannot be detected using conventional security tools. A more balanced strategy incorporates robust prevention mechanisms to strengthen overall security by reducing dependency on after-the-fact mitigation once an attack has already taken place.

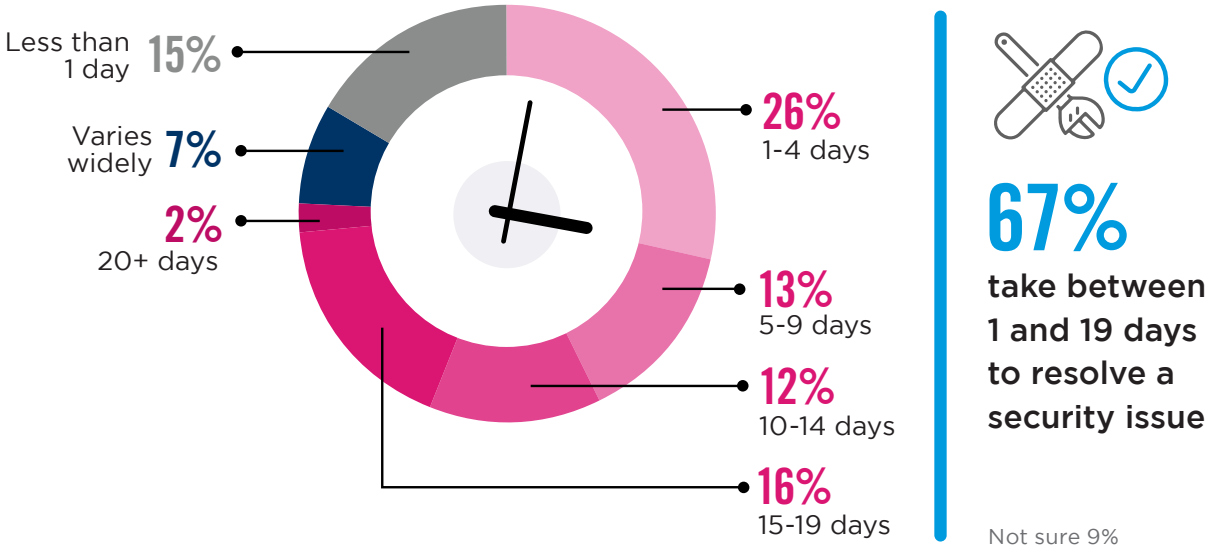
Slowness in Security Response

The survey confirms one of the biggest challenges faced by cybersecurity operations: an overwhelming volume of daily security alerts. Notably, **40%** of organizations receive over 40 alerts each day. This situation not only strains SOC analyst resources but also lengthens the time required to resolve each alert, with **43%** reporting resolution times exceeding five days. This deluge of alerts can exhaust teams and increase vulnerability due to delayed responses to potentially critical threats.

How many security alerts does your security team receive on an average day?



How long does it typically take your team to resolve a security issue?



KEY INSIGHTS:

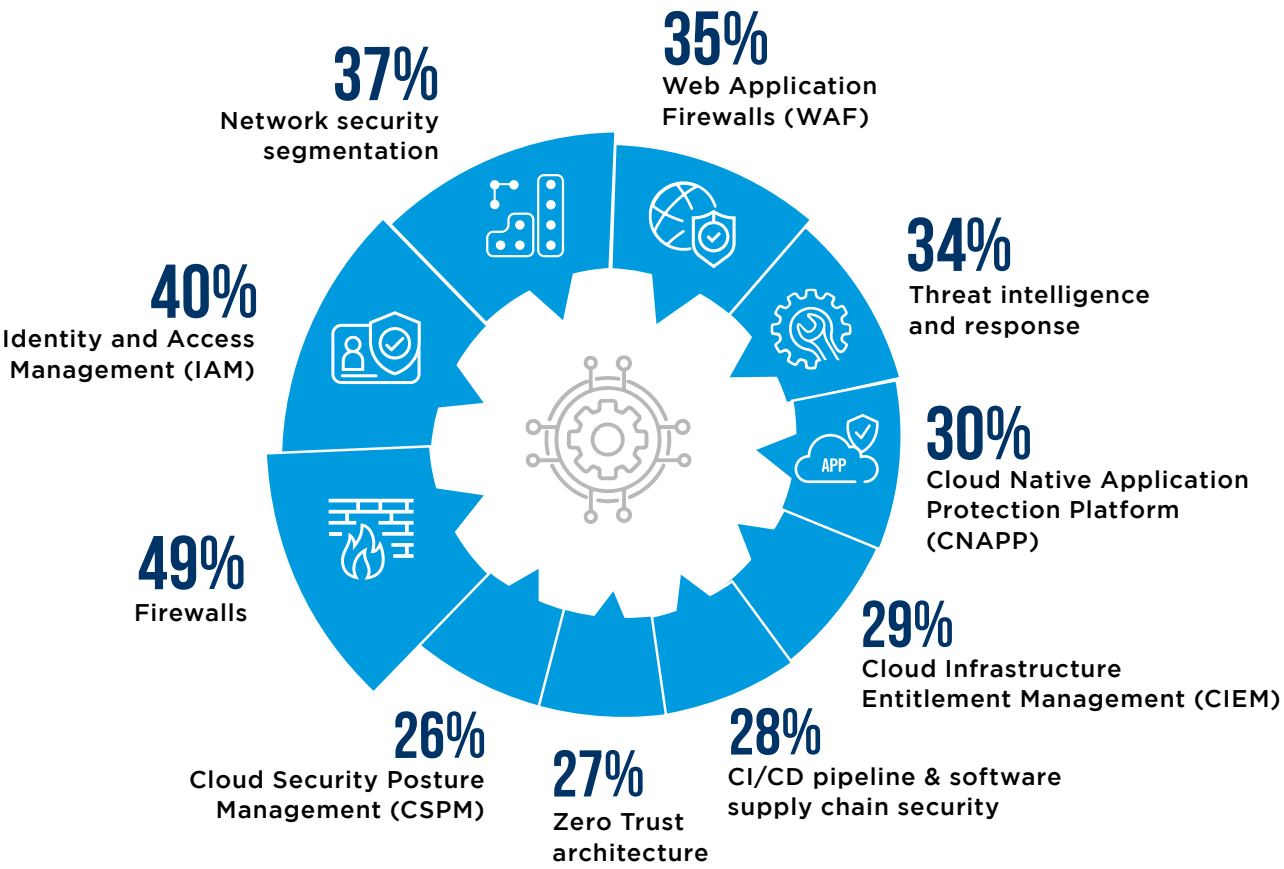
It is common for organizations to identify millions of potential issues upon scanning their cloud environment— most are not harmful unless malicious actors can exploit them. To combat this challenge, vendors have implemented 'attack graphs' to group and correlate static misconfigurations and vulnerabilities to better prioritize alerts. However, prioritization is not enough, as teams may still be ignoring alerts below the attention threshold. This false sense of confidence can be detrimental. By focusing on preventing attacks before they occur, organizations can significantly reduce the volume of alerts generated that would otherwise be considered high risk. This shift not only frees up valuable resources but also enhances the organization's ability to thoroughly investigate and manage true risks that would otherwise pose significant threats.

Navigating Cybersecurity Tool Fragmentation

The survey reveals significant fragmentation of the security platforms and tools organizations deploy to manage their cloud infrastructures. Firewalls lead as the primary defensive measure (**49%**), reflecting their critical role in network security. However, only **37%** have effectively implemented segmentation strategies. This oversight can be particularly detrimental, as insufficient segmentation can allow attackers to exploit vulnerabilities, which allows them to gain access to broader parts of the network, causing extensive damage.

The use of WAF by **35%** of respondents, along with Cloud Security Posture Management (CSPM) at **26%**, points to a layered approach to security that addresses both network defense and application-level vulnerabilities, and everything in between.

What are your organization's primary measures and controls to manage your entire cloud infrastructure?



Additional responses include: Kubernetes Security Posture Management (KSPM) 26% | Cloud Workload Protection Platform (CWPP) 25% | Content Disarm and Reconstruction (CDR) 12%

Cloud Policy Sprawl

While we are witnessing a noticeable rise in the comprehension and utilization of various cloud security components, the increasing number of security solutions—highlighted by **43%** employing seven or more tools to configure policies alone—indicates a complex and highly inefficient security landscape.

How many separate security solutions are required to configure the policies securing your enterprise's entire cloud footprint?

83%

have to access 4 or more dashboards to configure their enterprise's cloud policies

KEY INSIGHTS:

Consolidating security measures into a highly integrated platform that can offer comprehensive coverage without the need for multiple, disjointed tools is the way forward.

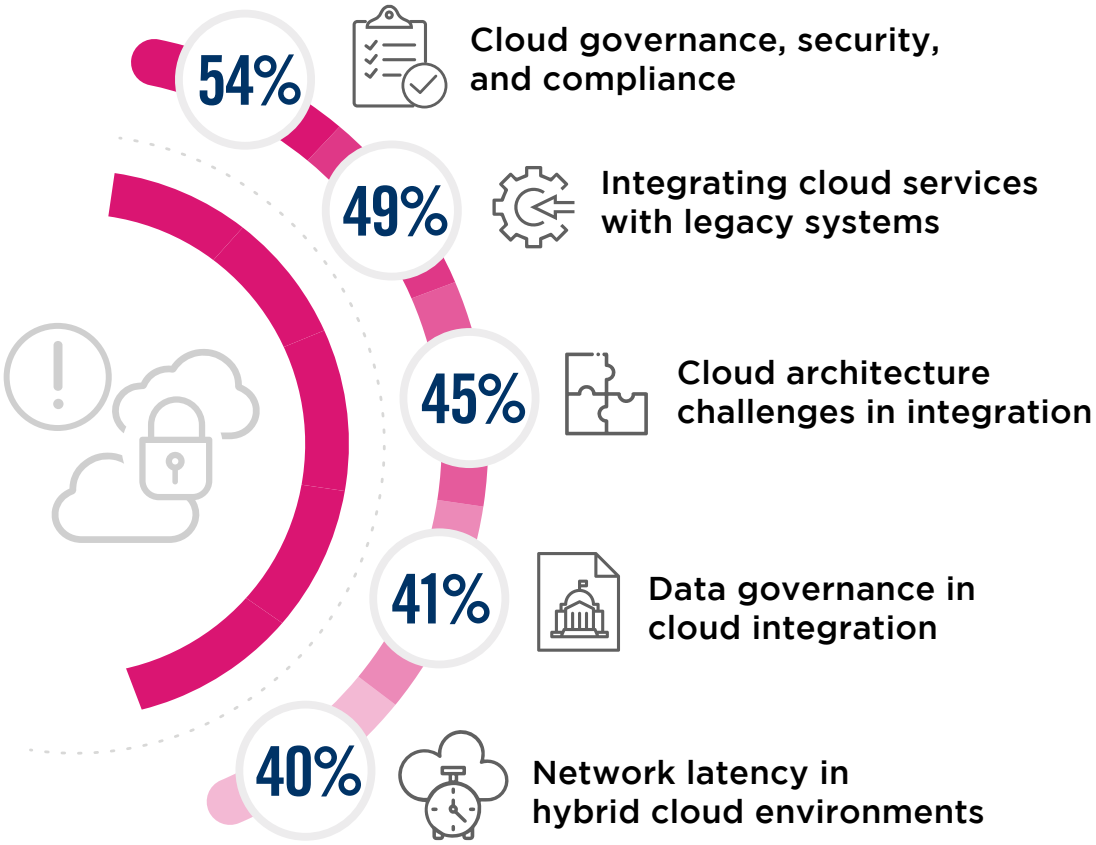
By streamlining broader capabilities like WAF, network segmentation, cloud detection and response, and CNAPP under a single umbrella, companies can enhance their security efficacy while simplifying the administrative burden.

Cloud Integration Challenges

If the majority of security issues organizations face can be alleviated through a more streamlined solution, why does the number of tools and policies continue to rise every year? The survey illuminates the pains organizations face when trying to better integrate cloud security.

The complexity of maintaining consistent regulatory standards in hybrid or multi-cloud architectures becomes apparent, as **54%** of respondents grapple with ensuring compliance and cloud governance across diverse environments. Additionally, nearly half (**49%**) struggle with integrating cloud services into aging legacy systems, a task complicated by scarce IT resources which can hinder effective and secure integration.

What cloud integration challenges do you face?

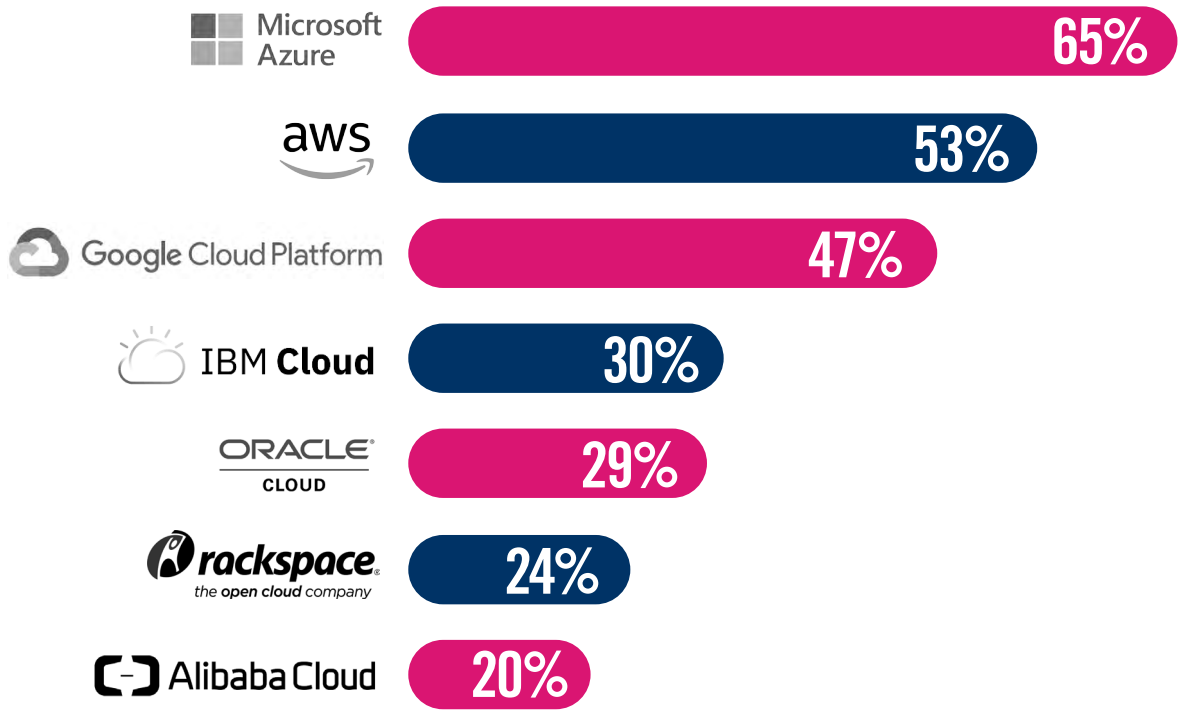


Additional responses include: Deciding between custom and pre-built integrations 39% | Issues stemming from cloud integration anti-patterns 29% Vendor lock-in concerns 27%

Cloud Providers

When we talk about integration challenges, it's important to note that a majority of organizations are also managing multiple cloud IaaS providers within their security landscape. The survey shows that Microsoft Azure leads the market with **65%** of surveyed organizations deploying their cloud services, followed by Amazon Web Services (AWS) (**53%**) and Google Cloud (**47%**).

What cloud IaaS provider(s) do you currently use or plan to use in the future?



KEY INSIGHTS:

Cloud native solutions often lack uniformity across cloud services, including on-premises data centers, leading to disparate policies and complicating security oversight. Look for a network security solution that is tightly integrated with the WAN networking infrastructure of various cloud security providers, enabling rules to be applied universally across different cloud environments.

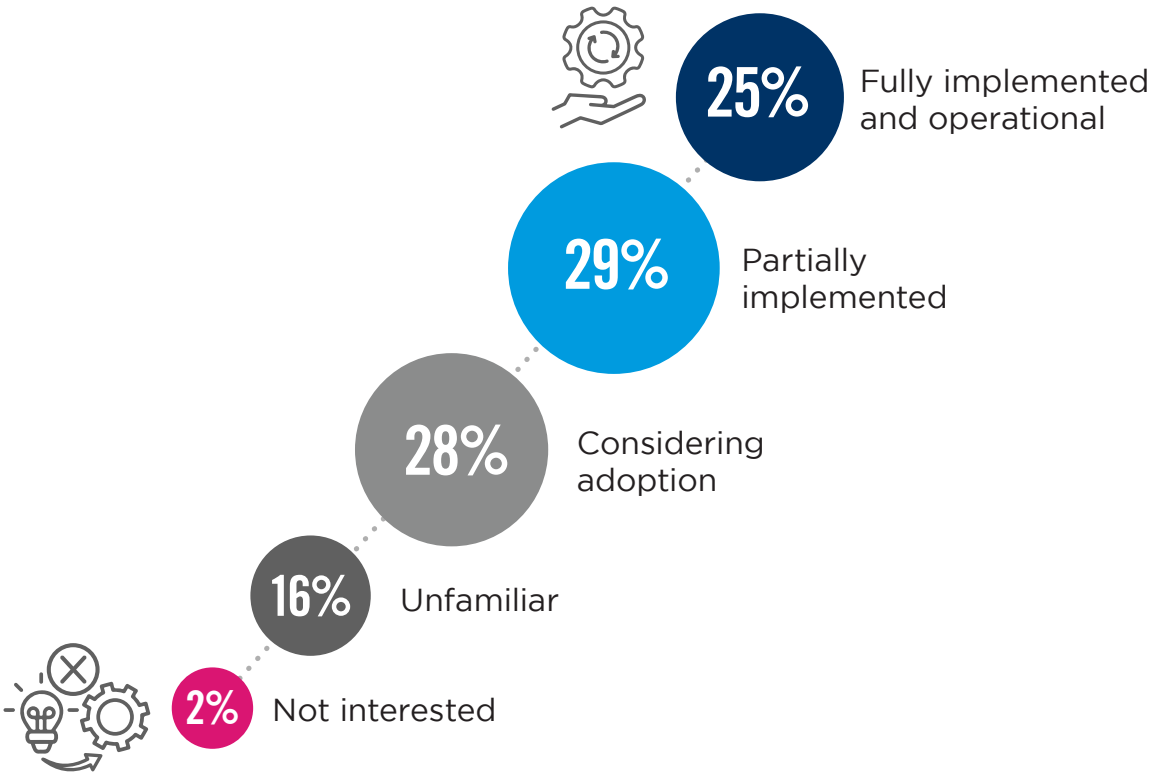
By incorporating WAF as a service with API schema discovery, organizations can further streamline the process for on-premises deployments. Leading vendors provide this level of advanced security within a CNAPP to ensure ease of integration and full coverage.

Rapid CNAPP + Prevention Adoption

A CNAPP should be the cornerstone of any cloud security strategy, as it unifies Cloud Security Posture Management (CSPM), Cloud Workload Protection (CWP), Cloud Infrastructure Entitlement Management (CIEM), Cloud Detection and Response (CDR), and code security, making it much easier to automate processes and reduce manual inefficiencies.

The survey reveals a promising trend towards the adoption of CNAPP: **25%** of organizations have already fully implemented a comprehensive CNAPP solution, indicating a strong commitment to advanced cloud security practices. Another **29%** are in the process of integrating CNAPP into their systems, showing that a majority of respondents recognize the benefits of such platforms.

What is your organization's current stage of CNAPP (Cloud Native Application Protection Platform) adoption?



KEY INSIGHTS:

Not all CNAPPs are created equal. Be sure that you invest in a platform that provides those preventative components that can only be found by integrating WAF and network security. Most solutions on the market overlook this important integration and, as a result, are creating too many alerts and risk factors.

Enhancing CNAPP systems with additional components that emphasize prevention over remediation can fortify cloud infrastructures.

Proactive Cloud Defense Strategies

As cloud threats become increasingly frequent and sophisticated, it is vital for organizations to shift from traditional reactive security measures to a prevention-first approach by leveraging the following cloud security framework.

Employ AI-Powered WAF for Zero-Day Protection:
With 91% concerned about zero-day attacks, employing an AI-powered Web Application Firewall is critical. These WAFs intelligently counteract web threats, including zero-day exploits, without relying on signature-based detection, offering immediate protection that aligns with modern attack vectors.

Deploy Advanced Network Security:
Consider advanced network security solutions that scale with your cloud infrastructure. This solution should support seamless integration and provide comprehensive protection, facilitating both macro and micro-segmentation and unified policy management across cloud platforms.

Adopt a Prevention-First Approach:
With a significant focus on threat detection (47%), adopting a prevention-first CNAPP can shift the approach from reactive to proactive. This platform minimizes alerts and incorporates preventative measures, significantly reducing the volume of risks needing attention by scarce security analysts.

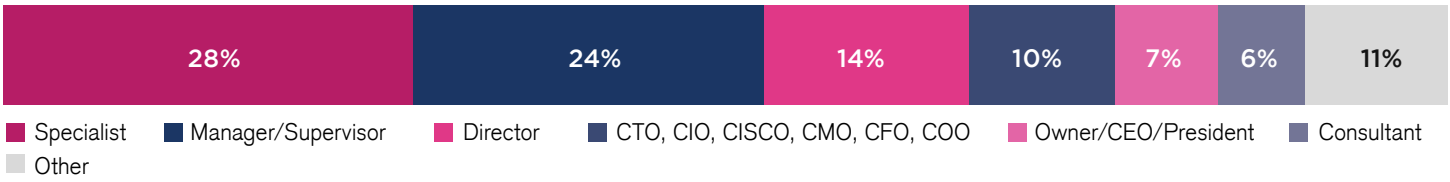
Leverage Comprehensive CNAPP Features:
To manage the complexity highlighted by 43% using seven or more tools to configure policies, a sophisticated CNAPP with extensive features like Cloud Workload Protection, Cloud Detection and Response, Code Security, and Cloud Security Posture Management should be employed. These features help streamline security processes and enhance the management of cloud environments.

Incorporate AI Technologies:
With 91% of organizations now prioritizing AI to enhance their security posture, the focus has shifted towards leveraging AI for proactive threat prevention and enhancing employee deficits.

Methodology & Demographics

The 2024 Cloud Security Report is based on an in-depth survey of 813 cybersecurity professionals conducted in April 2024. This research provides insights and trends in cloud security management, highlighting the threats and pressing challenges organizations face while providing guidance for enhancing cloud security posture. Participants span various roles, from technical and business executives to hands-on IT security practitioners, representing a balanced mix of organizations of different sizes across various industries.

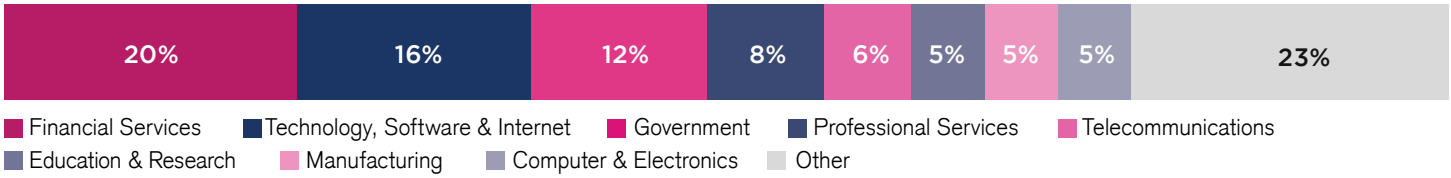
CAREER LEVEL



DEPARTMENT

COMPANY SIZE

INDUSTRY



Check Point Software Technologies Ltd. is a leading AI-powered, cloud-delivered cyber security platform provider protecting over 100,000 organizations worldwide. Check Point leverages the power of AI everywhere to enhance cyber security efficiency and accuracy through its Infinity Platform, with industry-leading catch rates enabling proactive threat anticipation and smarter, faster response times. The comprehensive platform includes cloud-delivered technologies consisting of Check Point Harmony to secure the workspace, Check Point CloudGuard to secure the cloud, Check Point Quantum to secure the network, and Check Point Infinity Core Services for collaborative security operations and services.

www.checkpoint.com

Cybersecurity
INSIDERS

Cybersecurity Insiders brings together 600,000+ IT security professionals and world-class technology vendors to facilitate smart problem-solving and collaboration in tackling today's most critical cybersecurity challenges.

Our approach focuses on creating and curating unique content that educates and informs cybersecurity professionals about the latest cybersecurity trends, solutions, and best practices. From comprehensive research studies and unbiased product reviews to practical e-guides, engaging webinars, and educational articles - we are committed to providing resources that provide evidence-based answers to today's complex cybersecurity challenges.

Contact us today to learn how Cybersecurity Insiders can help you stand out in a crowded market and boost demand, brand visibility, and thought leadership presence.

Email us at info@cybersecurity-insiders.com or visit cybersecurity-insiders.com