

THE NEXT ERA OF CLOUD SECURITY:

Cloud-Native Application Protection Platform and Beyond



Philip Bues
Senior Research Manager,
Cloud Security, IDC



THIS PDF USES
HYPERLINKS

Table of Contents



CLICK ANY HEADING TO NAVIGATE
DIRECTLY TO THAT PAGE.

Introduction	3
In This White Paper	4
Situation Overview	6
CNAPP: A Top 3 Security Investment Priority for 2025 and Beyond	6
Evolving Role of the CISO	8
Need for End-to-End Visibility and Tool Consolidation	9
Why CNAPP Must Be Part of the SecOps Platform	11
Unique Benefits of GenAI-Powered CNAPP	14
Essential Guidance	16
Challenges/Opportunities	17
Conclusion	18
About the IDC Analyst	19
Message from the Sponsor	20



On average, in 2024, organizations experienced **more than nine cloud security incidents.**

89% reported a **year-over-year increase in cloud security incidents,** according to IDC.



In response to cloud security challenges, organizations are prioritizing cloud-native application protection platforms (CNAPP) as one of their top three security investments for 2025.

In This White Paper



IDC's research indicates that the CNAPP market will grow significantly, with a forecasted **CAGR of 23% through 2028.**

IDC research highlights that the proliferation of cloud services and the increasing sophistication of cyberthreats exacerbate the complexity of managing cloud security. The integration of advanced technologies such as adversarial AI by cybercriminals complicates the security landscape, making it imperative for organizations to adopt comprehensive and integrated security solutions.

According to IDC, on average, organizations experienced more than nine cloud security incidents in 2024, with 89% reporting a year-over-year increase in such incidents. This increase in security incidents has led to significant concerns among chief information security officers (CISOs), who are under mounting pressure to report on their digital resiliency.

In response to these challenges, organizations are prioritizing CNAPP as one of their top three security investments for 2025. These investments aim to enhance security measures and improve the overall security posture of organizations. IDC's research indicates that the CNAPP market will grow significantly, with a forecasted CAGR of 23% through 2028. The need for visibility, risk management, and compliance across cloud infrastructures is driving this growth. The integration of CNAPP with other security solutions, such as extended detection and response (XDR) and security information and event management (SIEM), is crucial for providing a unified security platform that can effectively address the complexities of modern cloud environments.

As the role of the CISO evolves and the need for end-to-end visibility and tools consolidation proliferates, IDC sees congruent mutually beneficial trends leading to greater investment in integrated, unified security operations (SecOps) platforms with CNAPP as the anchor owing to several factors, including lowering mean time to detect (MTTD) and mean time to respond (MTTR), cost management, unification of security data, assets, entities, and easier deployment of AI.

The evolving threat landscape and the increasing number of cloud security incidents underscore the importance of integrated security solutions. CISOs must prioritize investments in managed services, CNAPP, and XDR/SIEM systems to enhance their organization's security posture. End-to-end visibility and tool consolidation are critical for managing costs and improving efficiency. By adopting CNAPP as part of an integrated SecOps platform, organizations can achieve a unified security approach that addresses the complexities of modern cloud environments.

This paper provides essential guidance for organizations looking to combat the rising tide of sophisticated cyberthreats and ensure a resilient and cost-effective cloud security posture for their organization.

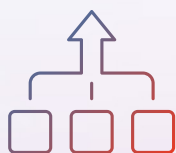
This paper references IDC's *U.S. 2025 CNAPP Survey* (hereafter known as "*IDC CNAPP Survey*"), conducted in March 2025, throughout the study.

Responses are from 300 organizations across major industry verticals and varying organization sizes. The solution section features Microsoft Defender for Cloud, a CNAPP solution.

Key Themes:



Visibility



Consolidation



Platformization



Accountability

Situation Overview

In the evolving landscape of cybersecurity, cross-domain attacks have emerged as a significant threat, leveraging the interconnected nature of modern IT environments to exploit vulnerabilities across different domains. These attacks, which could come in the form of fileless, living off the land, or ransomware, can traverse multiple security domains, such as networks, applications, and cloud environments, to achieve their malicious objectives. The complexity and sophistication of cross-domain attacks make them particularly challenging to detect and mitigate, posing a substantial risk to organizations of all sizes.

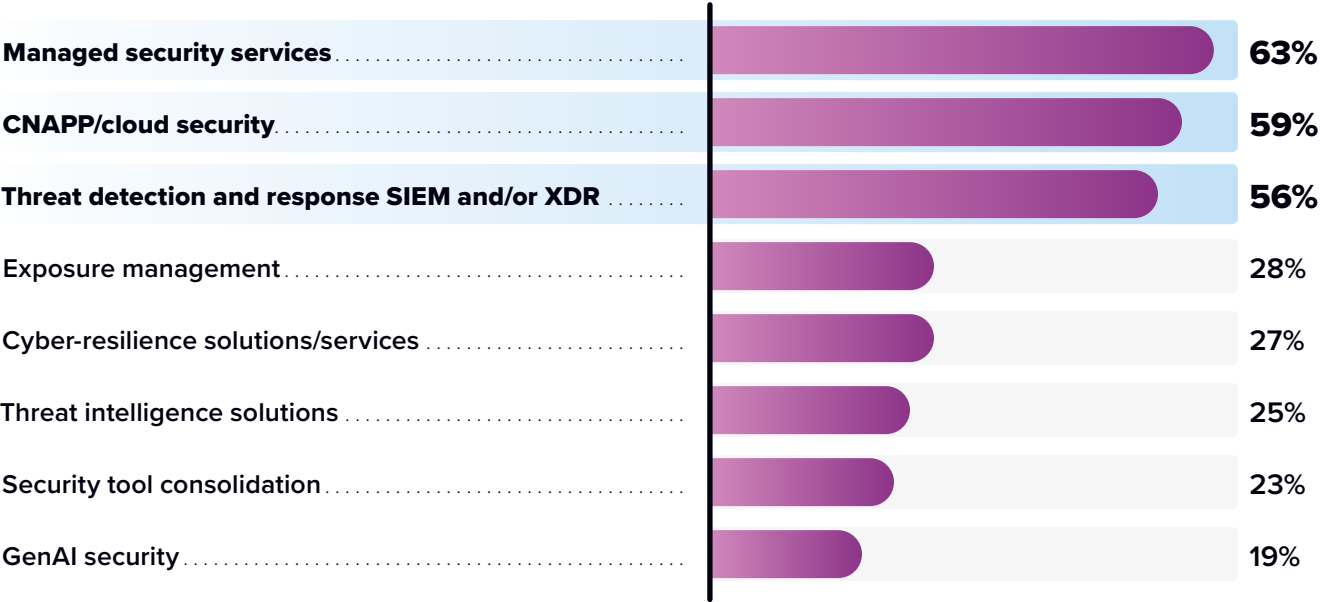
For instance, an attacker might compromise a web application to gain access to the underlying network infrastructure or, more commonly, compromise credentials to move laterally across different systems, escalate privileges, then encrypt and possibly exfiltrate data. These attacks often employ advanced techniques such as adversarial AI, social engineering, and multi-stage exploitation to bypass traditional security measures.

CNAPP: A Top 3 Security Investment Priority for 2025 and Beyond

In response to advanced persistent threats, such as cross-domain attacks and insider threats, and the consequences of compliance gaps, organizations are prioritizing their security spending in three key areas for 2025: managed services, CNAPP, and XDR/SIEM systems, as found in the *IDC CNAPP Survey* (see **Figure 1**, next page).

Further reinforcing the importance of ecosystems, consolidation, and reducing MTTD and MTTR over the next two years, CNAPP was again one of the top security investments for these organizations, along with generative AI (GenAI) and zero trust network access.

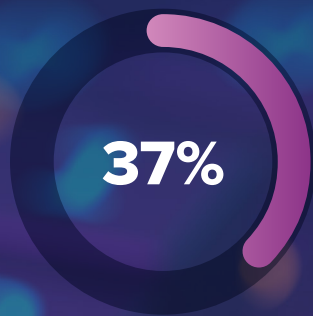
FIGURE 1
2025 Security Spending Priorities
What are the top 3 areas of security spending in 2025?
(Percentage of respondents)



Source: IDC, 2025

Organizations are increasingly recognizing the need to transition from a traditional detect-and-respond security model, which relied on consolidating suspicious events into log formats for subsequent investigation, to a more proactive approach. This new paradigm leverages contextualization, correlation, prioritization, and real-time remediation, with delivery through a single pane of glass and a customized user view.

These investments aim to enhance security measures and improve the overall security posture of organizations.



CISOs are increasingly taking more ownership of overall cloud security management, now 37% of organizations, followed by the cloud security architect, chief compliance officer, and cloud security engineer.

Evolving Role of the CISO

IDC has reported that CISOs are increasingly taking more ownership of overall cloud security management, with 37% of organizations now following this approach, followed by the cloud security architect, chief compliance officer, and cloud security engineer. This includes implementing security policies, managing access controls, and ensuring compliance with regulatory requirements. However, as the role of the CISO evolves, IDC has introduced the concept of the “3D CISO,” who operates across three dimensions: security, business, and digital. This new breed of CISOs will create change within their organizations, align security with business priorities, and support digital innovation. This involves adopting zero trust security principles, embedding security early in the development life cycle (DevSecOps), and fostering collaboration among development, operations, and security teams.

The role of the CISO is evolving to address business risk mandates. This new era requires integrated security solutions such as CNAPP, which include shift-left DevSecOps tools with infrastructure as code (IaC) and software composition analysis (SCA). The IDC mantra “security risk is business risk” fits this context well.

CISOs should align security with business priorities and support digital innovation. This shift necessitates a consolidated approach to security tooling and improved efficiencies in security frameworks. For example, cloud security architects now facilitate expanding visibility, monitoring posture, and prioritizing existing risks while serving as an interface between security teams, developers, and cloud engineers to address vulnerabilities and misconfigurations. In contrast, only 20% of DevOps teams have visibility or participate in this cloud security life cycle. This suggests that not all security teams have uniform visibility and capabilities to leverage cloud security tools, including a CNAPP platform.

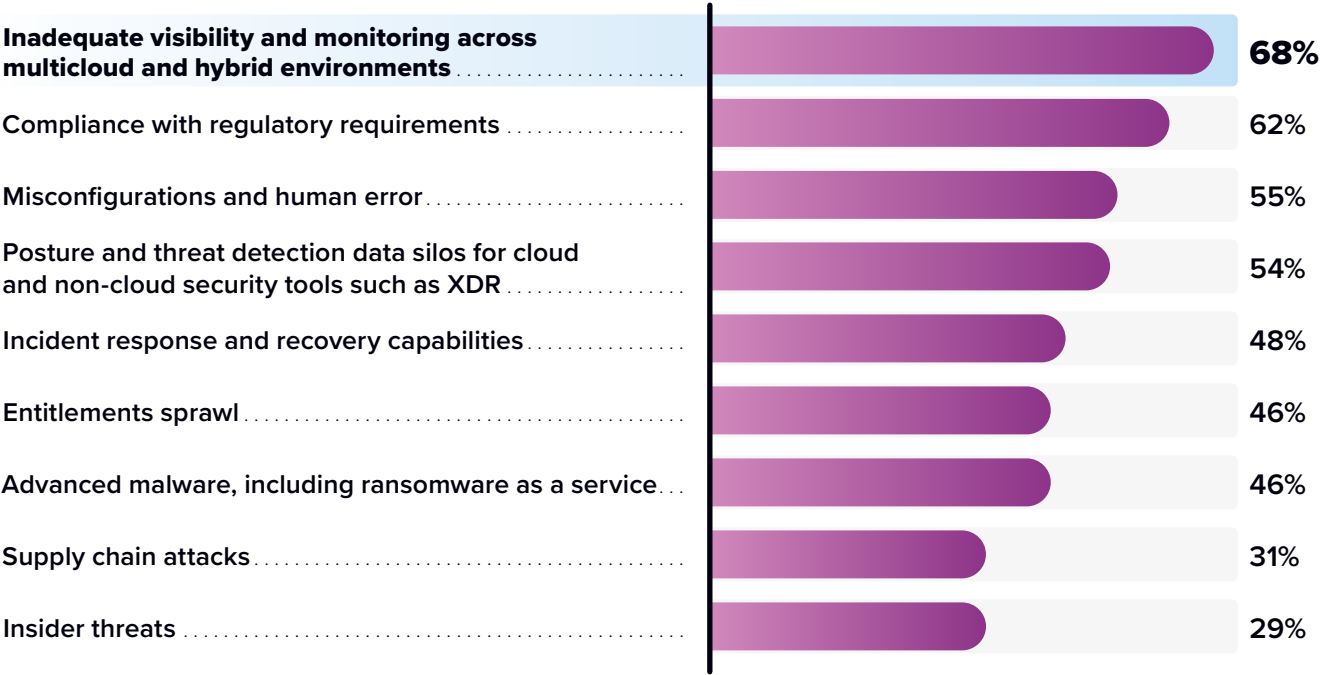
Additionally, the CISO persona has traditionally led compliance initiatives. CNAPP platforms have become instrumental in addressing regulatory requirements and governance frameworks. Regulations such as the EU’s Network and Information Security Directive 2.0 and the Digital Operational Resilience Act now enjoy support from continuous compliance management and automated reporting delivered through CNAPP, which reduces the operational overhead on CISOs, prevents CISO burnout, and enhances the organization’s security posture.

Need for End-to-End Visibility and Tool Consolidation

Organizations worldwide are utilizing between 0 and 20 cloud security tools, with an average of 10 tools per organization. Additionally, 47% of organizations indicated that the number of tools they use has increased year over year. This tool sprawl highlights the need for end-to-end visibility and consolidation of security tools to manage costs and improve efficiency.

The complexity of managing security across different platforms and environments with varying standards, configurations, and compliance with regulatory standards exacerbates these challenges (Figure 2).

FIGURE 2
Cloud Security Concerns
What are your organization’s biggest cloud security concerns?
(Percentage of respondents)



Source: IDC, 2025

Organizations need full end-to-end visibility, from a single pane of glass, to contain the blast radius in the event of a breach.

The integration of legacy systems with cloud services complicates the security landscape, requiring a balanced approach to ensure data flows securely without introducing vulnerabilities and maintaining compliance with regulatory requirements.

These sentiments saw reinforcement as organizations detailed additional cloud security concerns, including:

- ▶ Misconfigurations and human errors
- ▶ Posture and threat detection data silos for cloud and non-cloud security tools such as XDR
- ▶ Entitlements sprawl, advanced malware including ransomware, supply chain attacks, and insider threats

Organizations need full end-to-end visibility, from a single pane of glass, to contain the blast radius in the event of a breach.

To act quickly, organizations need on-demand prioritization of alerts. Leveraging additional resources, such as targeted deep telemetry, can alleviate alert fatigue. This approach enables teams to visualize the connections in progress and comprehend the conversations unfolding through attack path analysis. By focusing on alerts that matter and reducing false positives, teams can enhance their efficiency and effectiveness in managing security threats. Prioritization of misconfigurations and vulnerabilities, AI/ML-driven analytics, and security for AI and network detection and response are some of the services that must be in place to secure modern environments.

Achieving this level of foundational cloud security can be difficult. In security, when time allows, the security operations center (SOC) or tier 1 analyst will always opt to perform a root cause analysis, which is a best practice.

However, several factors can prevent that from happening:

- ▶ Inability to route alerts to developer teams fast enough
- ▶ Lack of infrastructure context
- ▶ Tool sprawl — hard to use and not fully integrated
- ▶ No central dashboard to manage, monitor, alert, and remediate issues



IDC research confirms that when it asked organizations, on average, how long it took for their security operations center or cloud security analyst teams to perform basic research once receiving a unique alert, 30% of organizations answered one day or more.

Why CNAPP Must Be Part of the SecOps Platform

Tool sprawl highlights the need for end-to-end visibility and consolidation of security tools to manage costs and improve efficiency. These constitute investment drivers for integrated security operations platforms.

Several factors drive investment in integrated SecOps platforms, including the need to lower MTTD and MTTR; enhance visibility into possible and active threats; consolidate tools for better cost management; unify security data, assets, and entities; and facilitate easier AI deployment.

Cloud-native applications have challenges. Data breach or loss due to ransomware, automation of policy management, and management of multiple identity and access domains compound organizational concerns. This is most aptly visible in operational efficiency. The time between discovering a vulnerability and its exploitation is growing shorter. IDC research confirms that when it asked organizations, on average, how long it took for their security operations center or cloud security analyst teams to perform basic research once receiving a unique alert, 30% of organizations answered one day or more. Siloed teams are taking their toll on security health, hygiene, and posture.

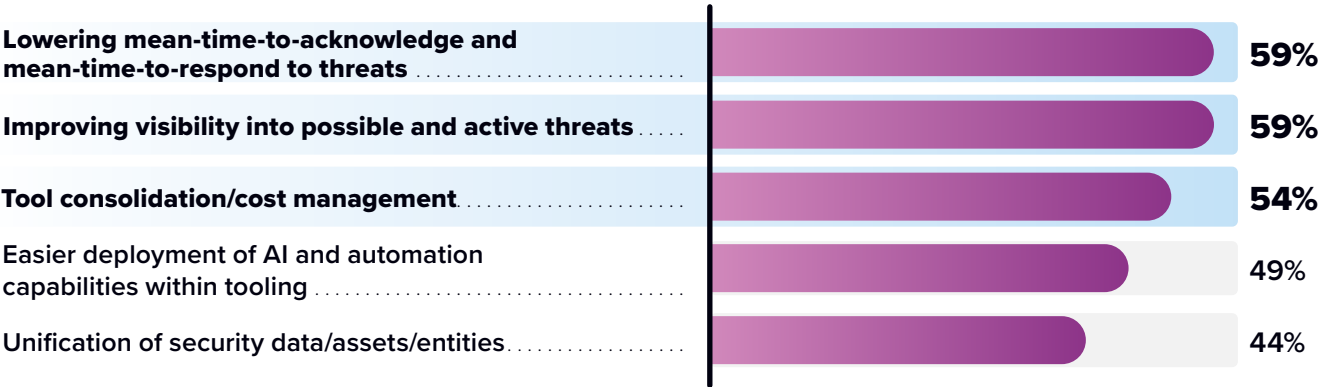
The premise of an integrated SecOps platform (see **Figure 3**, next page) enhances the future proofing of the SOC. By unifying various security tools and processes into a cohesive platform, organizations can achieve greater efficiency, visibility, and coordination in their security operations. This integration ensures that security teams can respond to threats more effectively, streamline workflows, and leverage advanced analytics and automation to stay ahead of emerging threats. The integrated SecOps platform is a critical component in building a resilient and adaptive SOC that can meet the evolving demands of cloud security.

FIGURE 3

Why CNAPP Must Be Part of the End-to-End Security Platform

What would be your top 3 drivers for investing in an integrated SecOps platform?

(Percentage of respondents)



Source: IDC, 2025



According to the *IDC CNAPP Survey*, 50% of organizations stated that ease of integration with SIEM/XDR would influence their decision to adopt a new CNAPP.

Given the cloud security team's need to operate at maximum speed while minimizing risk, platforms have become essential tools for gaining visibility into cloud environments; assessing vulnerabilities and misconfigurations; and detecting, alerting, and remediating threats. As CNAPP solutions are the product of consolidating multiple technologies, they serve as the anchor for an integrated SecOps platform.

According to the *IDC CNAPP Survey*, 50% of organizations stated that ease of integration with SIEM/XDR would influence their decision to adopt a new CNAPP. This integration is crucial for reducing MTTR, mitigating cross-domain attacks, and addressing adversarial AI use. A unified platform provides defenders with the edge they need to see all threats and act quickly.

CNAPP platforms have evolved rapidly, with promises of contextualization, correlation, prioritization, and remediation for hybrid and multicloud environments. IDC previously referred to them as cloud workload security, as cloud workload protection platform and cloud security posture management were two sides of the same coin. However, as more companies refactor their applications, CNAPP solutions have added new capabilities. These include functionalities such as cloud identity entitlement management, Kubernetes/container security posture management, data security posture management, application security posture management, AI-security posture management, and some

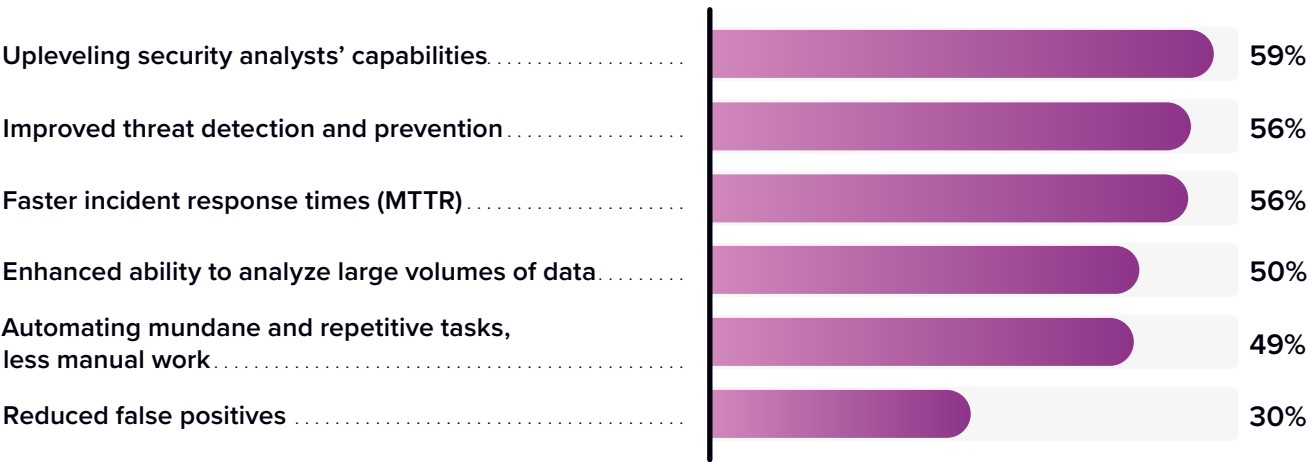
DevSecOps/software supply chain additions, including SCA and IaC scanning. With the idea of unifying all data from code to cloud, cloud detection and response saw its introduction.

Organizations have established their security teams in various ways, including internal structuring and partial or full outsourcing. In addition to the SOC, there have been security teams dedicated to providing various approaches, ranging from code to cloud. As noted earlier, some teams have more influence than others during the security life cycle, which can lead to friction. Those focused on proactive security and reactive security delineate these roles. However, they share a common connection — they’re all short-staffed. The *IDC CNAPP Survey* found that 64% of proactive security teams reported a shortage, which aligns with the 61% shortfall in reactive security.

Unique benefits come from a GenAI-powered CNAPP. We’re long past the hype and can now see tangible outcomes to proactive and reactive security teams and the SOC. Here’s a breakdown of benefits from the *IDC CNAPP Survey* (see **Figure 4**).

FIGURE 4
GenAI-Powered Security

What are the top three benefits you expect from adopting GenAI-powered security solutions?
(Percentage of respondents)



Source: IDC, 2025

Unique Benefits of GenAI- Powered CNAPP



Upleveling of security analysts' capabilities:

GenAI-powered CNAPP enhances the capabilities of security analysts by providing advanced tools and insights that help them identify and mitigate potential threats before they materialize. This includes predictive analytics and automated threat hunting.



Improved threat detection and prevention:

By leveraging GenAI, CNAPP can analyze vast amounts of data to detect anomalies and potential threats more accurately and quickly, enabling proactive measures to prevent security incidents.



Faster mean time to respond:

GenAI-powered CNAPP accelerates the incident response process by automating the detection, analysis, and remediation of security incidents. This reduces the time it takes to respond to and contain threats.



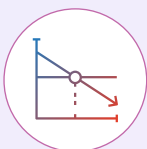
Enhanced ability to analyze large volumes of data:

GenAI can process and analyze large data sets in real time, providing reactive security teams with the information they need to understand the scope and impact of security incidents quickly.



Automation of mundane and repetitive tasks:

GenAI-powered CNAPP automates routine tasks such as alert triage, log analysis, and report generation, freeing up SOC analysts to focus on more complex and strategic activities.



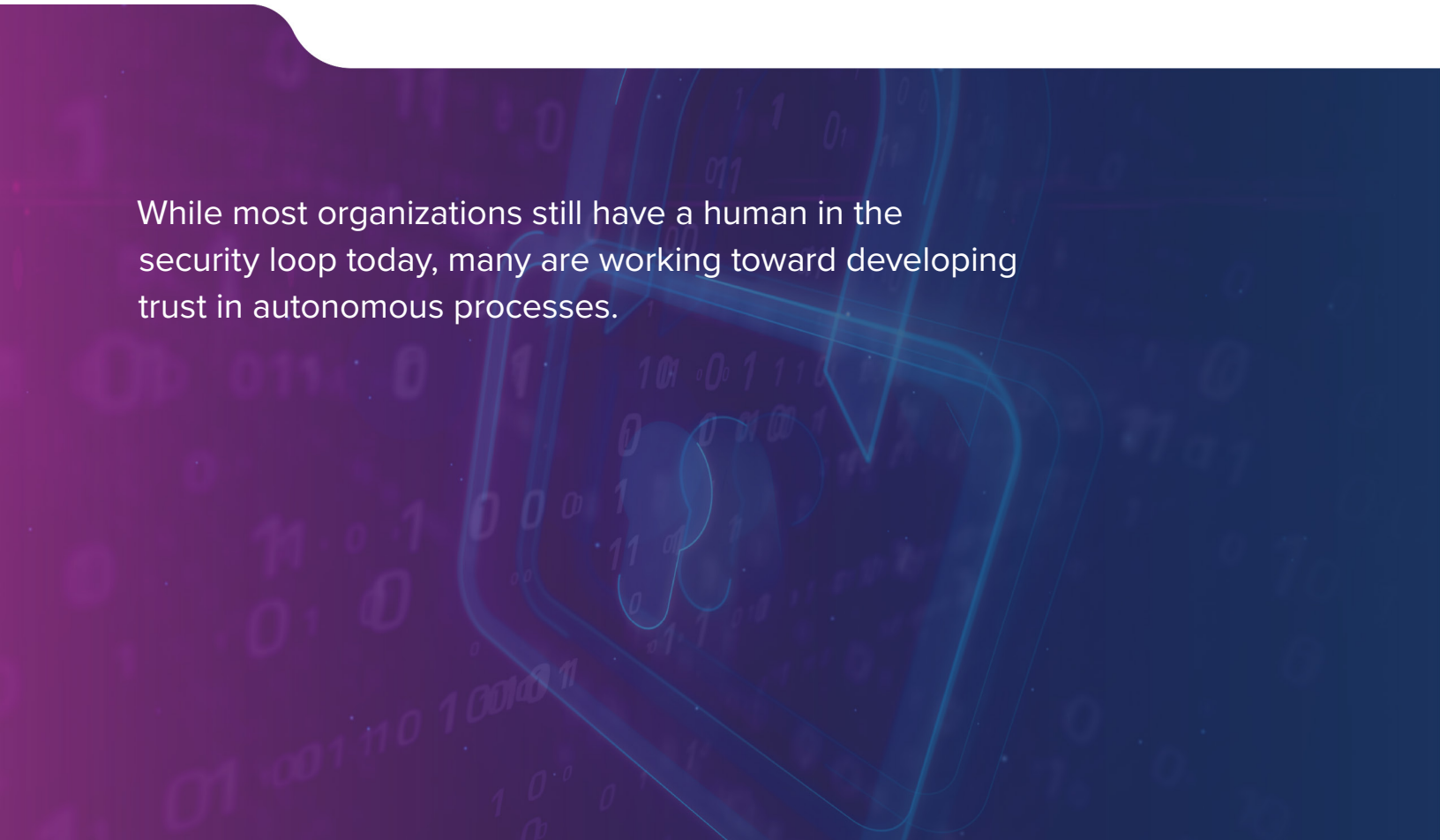
Reducing false positives:

By leveraging advanced ML algorithms, GenAI-powered CNAPP can reduce the number of false positives, enabling SOC analysts to focus on genuine threats and improve overall efficiency.

The combination of these features underscores the robust nature of platforms and their potential contributions to cloud security strategies. As organizations traverse the AI landscape, in addition to GenAI, there is agentic AI. Agentic AI refers to large language model-powered autonomous software entities that can perceive their environment, make decisions, act upon them, and interact with users or other systems in a human-like manner.

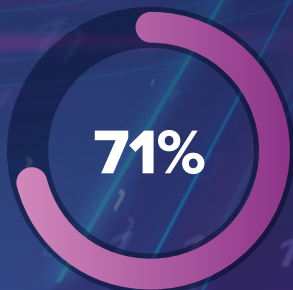
As organizations consider Agentic AI and its application with CNAPP, imagine a scenario where a CNAPP detects an unusual pattern of behavior that indicates a potential security breach. An agentic AI can recognize anomalies, determine the best course of action, automatically isolate affected systems, block malicious traffic, initiate remediation processes, and communicate with other systems and security personnel, providing updates and requesting additional actions as necessary.

Reducing manual and repetitive tasks and providing autonomous incident response in real time frees up the CISO and SOC to focus intently on securing the organization's critical assets and infrastructure. While most organizations still have a human in the security loop today, many are working toward developing trust in autonomous processes.



While most organizations still have a human in the security loop today, many are working toward developing trust in autonomous processes.

Essential Guidance



The *IDC CNAPP Survey* affirmed that 71% of respondents believe that over the next two years, it would be beneficial for their organization to invest in an integrated SecOps platform that includes technologies such as XDR/EDR, SIEM, CNAPP/cloud security, GenAI, and threat intelligence.

✓ **Optimize security spend and reduce complexity:**

The primary driver of cloud security overspend is complexity. Organizations should focus on consolidating tools and vendors to streamline SecOps for better efficiency and effectiveness. Implementing a CNAPP that's integrated or part of a broader unified SecOps experience can help reduce complexity and MMTR, and minimize costs.

✓ **Explore CNAPP differentiation:**

Organizations should always seek a simpler way to manage risk. CNAPP solutions should continuously innovate to provide security teams with knowledge of cloud risk exposure and the ability to autonomously or semi-autonomously activate appropriate response playbooks, leveraging GenAI.

✓ **Integrate CNAPP and SecOps:**

Extended detection and response and security information and event management solutions should provide comprehensive visibility and robust data protection. XDR platforms should offer integrations with CNAPP, identity and access management, firewalls, and domain service providers to enhance threat context and response capabilities. The *IDC CNAPP Survey* reinforced these sentiments, with 71% of respondents affirming that over the next two years, they believe it would be beneficial for their organization to invest in an integrated SecOps platform that includes technologies such as XDR/EDR, SIEM, CNAPP/cloud security, GenAI, and threat intelligence.

✓ **Leverage managed security services (MSS) for comprehensive coverage:**

Managed security services providers offer a range of services, including managed detection and response, managed SIEM, and managed cloud security. These services help organizations address security challenges by providing expertise, operational excellence, and continuous compliance validation. MSS providers should focus on delivering platform-based offerings that enhance efficiency through automation and cloud-based platforms.



Challenges/Opportunities

47%

of organizations experienced a year-over-year increase in the number of security tools, marking an almost 50% rise since 2022.

Overcoming Security Tool and Entitlements Sprawl

The proliferation of security tools is fragmenting teams. This issue has been highlighted for some time, with IDC's *U.S. 2022 Cloud Security Survey* reporting a 32% year-over-year increase in the number of security tools. Comparatively, the *IDC CNAPP Survey* revealed that 47% of organizations experienced a year-over-year increase, marking an almost 50% rise since 2022. Traditional drivers for this stem from increasing cloud usage, mergers and acquisitions, and shadow IT. This could be due to getting to market faster and the increasing trend of non-security staff (e.g., IT admins) filling in for security practitioners owing to the talent gap. In this case, organizations can argue for credentialed and certified MSS to avoid a crisis.

Likewise, with the rise of identity as the new security perimeter, organizations are facing challenges with entitlement sprawl. IDC research confirms that among organizations with a current cloud infrastructure entitlements management (CIEM) solution, two-thirds face restrictions in tracking machine entitlements. The highly ephemeral nature of nonhuman workloads (which can last for minutes or seconds and are commonly referred to as "invisible") makes this percentage likely higher. As stated earlier, multicloud, the correlation of entitlement data with other security findings, and regulatory compliance reporting compound these challenges. Improper management and tracking of entitlements lead to excessive permissions, creating visibility gaps and opening the door to cybercriminals, malicious insider threats, or unintended employee negligence. The use of a CNAPP rather than a standalone CIEM solution will provide broader context and compliance support.

Conclusion

As organizations navigate the complexities of cloud security in 2025 and beyond, integrating cloud-native application protection platforms with other advanced security solutions, such as XDR and SIEM systems, becomes imperative. IDC's research highlights the critical need for comprehensive and unified security measures to combat the increasing sophistication of cyberthreats and the proliferation of cloud services.

The evolving threat landscape and the increasing number of cloud security incidents underscore the importance of integrated security solutions. By prioritizing investments in managed services, CNAPP, and XDR/SIEM systems, organizations can enhance their security posture, achieve end-to-end visibility, and streamline security operations.

The evolving role of the CISO, coupled with the necessity for tool consolidation and the adoption of advanced technologies such as AI, underscores the importance of a cohesive security strategy. Embracing an integrated SecOps platform with CNAPP will enable organizations to address the complexities of modern cloud environments, reduce mean time to detect and respond, manage costs, and ensure a resilient and cost-effective security framework.

As organizations navigate the complexities of cloud security in 2025 and beyond, integrating cloud-native application protection platforms with other advanced security solutions becomes imperative.

About the IDC Analyst



Philip Bues

Senior Research Manager, Cloud Security, IDC

Philip Bues is the senior research manager for IDC Cloud Security. In this role, Bues drives research, provides thought leadership, and advises clients on complex issues, including cybersecurity of the cloud and in the cloud. His commentary will address the benefits and challenges to what's been called the shared responsibility model and how that line may change going forward.

[More about Philip Bues](#)

Message from the Sponsor



Unify security across the cloud app lifecycle and innovate faster.

Microsoft Defender for Cloud, a Cloud-Native Application Protection Platform (CNAPP) offers comprehensive security for your cloud-native applications, providing near real-time cloud detection and response, vulnerability scanning, and proactive risk management. Designed to seamlessly integrate with your DevOps pipelines, our CNAPP solution ensures that security is embedded at every stage of development.

With full visibility into your multicloud and hybrid infrastructure, you can identify, prioritize and mitigate risks early, ensuring compliance and preventing security breaches. Innovate securely, quickly, and confidently with Defender for Cloud, protecting your applications against emerging threats and vulnerabilities in the cloud.

[Learn more about Microsoft's Cloud Security solutions.](#)

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.



IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

idc.com

[@idc](https://www.linkedin.com/company/idc)

[@idc](https://twitter.com/idc)

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

©2025 IDC. Reproduction is forbidden unless authorized. All rights reserved. [CCPA](#)