Omdia
by informa techtarget

CNAPP Meets SOC

The End of Fragmented Defense

Authors: Ketaki Borade, Andrew Braunberg, and Elvia Finalle

December 2025

In partnership with:

paloalto NETWORKS

Contents

© 2025 TechTarget, Inc. All rights reserved. Unauthorized reproduction prohibited.

Omdia View

The acceleration of digital transformation has driven the adoption of cloud workloads, outpacing traditional security measures. Historically, organizations have opted for a unified cloud security platform, Cloud-Native Application Protection Platform (CNAPP), to address these challenges. However, this approach created a siloed security environment that has remained poorly integrated with security operations, with most organizations using over 30 standalone security products during 2025. According to Omdia's Decision Maker Survey, 59% of enterprises saw the severity of issues rise over the past two years. In the last year, 41% of these enterprises reported that several severe security incidents required meaningful escalation. The sophistication of modern attacks has illuminated the weaknesses of this siloed approach and necessitated the need for a more unified strategy.

The CNAPP Evolution: From Fragmented Tools to Integrated Platform

As cloud-native applications became prominent, cloud security had to undergo a dramatic evolution, transitioning from siloed, agent-based workload protection to integrated, context-aware platforms. Point solutions were deployed to address emerging threats, but this fragmented approach quickly became unsustainable, thus giving rise to CNAPPs.

Today, CNAPP unifies critical capabilities within cloud environments across posture and runtime security, including Cloud Workload Protection Platform (CWPP), Cloud Security

Posture Management (CSPM), Cloud Permissions Management (CPM, also known as Cloud Identity Entitlement Management or CIEM), Infrastructure as Code (IaC), Data Security Posture Management (DSPM), Cloud Detection and Response (CDR), and, most recently, Application Security Posture Management (ASPM).

While this bundling provides a more unified management experience from code to cloud, traditional security operations teams have limited visibility to drive their insights. Despite being integrated into the Software Development Lifecycle (SDLC) from build to deploy to run, CNAPP still continues to operate in isolation from incident response tools such as SOC, SIEM, SOAR, and XDR. According to Omdia's Cybersecurity Decision Maker Survey 2025 on infrastructure security, the market is expected to see an 11% adoption of pilot programs within the next six months for 2026, demonstrating the rapid shift from fragmented point solutions to unified platforms.

CNAPP Capabilities and Limitations

Cloud environments remain a major target for cyberattacks, and as discussed, CNAPP solutions have evolved to keep pace. It is important to understand what CNAPPs do well, as well as the gaps that exist.

Key strengths of CNAPPs include:

- Comprehensive visibility across multi-cloud environments
- Detection and remediation of a host of exposures, such as misconfigurations
- Enforced policy and compliance
- API integrations with CI/CD tools

The siloed nature of CNAPPs leads to:

- Incomplete visibility into hybrid/on-premises environments
- Inability to correlate alerts across the entire digital domain for comprehensive threat detection and response
- Lack of holistic context to properly assess and prioritize cyber risk in proactive use cases, fully investigate incident response, and perform digital forensics

CNAPP was designed to bring point products together to offer unified platforms, but in the race to offer it faster than others, vendors created self-contained ecosystems—only to

realize later the disconnect between CNAPP and SOC workflows. However, few serious attacks start and end in a single cloud environment. To understand and map an entire attack path across an organization's digital infrastructure requires a breadth of visibility only available in the SOC.

Today, 63% of organizations have adopted CNAPP in production use, according to Omdia's Cybersecurity Decision Maker Survey. However, these consolidation efforts remain confined within cloud-specific boundaries, failing to bridge the growing divide between cloud-native security capabilities and traditional SOC operations.

Omdia sees the disconnect between CNAPP and SOC broken down into three key categories:

- **Organizational issues**: Cloud security teams use CNAPP for configuration and risk management, while SOC teams monitor enterprise-wide threats via SIEM, SOAR, and XDR tools. Both teams work in parallel rather than in partnership.
- **Technical issues:** One of the biggest challenges for CNAPP is the high volume of alerts, which causes alert fatigue for analysts. CNAPP lacks the ability to deliver standardized telemetry formats consumable by SOC, and SOC alerts lack cloud-native context. Telemetry is fragmented, as context generated by cloud-native assets cannot be integrated into SOC teams.
- **Process misalignment:** The misalignment leads to duplication of alerts, manual intervention, and delays in remediation. Because CNAPP and SOC teams are often disconnected, it is not uncommon for a "Shadow Cloud SOC"—a parallel team dedicated to monitoring and responding to cloud incidents—to emerge. In other words, it is an informal duplication of security operations setup due to the lack of SOC visibility in cloud-native environments.

This disconnect will matter now more than ever as AI and automation usage accelerate and application development cycles continue to shorten. With this evolving landscape, both cloud and security operation teams cannot continue to operate reactively with partial visibility and poor collaboration.

From Code to Cloud to SOC: The New Blueprint for Enterprise Security

While cloud infrastructure clearly has unique features, cloud security does not need to remain on an island disconnected from broader security strategies. CDR as a standalone solution started as a bridge from cloud security to SecOps but has become almost nonexistent as a standalone product, with a 42% replacement rate in the following six months, according to Omdia's 2025 Cybersecurity Decision Maker Survey. In fact, the best future for cloud security would be the disappearance of cloud security as a standalone practice. Yes, cloud tools can competently detect threats in cloud infrastructure, but the bigger picture remains hidden.

Integration of cloud security into the SOC makes sense now more than ever, as the industry moves to democratize security data with support for common data models and federated access to threat and risk engines. By decoupling data sources from data destinations and adding the ability to process and operate on the data before it reaches a destination, several pressing challenges for security teams can be solved.

Perhaps most importantly, security teams can more effectively and efficiently manage the large and growing volume of security telemetry needed for TDIR. In practice, security teams can be more selective with telemetry and better differentiate data ingested for TDIR versus other uses (e.g., compliance). The addition of CDR data into existing TDIR solutions will enable the creation of unified detection and response across the entire digital landscape.

An integrated approach to SecOps and cloud security would support a "Code to Cloud to SOC" security strategy that integrates security practices throughout the entire application and cloud lifecycle—from initial code development to code deployment—with real-time monitoring and defense for an organization’s entire digital infrastructure managed within the SOC.

However, this shift can create ripple effects that extend throughout the organization and beyond. Organizations must keep in mind the various strategic implications for key roles as they navigate this security evolution (see Figure 1.)

Figure 1: Implications of CNAPP and SOC Evolution as Fundamental Pillars

Source: Omdia

Recommendations

The persistent fragmentation between CNAPP solutions and traditional security operations represents more than a technical integration challenge. It is a fundamental misalignment between how organizations secure their cloud environments and how they detect and respond to threats across their entire digital infrastructure. Omdia recommends:

For SMB and Small Enterprises

Solutions: Organizations should conduct gradual vendor reduction by first identifying overlapping security tools, then systematically replacing multiple point solutions with integrated platforms during contract renewal periods. Start by consolidating the most resource-intensive areas, such as endpoint security and email protection, then gradually expand to network security and monitoring tools while ensuring no security gaps during transitions.

Next Steps: Smaller organizations can transition into next-generation cloud-based SIEM or integrate security platforms that offer SOAR, threat detection, and cloud posture management. This consolidation reduces operational complexity, improves threat correlation, and enables consistent policy enforcement across all infrastructure components. According to the CDM survey, 43% of small and medium enterprises (up to

5,000 employees) say reduced complexity is the top driver for platformization and product consolidation.

For Enterprises

Solutions: Large enterprises should adopt integrated security platforms that have both cloud-based solutions and security operation solutions with a single field of view. Vendors that can provide platform suites with shared telemetry and response capabilities might meet end users' needs.

Next Steps: Enterprises should implement unified Zero Trust frameworks that consolidate cloud, network security, and data protection under centralized policy engines. These engines can enforce consistent security controls across cloud services, applications, and user access points. This approach simplifies security governance while providing granular visibility and control over all digital assets.

For Vendors

Solutions: Invest in developing threat intelligence sharing capabilities between your CNAPP and SecOps solutions. Gradually expand to more sophisticated capabilities, such as automated incident response, cross-platform analytics, and unified reporting, as your team develops operational maturity. Startups should aim to accommodate potential rapid growth and evolving security requirements. According to the CDM survey, enterprises see the need for innovation from start-ups in cloud security (31%) and security operations (19%).

Next Steps: Integrate within your roadmap and architecture the possibility of being acquired by a larger vendor. Develop clear objectives and provide technical support, documentation, and future development priorities that support your unified security operations vision. At the same time, ensure compatibility with multiple vendors in the cloud and security operations market.

For Service Providers

Solutions: Service providers should develop unified platforms that natively combine CNAPP capabilities with SOC operations, eliminating the need for customers to manage separate vendor relationships and complex integrations.

Next Steps: To develop a unified platform, service providers should create unified dashboards that correlate cloud security posture data with real-time threat intelligence. This will enable security teams to see both preventive controls and active threats in a single interface.

Conclusions

While the recommendations outlined above provide practical pathways for different organizational sizes to bridge this divide, the ultimate success of these efforts depends on a strategic commitment to unified security operations that transcend vendor boundaries and enterprise silos.

Organizations that recognize CNAPP and SOC as complementary pillars of enterprise cybersecurity, rather than competing capabilities, will achieve strong threat prevention, detection, and response outcomes. CNAPP's proactive cloud security posture management and vulnerability intelligence must inform SOC's real-time threat hunting and incident response. Meanwhile, SOC's behavioral analytics and attack telemetry should enhance CNAPP's risk prioritization and remediation workflows.

This complementary architecture transforms enterprise cybersecurity from a collection of isolated security functions into a unified defense capability. It can both prevent attacks through strong security posture and rapidly neutralize sophisticated threats that evade preventive measures, ultimately delivering the comprehensive protection that modern digital enterprises require.

Appendix

Methodology

This report references data collected from Omdia's Cybersecurity Decision Maker Survey, fielded in September 2025. Data from the Enterprise Cybersecurity Operations (SecOps) and Infrastructure Security sections are included.

Further reading

Fundamentals of Multicloud security (March 2025)

A new Omdia tracker shows key competitors in cloud security offerings and healthy sector growth (November 2024)

Cybersecurity Decision Maker Survey 2025: Enterprise Cybersecurity Operations (SecOps) (September 2025)

Cybersecurity Decision Maker Survey 2025: Infrastructure Security (September 2025)

Ketaki Borade, Senior Analyst, Infrastructure Security
Andrew Braunberg, Principal Analyst, SecOps
Elvia Finalle, Senior Analyst, SecOps
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Get in touch

www.omdia.com
askananalyst@omdia.com