White Paper

Bridging the CNAPP — SecOps Divide

Sponsored by: Palo Alto Networks

Philip Bues Emanuel Figueroa

April 2025

IN THIS WHITE PAPER

The landscape of cloud security and security operations centers (SOCs) is evolving rapidly, driven by the increasing complexity of cyberthreats and the need for more integrated and efficient security solutions. The cyber battlefield is fraught with threats, cloud misconfigurations, and identity risks that can cripple an organization in moments.

Furthermore, breaches are now presumed to have occurred, and postures are tracked based on a threat graph bringing together all the telemetry obtained from workloads, identities, endpoints, configurations, and DevOps. In response to these changes, numerous tools and platforms have been developed to generate more intelligence to stop incidents in the early stages. However, these new tools and platforms are also challenging the way security teams are organized and how they interact with each other and with other elements of the security stack.

Organizations must balance their security strategies between peacetime (posture management) and wartime (active threats). This duality requires SOCs to be adaptable, with capabilities to shift from monitoring and compliance to active threat detection and response.

However, the emergence of shadow IT and unsanctioned cloud services has led to the rise of shadow cloud SOCs. These entities operate outside the purview of traditional IT and security departments, creating blind spots and increasing the risk of security breaches.

To address these challenges, organizations are focusing on integrating cloud security with SOC operations. This integration involves adopting cloud-native security tools, enhancing visibility across cloud environments, and ensuring consistent security policies and practices.

April 2025, IDC #US53351025

Cloud-native application protection platform (CNAPP) has established itself as the new standard for cloud security, providing contextualization, correlation, smart prioritization, and automated remediation for alerts and threats, prompting many organizations to adopt different operational approaches — and, for many, in the nick of time. IDC research shows that 57% of cloud operations teams — including those responsible for allocating resources, monitoring, and fixing issues related to traditional IT operations — remain responsible for cloud security programs even when they are not security specialists.

Cloud-native application protection platforms offer comprehensive security for cloud-native applications but often remain disconnected from traditional SOCs. This disconnect creates additional security blind spots, further emphasizing the need for SOCs to incorporate CNAPP capabilities into their operations.

During an active attack, the importance of a unified SOC becomes evident. A unified SOC can more effectively coordinate responses, leverage integrated tools, and provide real-time visibility, significantly improving the organization's ability to mitigate and recover from attacks.

A unified approach that combines CNAPP and SOC capabilities across a common data model/framework can offer a holistic security solution. This approach enables comprehensive protection for cloud-native applications and seamless integration with SOC operations.

Coupled with artificial intelligence (AI) and automation, SOC operations are being transformed by enhancing threat detection, reducing response times, and alleviating the burden on security practitioners. These technologies enable SOCs to handle the increasing volume and complexity of security threats more effectively.

IDC believes CNAPP has been continuously adapting to meet the required competencies for effective management, but a cultural shift into the organizational structure, requiring more coordination than usual, is needed to effectively avoid breaches and future incidents that span both cloud and enterprise environments.

This white paper explores the current state and future directions of cloud security and SOCs, examines key trends such as organizational cultural shifts, analyzes challenges and opportunities, provides essential guidance for integration, and seeks to answer the question: Does the future of security lie in the seamless integration of CNAPP and SOC working as a unified system?

Through best practices, this paper provides insights for organizations considering similar initiatives and highlights Palo Alto Networks (PAN) Cortex Cloud. With a future outlook on the continuous evolution and integration of CNAPP and the SOC,

organizations will have a unique lens into bridging modern security gaps and future proofing the SOC.

SITUATION OVERVIEW

Introduction: The SOC and CNAPP — Shifting Security Paradigms

The rapid evolution of cloud security has created a significant divide between cloud security teams and traditional security operations centers. This disconnect is primarily due to the differences in the tools and telemetry used by each group. While cloud security teams leverage advanced cloud-native tools, SOCs may rely on legacy systems that are not designed to handle the dynamic nature of cloud environments. This mismatch leads to inefficiencies and gaps in the overall security posture of organizations, a dangerous proposition in a world where it is not *if* a breach will occur but *when*.

As CNAPPs gain traction, security leaders must confront a difficult question: Is posture management enough to protect cloud environments during active attacks? These platforms excel at identifying misconfigurations and enforcing policy — but when attackers move fast, is detection without response truly protective?

The security operations center is considered the security office's "vertebral column." As such, it is expected that this team must be capable of detecting, responding to, and coordinating all efforts to contain a possible incident. Ideally, the team can also avoid the impact of a possible breach by identifying signs of compromise. But what happens if the findings are related to an application deployed in two-plus cloud service providers and the SOC does not have context on the API configuration, how microservices work, or if the image instance is misconfigured? Requiring that the SOC first ascertains the owner of the asset and then collaborates with other groups to implement the necessary actions involves precious time that the SOC does not have, as time to exploit grows shorter through the use of advanced technologies including adversarial AI.

Cloud security has advanced rapidly, with organizations adopting cloud-native application protection platforms to manage their security posture. However, some enterprise SOCs have struggled to keep pace with these advancements. Traditional SOCs are often disconnected from cloud security, leading to a fragmented security approach that opens the door to vulnerabilities, sometimes driven by internal security teams, and external attacks.

Shifting Focus During an Attack

Traditional cloud-native application protection platforms excel at security hygiene and as an extension posture management during routine operations, often referred to as "peacetime." The focus is on continuously monitoring, hunting for threats, detecting anomalies, optimizing security measures, and ensuring compliance.

But when cloud environments come under active attack, those same tools often operate in isolation — without the real-time context, shared visibility, or coordination needed to respond at speed.

During an "attack," the focus should be on:

- Enhanced visibility, contextual awareness, and unified security posture management
- Advanced threat detection and real-time response
- Improved collaboration and accountability

These limitations create a gap in the ability to respond to threats promptly and effectively.

As a result of the disconnect between cloud security teams and traditional SOCs, what's become known as a "shadow cloud SOC" has emerged. Cloud security teams are operating security tools independently of the SOC, without any broader enterprise context, leading to slow, disjointed responses. This parallel security function fragments defenses and delays critical response efforts, undermining the overall security posture of the organization.

CNAPP's Strengths and Shortcomings

Cloud-native application protection platforms have become essential tools for managing cloud security posture and ensuring compliance. They excel in areas such as misconfiguration management and compliance enforcement, providing organizations with the ability to continuously monitor and remediate security issues in their cloud environments. Many organizations view CNAPP adoption as a natural evolution of security in the cloud, enabling greater visibility and more consistent policy enforcement across multicloud environments.

According to the results of IDC's 2024 *Cloud Security Survey,* when organizations were asked about their plans for professional cloud services over the past 18 months, 56.6% of respondents indicated that they had validated and assessed their cloud security controls (CSPM, CNAPP), and another 32.4% intend to over the next 12 months (see Figure 1). The level of engagement seen in this survey and others highlights CNAPP's central role in many organizations' cloud security strategies.

Yet, as CNAPPs become more embedded in enterprise architectures, new challenges surface, particularly in their ability to support real-time detection and response. While CNAPPs are effective at identifying and addressing potential vulnerabilities and misconfigurations, they may lack the capabilities needed to detect and respond to active threats in real time.

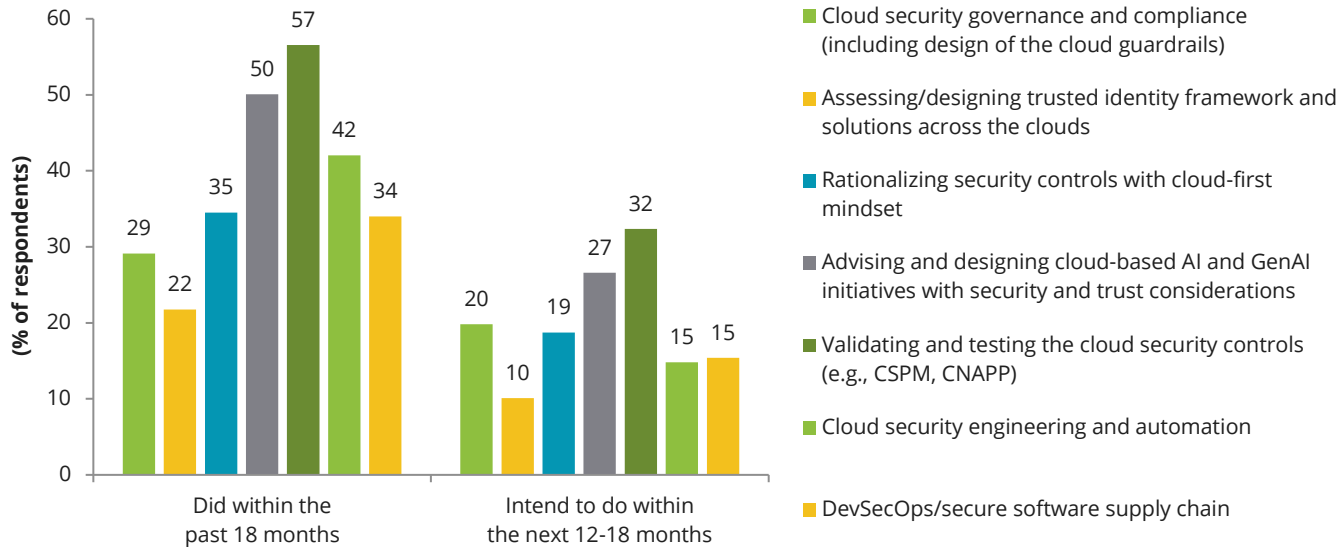
Ultimately, SOCs can benefit from enhanced collaboration and accountability by fostering a culture of continuous assessment and improvement. When clear roles and responsibilities can be established, SOCs can ensure that all security teams are aligned and working toward common security goals.

Figure 1 shows the plan for professional cloud security services from IDC's 2024 *Cloud Security Survey.*

FIGURE 1

Plan of Action for Professional Cloud Security Services

Q. Which best describes your organization's actions/plan of action for the following professional cloud security services?



n = 1,020

Source: IDC's *Cloud Security Survey,* 2024

SOCs Are Responsible for Enterprisewide Security But Lack Direct Cloud Security Insights

SOCs are tasked with overseeing the overall security of the organization, including threat detection and incident response. However, without direct insights into cloud

security provided by CNAPP, it is more difficult, and precious time is wasted trying to effectively monitor and respond to threats in cloud environments. Today, many SOC teams rely on disparate tools to gather information from various sources. This fragmented approach often results in incomplete visibility and a lack of context, making it difficult to fully understand the nature of the threat, and this can lead to inconsistencies in security policies and configurations. Furthermore, the lack of comprehensive visibility and context slows down the mean time to detect (MTTD) and mean time to respond (MTTR) as SOC analysts spend valuable time piecing together information from multiple sources.

The lack of integration between CNAPPs and SOCs creates gaps in the organization's security posture. Attackers often exploit these blind spots, moving quickly through cloud-native environments that lack real-time monitoring or integrated remediation workflows.

The Shadow "Cloud SOC" — A By-Product of Fragmentation

Unintended Consequences of CNAPP Adoption

What happens when cloud security succeeds — independently? With cloud security teams adopting modern tools and workflows tailored to the dynamic nature of the cloud, a new operational challenge has surfaced: Security functions evolve in silos.

This phenomenon is characterized by the following issues:

- **Cloud security engineers manage security without SOC oversight:** Cloud security engineers often operate independently of the traditional SOC, managing security posture and compliance within their cloud environments. Independence means that their activities and findings are not always visible to or coordinated with the SOC, leading to a lack of oversight and integration. For example, if a cloud security engineer detects a misconfiguration in a cloud environment, they may address the issue without informing the SOC. If the misconfiguration leads to a security incident, the SOC may be unaware of the root cause, leading to delays in containment and remediation. The resulting lack of communication and accountability can have severe consequences for the organization's security posture.
- **Teams operate in silos, resulting in missed attack paths and uncoordinated workflows/responses:** The separation between cloud security teams and SOCs creates operational silos. These silos lead to missed attack paths as each team may only have a partial view of the threat landscape. In addition, uncoordinated workflows and responses can result in inefficiencies and gaps in the overall security posture. Although each team may remain vigilant, the lack of shared

context means attackers can move between misconfigurations, vulnerabilities, and runtime threats with little resistance.

What Happens When an Attack Is Underway?

When an attack is underway, the fragmentation between CNAPPs and SOCs becomes even more apparent and problematic:

- **The SOC cannot investigate and respond to cloud-native threats in real time:** Without real-time insights into cloud environments, the SOC is unable to effectively investigate and respond to cloud-native threats. This limitation hampers its ability to contain and mitigate the impact of an attack.
- **Attackers move freely between cloud misconfigurations, runtime threats, and identity risks without detection:** The gaps created by the lack of integration between CNAPPs and SOCs allow attackers to move laterally within the cloud environment. They can exploit cloud misconfigurations, runtime threats, and identity risks without being detected. For example, ransomware delivered via phishing typically succeeds by compromising credentials, moving laterally, escalating privileges, and then encrypting and possibly exfiltrating data. This freedom of movement increases the likelihood of a successful breach and the potential damage to the organization.

The emergence of a shadow "cloud SOC" highlights the critical need for better integration between CNAPPs and traditional SOCs.

Why a Unified SOC Matters

Cloud Security Without Boundaries

The SOC needs direct, real-time insight into misconfigurations, runtime risks, and adversarial activity. The traditional boundaries of on-premises security no longer apply, and security operations must adapt to the fluid nature of cloud infrastructure. This requires a shift from static security measures to dynamic, continuous monitoring and response capabilities that can keep pace with the rapid changes in cloud environments.

The Role of Cloud Detection and Response

Cloud detection and response (CDR) is a CNAPP security capability that provides threat detection, identification, and response for multiple cloud environments, services, and cloud workloads. As highly distributed cloud assets continue to expand, gaining visibility in threat identification, misconfigurations, and vulnerability identification, along with compliance deviations, is essential.

By continuously monitoring cloud environments, CDR solutions aim to prevent unauthorized access and breaches by proactively identifying risks and adapting to the ever-changing cloud infrastructure environment.

Operationalizing Cloud Security in the SOC

Effective integration with comprehensive ecosystems is essential for achieving optimal precision in security operations. Cybersecurity vendors facilitate this integration by providing solutions that work well with existing security tools and platforms. This promotes collaboration between different teams, ensuring that security measures are implemented consistently across the organization to effectively future proof the SOC. Further:

- Cloud security should not be treated as an isolated discipline but rather as an integral part of the SOC's operations. This means incorporating cloud security tools and processes into the SOC's workflows and ensuring that cloud security incidents are managed with the same rigor as on-premises incidents.
- Cloud and enterprise security teams need a shared intelligence framework for responding to threats. This framework should facilitate the exchange of threat intelligence, incident data, and response strategies between teams, enabling a coordinated and unified approach to security.

  Threat intelligence plays a distinctive role by bolstering both preventive measures and detection capabilities in the field of cybersecurity. When a threat intelligence vendor identifies adversarial tactics in the real world or characterizes exploited vulnerabilities, the goal is that this information can contribute to populating CNAPP products, thereby enhancing prevention. Likewise, in instances where a business encounters a series of indicators of compromise (IoCs), the expectation is that these IoCs can be cross-referenced with the threats, tactics, and procedures employed by adversaries, proving vital for effective detection against ransomware, data exfiltration, cryptomining, and compromised identities.

  In the same vein, threat intelligence is pivotal for empowering a modern SOC with contextual, actionable information about potential and existing threats. It goes beyond raw data, providing analyzed insights into adversaries' tactics, techniques, and procedures. In an SOC, threat intelligence feeds inform detection rules, guide incident response strategies, and enhance proactive threat hunting. It enables the SOC to stay ahead of emerging threats, understand attack motivations, and effectively prioritize defensive efforts. Furthermore, threat intelligence aids in risk assessment and strategic decision-making, helping organizations allocate resources efficiently and adapt their security posture to address relevant threats.

A Unified CNAPP + SOC Approach

If CNAPP adoption continues to grow, how must the technology evolve to meet real-time operational demands? The answer isn't obvious. The growing complexity of multicloud environments and distributed development teams has forced organizations to reassess the role CNAPP plays — not just in posture but in response.

Organizations have several options:

- Leave CNAPPs siloed, letting cloud security teams operate independently with dedicated tools but limited SOC integration.
- Push CNAPP data downstream into DevOps pipelines, treating security as a shift-left engineering challenge.
- Operationalize CNAPP capabilities within the SOC, merging posture with detection and response to create shared context and faster action.

Each model carries trade-offs. The first risks fragmentation. The second blurs roles and may overwhelm developer workflows. The third unification offers the promise of full-scope visibility and coordinated response but requires cultural and technical integration.

The Role of AI and Automation

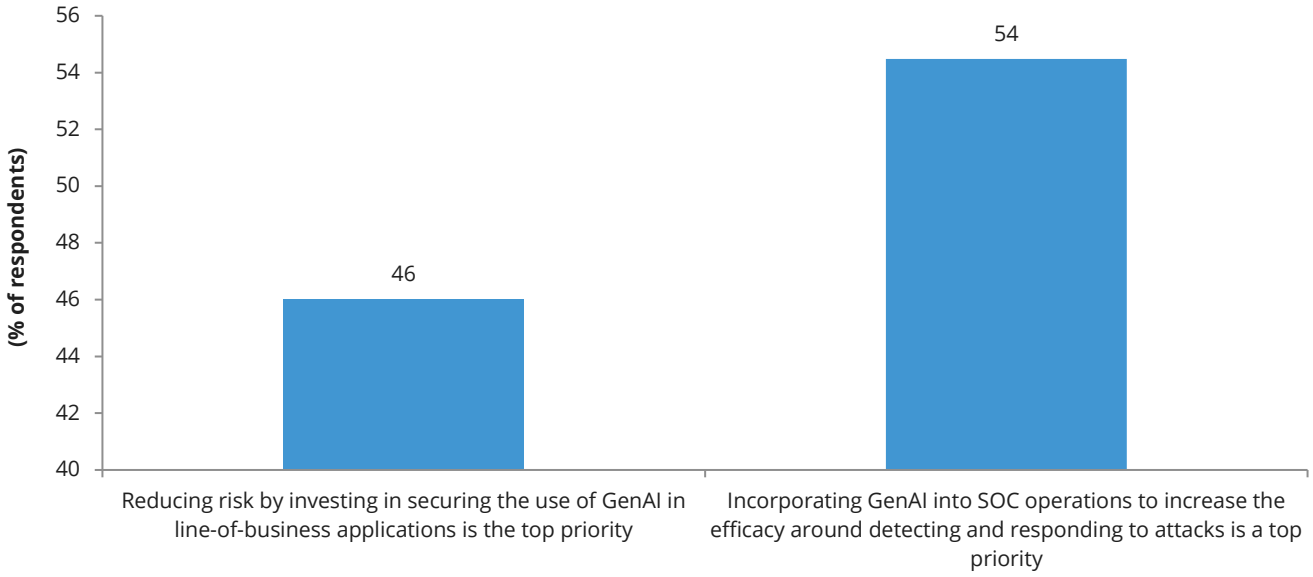
Artificial intelligence and automation are pivotal in closing cloud security gaps. AI-driven prioritization helps in identifying the most critical threats and vulnerabilities, ensuring that security teams focus on the most pressing issues. Much like the modern SIEM, CNAPPs leverage AI and machine learning to detect patterns and anomalies that may indicate security incidents. AI guiding threat intelligence will personalize the vast world of the internet, leading to meaningful feeds for individual companies. AI-driven automation is only touching its potential as a means to connect users, applications, and data for security outcomes.

The use of AI is not new; AI with machine learning has been prevalent for years. For example, user and entity behavior analytics establishes baseline behavior for devices or personas, and it will look for abnormalities or deviations from expected behavior. By integrating generative AI (GenAI) into the SOC alongside CNAPP capabilities, organizations can significantly enhance the efficiency, accuracy, and scalability of security operations (see Figure 2).

FIGURE 2

Priorities on Cybersecurity-Related Investments in GenAI

Q. Which of the following best matches your organization's priorities on cybersecurity-related investments in GenAI?



n = 1,123

Source: IDC's *Security Services Survey,* 2024

Automated response mechanisms enable rapid mitigation of threats, reducing the window of opportunity for attackers. These technologies enhance the efficiency and effectiveness of security operations, allowing for real-time threat detection and response.

Bridging the Gap: Integrating Cloud Security and SOC

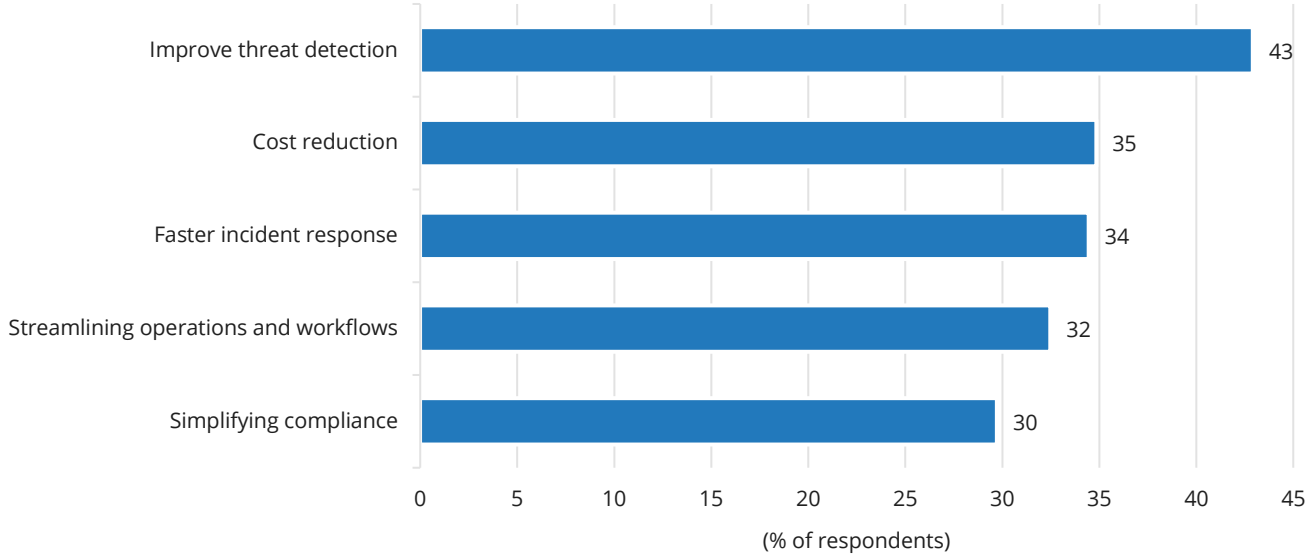
Traditionally, it has been optional for cloud security teams to interface with SOC analysts, who are responsible for triaging and prioritizing alerts and risks. CNAPP can move the line from optional to indispensable by providing a direct line of sight for the SOC promoting proactive security and employing reactive when necessary. The following best practices can help organizations make this a reality:

- **Unified security platforms:** Implementing platforms that provide a single pane of glass for both cloud security and SOC operations (This approach ensures that both teams have access to the same data and can collaborate more effectively, optimizing mean time to detect and mean time to respond. Organizations prefer 1 console or dashboard over 10, and vendors have evolved their point products into platforms that are easy to consume and scalable in capacity. Of respondents in IDC's November 2023 *North American Vendors and Tools Consolidation Survey,* 42.9% indicated that improved threat detection is the top objective for security tool consolidation efforts [see Figure 3].)
- **Real-time threat detection and response:** Enhancing CNAPPs with real-time threat detection and response capabilities (This includes integrating advanced threat intelligence and automated response mechanisms to address threats as they occur.)
- **Cross-functional collaboration:** Encouraging collaboration between cloud security teams and SOCs through regular communication, joint training sessions, and shared objectives (This collaboration helps bridge the cultural and operational gaps between the two teams.)
- **Advanced telemetry and analytics:** Leveraging advanced telemetry and analytics to provide comprehensive visibility into cloud environments (This includes using AI and machine learning to identify and prioritize threats, reducing the time to detect and respond to incidents.)
- **Continuous compliance and risk management:** Implementing continuous compliance and risk management practices to ensure that security controls are consistently applied across cloud and on-premises environments (This approach helps maintain a strong security posture and reduces the risk of compliance violations.)

FIGURE 3

Top Objectives for Security Tools Consolidation Efforts

Q. What are the top objectives for security consolidation efforts in your organization?



n = 508

Source: IDC's *North American Vendors and Tools Consolidation Survey,* November 2023

Palo Alto Networks Cortex Cloud: A Unified Security Platform

One example of this emerging integration model is Palo Alto Networks Cortex Cloud. Designed to support the convergence of posture management and operational response, Cortex Cloud reflects many of the principles outlined in this paper. It integrates CNAPP capabilities with detection and response functions traditionally handled by the SOC, helping organizations reduce fragmentation and accelerate decision-making.

How Cortex Cloud Aligns to a Unified SOC Model

Palo Alto Networks has developed Cortex Cloud, a new solution that combines the capabilities of Prisma Cloud and Cortex CDR to provide real-time cloud security.

Cortex Cloud offers a context-driven defense, providing continuous protection from code to cloud to SOC. This platform includes CNAPP capabilities, providing end-to-end cloud security on a single platform.

This integration aims to address the evolving security needs of organizations by offering a holistic approach to cloud security. Further:

- **Unified data intelligence:**
  - **Consolidates security insights:** Cortex Cloud consolidates security insights into a single data plane, providing a unified view of security posture across the entire cloud environment. This consolidation helps in breaking down silos and ensures that all security data is accessible from a central location, facilitating better analysis and decision-making.
  - **Enhanced visibility:** By integrating data from various sources, including cloud workloads, applications, and infrastructure, Cortex Cloud provides enhanced real-time visibility into potential security threats and vulnerabilities, reducing investigation times, prioritizing critical issues, and automating responses.
- **AI-powered detection and response:**
  - **Reduces investigation time:** Cortex Cloud leverages artificial intelligence to prioritize and analyze security alerts, significantly reducing the time required for investigation.
  - **Automates remediation:** The platform includes automated response capabilities that enable rapid remediation of security incidents. Automated playbooks and workflows ensure that threats are addressed promptly, minimizing the impact on the organization.
- **Operational efficiency gains:**
  - **Improved mean time to resolution:** Organizations using Cortex Cloud have reported significant improvements in their mean time to resolution for security incidents. Faster detection and response times lead to quicker containment and mitigation of threats.
  - **Reduced analyst workload:** The automation and AI-driven capabilities of Cortex Cloud reduce manual tasks and alert fatigue. This efficiency helps in managing the growing volume of security alerts without increasing the head count.
  - **Higher incident resolution rates:** With its comprehensive detection and response capabilities, Cortex Cloud has demonstrated higher incident resolution rates.

CHALLENGES/OPPORTUNITIES

Breaking Down Silos Created by Traditional CNAPP Tools

Organizations must take proactive steps to dismantle the silos created by traditional cloud-native application protection platforms. These silos have led to fragmented security operations, where cloud security teams and SOCs operate independently,

resulting in gaps that attackers can exploit. By breaking down these silos, organizations can ensure that security operations are cohesive and comprehensive.

While CNAPPs are essential for managing cloud security posture and compliance, they may not be sufficient on their own. Security needs unification to leverage the myriad benefits it offers, including enhanced visibility, faster response times, and improved threat detection. A unified approach ensures that security measures are consistent across both cloud and on-premises environments, providing a more robust defense against cyberthreats.

CONCLUSION

The End of the Shadow Cloud SOC

The future of security lies in the integration of CNAPP and SOC, working together as one unified system. This approach combines the strengths of CNAPPs in managing cloud security posture with the real-time detection, investigation, and response capabilities of SOCs. By unifying these functions, organizations can achieve significant improvements in their security operations, including:

- **Enhanced threat detection:** A unified system provides comprehensive visibility into both cloud and on-premises environments, enabling more effective threat detection.
- **Faster response times:** Integration of CNAPP and SOC ensures that security teams can respond to threats more quickly, reducing the window of opportunity for attackers.
- **Improved collaboration and accountability:** A unified approach fosters better collaboration between cloud security teams and SOCs, leading to more coordinated and efficient security operations by ensuring one security command center across the cloud and enterprise.
- **Stronger security posture:** By leveraging the combined capabilities of CNAPP and SOC, organizations can achieve a stronger and more resilient security posture, capable of defending against the evolving threat landscape.

In conclusion, the end of the shadow cloud SOC requires a concerted effort to unify cloud security and SOC operations. By breaking down silos, integrating cloud security as a core SOC function, and adopting a unified CNAPP + SOC approach, organizations can enhance their security posture and better protect against cyberthreats.

ABOUT 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, IT benchmarking and sourcing, 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. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2025 IDC. Reproduction without written permission is completely forbidden.