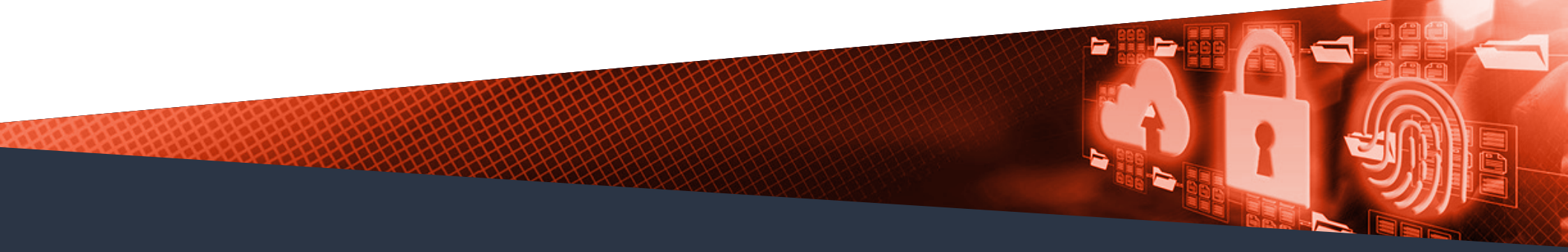

The Code to Cloud to SOC Continuum:
An Architectural Mandate for Resiliency in the Age of Agentic AI

November 2025 EMA White Paper
By **Christopher M. Steffen**, CISSP, CISA, CCZT, VP of Research
Information Security, Risk, and Compliance Management

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

The evolution of cloud-native security culminated in the Cloud-Native Application Protection Platform (CNAPP). CNAPP successfully resolved point solutions' internal fragmentation by consolidating posture management, vulnerability scanning, and workload protection into a unified suite. However, this success inadvertently masked a critical external architectural vulnerability: CNAPP operates in isolation from the enterprise incident response ecosystem—namely, the security operations center (SOC), SIEM, and XDR platforms.

This siloed approach is obsolete, especially given the hyper-speed and sophistication of adversarial operations driven by agentic AI. The resulting response deficit—characterized by extended mean time to detect (MTTD) and mean time to respond (MTTR)—is no longer an inefficiency, but a catastrophic systemic risk. The only path to resilience is mandatory architectural convergence: the Code to Cloud to SOC blueprint. This model requires a unified, real-time data fabric that seamlessly connects CNAPP's deep context with the SOC's behavioral threat intelligence, transforming security from fragmented risk management into a unified, high-velocity continuum.

The Evolution of CNAPP: From Fragmented Tools to Integrated Platform

The genesis of the CNAPP was a direct reaction to the chaos of early cloud security. Organizations attempting to secure cloud-native environments were burdened by a complex, fragmented collection of point solutions: cloud security posture management (CSPM), cloud workload protection platforms (CWPP), and cloud infrastructure entitlement management (CIEM). This proliferation of single-purpose tools led to massive operational overhead, integration challenges, and gaping visibility blind spots.

The CNAPP Mandate and the Progression of Capabilities

The aim of the CNAPP platform was to consolidate these disparate security and compliance controls into one unified platform. This represented a necessary operational imperative, providing security teams with a singular, end-to-end risk management suite.

Modern CNAPP platforms have achieved significant success by integrating security across the entire development, deployment, and runtime lifecycle. The progression of CNAPP capabilities highlights its strength as a proactive, shift-left platform.

- **Posture Management and IaC Scanning:** Policies are enforced early, embedding security directly into CI/CD pipelines. CNAPP natively incorporates IaC scanning to detect vulnerabilities, secrets, and misconfigurations within template code before deployment.
- **Vulnerability Scanning and CWPP:** It provides continuous scanning for vulnerabilities within container images and virtual machine workloads, along with runtime protection against known and zero-day exploits.
- **CIEM and Runtime Security:** It extends to cover identity risk, ensuring least-privilege policies are enforced and monitoring entitlements. Crucially, contemporary CNAPP solutions have extended to incorporate runtime security with some detection capabilities, identifying deviations in application behavior.

Despite its comprehensive integration within the software development lifecycle (SDLC), the CNAPP remains an island in the wider security enterprise. It is still operating in isolation from the incident response ecosystem, including the SOC, SIEM, SOAR, and XDR platforms. This separation creates a fatal flaw in the detection and response chain that automated threats are now exploiting.

Understanding the Current Market: The State of Cloud Security Today

To understand the current failure point, we must first recognize the strengths and weaknesses of the current CNAPP-centric model.

What Works Well: CNAPP's Strengths

The core value of CNAPP is unambiguous. It successfully delivers prevention and deep visibility into the cloud environment's posture, which is essential for compliance and hygiene.

- **Risk Prioritization:** CNAPP excels at correlating configuration data (CSPM) with workload data (CWPP) to prioritize risks based on exploitability, runtime reachability, and asset criticality.
- **Misconfiguration Remediation:** It directly addresses the primary vector of cloud breaches. Notably, approximately 65% of all cloud security incidents are attributed to misconfiguration or human **error**.
- **Unified Cloud Context:** It provides a single pane of glass for all configuration, compliance, and vulnerability issues across multiple cloud service providers.

What is Missing: The Gaps in CNAPP

CNAPP's focus on posture management inherently limits its effectiveness in real-time incident response.

Fundamentally, CNAPP delivers prevention and visibility, but lacks detection, response, and context sharing required by the high-velocity operations of the SOC. It tells the organization what is wrong (a misconfiguration), but cannot effectively assist the SOC in determining who is currently exploiting it and how to contain it instantly.

Why the Current Approach has Broken Down

The failure of the siloed CNAPP approach stems from a profound misalignment between cloud security teams and the SOC. This friction is now fatal in the context of emerging automated threats. The operational divide manifests across three critical dimensions.

Organizational Issue: Parallel Operations

- Cloud security teams use CNAPP as their primary tool, focusing on configuration and risk management. Their priority is ensuring compliance and fixing posture issues.
- SOC teams monitor enterprise-wide threats via their centralized platforms (SIEM, SOAR, and XDR). They lack native expertise and visibility into the intricacies of cloud-native assets (e.g., specific CIEM roles, API call patterns).

The result is that both teams work in parallel rather than in partnership, leading to friction and delayed incident handoffs.

Technical Issue: Fragmentation of Telemetry

CNAPP typically lacks the capability to deliver a standardized telemetry format that the central SOC platforms can easily consume.

- SOC Alerts Lack Cloud-Native Context: When the XDR platform flags malicious activity, the alert often contains only generic network or host data. It lacks the critical cloud-native context (e.g., the specific cloud account, the over-permissioned IAM role, or the originating IaC template).
- CNAPP Telemetry is Fragmented: The rich contextual data that cloud-native assets generate—such as granular identity and API-level activity that highlights behavioral anomalies—cannot be seamlessly integrated or correlated with traditional security logs by the SOC teams.

Process Misalignment: The Response Deficit

The technical and organizational gaps translate directly into operational drag. The process requires manual cross-checking between disparate tools, leading to:

- Longer MTTD/MTTR. Human-mediated correlation cannot keep pace with modern attack chains.
- Data Fatigue. Teams are overwhelmed by uncorrelated findings, with high-fidelity alerts lost in the noise of non-contextual warnings.
- Difficulty Tying Incident to Root Cause. The time lag makes it nearly impossible to instantaneously tie an active runtime incident back to its originating IaC vulnerability or configuration flaw.

Enter Agentic AI and Automation

The structural friction has become a significant risk with the emergence of agentic AI in the adversary's toolkit.

- Compression of Breakout Time: The average breakout time (the window between initial access and lateral movement) for interactive intrusions now averages around 80 minutes, with some attacks progressing much faster—sometimes in less than 30 minutes, and in certain cases, attackers have been able to exfiltrate data in under one **hour**.
- Automated Contextual Exploitation: Agentic AI can rapidly ingest and understand the context misconfigurations (CNAPP data) and behavioral anomalies (SOC data) provide, automating the exploit chain. It excels at entitlement chaining, rapidly leveraging a complex series of over-privileged cloud roles to achieve high-value access, far exceeding the speed of human analysis.

Since up to 82% of all data breaches involve **data stored in the cloud**, the current siloed security model is fundamentally incompatible with the speed and complexity of the AI-driven threat environment.

A Path Forward: From Code to Cloud to SOC

To counter threats that operate at machine speed, security must operate at machine speed. The necessary blueprint for enterprise security demands a code to cloud to SOC continuum, moving beyond a product strategy to an architectural mandate.

The Ideal Platform is Unified, Real-Time Convergence

The ideal platform must be a unified, real-time mechanism that connects development code, runtime data, centralized response systems, and contextual awareness. The key enablers of convergence are:

- Shared Data Fabric for Bidirectional Data Exchange: This is the most critical technical mandate. Security data, including deep CNAPP context (CIEM roles, IaC scanning results), must be instantly accessible and correlated by the SOC's XDR/SIEM layer. Furthermore, the SOC's active threat signal must loop back to the CNAPP to prioritize remediation based on a true active threat.
- Better Telemetry: CNAPP must evolve into a cloud context broker, generating and standardizing high-fidelity, actionable telemetry specifically for the SOC. This includes runtime telemetry that highlights behavioral anomalies at the API and identity level, not just configuration changes.
- Context Mapping (Semantic Context Exchange): The unified system must automatically connect the missing pieces, linking a runtime identity-based alert (from XDR) to the originating IaC template that created the over-privileged permission (from CNAPP). This connection transforms noise into actionable, contextualized intelligence.

The Benefits of Convergence

The fusion of CNAPP's risk data with SOC's threat data delivers profound operational advantages.

- Unified View of the Threat Environment: Security teams gain seamless end-to-end visibility, eliminating the need for manual cross-tool checks.
- Enhanced Detection and Fewer False Positives: Contextual data from CNAPP allows the SOC to triage alerts with high fidelity, drastically reducing alert fatigue.
- Faster Incident Response (Lower MTTR): The integration enables closed-loop response automation, allowing SOAR playbooks to launch simultaneous, cross-platform containment actions. For instance, an active threat that XDR detects can instantly trigger a CNAPP control to revoke an identity's excessive cloud permissions.
- Accelerated Containment: Organizations that implement security automation and AI are shown to **contain breaches 80 to 100 days faster**.

Recommendations/Strategic Implications

The shift from a siloed CNAPP model to the code to cloud to SOC continuum requires an organizational, process, and technology pivot.

Strategic Imperatives for the C-Suite

- Mandate Operational Convergence: Leadership must recognize that the failure is organizational, not technological. Mandate the technical integration of CNAPP and SOC platforms as a Level 1 strategic objective. Demand a unified SecOps model that forces collaboration between cloud security, development, and SOC teams.
- Prioritize Context Over Volume: Shift investment away from products that merely generate more alerts toward solutions that enable semantic context exchange—fusing cloud asset criticality with active threat signals for true risk-driven prioritization.
- Invest in Automation: Fund the development of robust SOAR playbooks that utilize CNAPP's rich context to execute simultaneous, cross-platform remediation actions (e.g., automatic revocation of permissions and workload isolation).

Operational Guidance for Practitioners

Achieving high-velocity cloud defense requires a unified strategy across practitioner teams, ending the traditional security silo.

- The cloud security teams (CNAPP owners) must initiate the convergence by standardizing and exporting their high-fidelity context—including identity exposure (CIEM), asset criticality, and infrastructure as code (IaC) lineage—directly into the central SIEM/XDR platform. This action is the foundation for enabling contextualized threat hunting and rapid incident triage by all parties.
- The SecOps/SOC teams then build upon this foundation. Their imperative is to develop advanced XDR detection rules and SOAR playbooks that explicitly consume and require this new CNAPP context before escalating any alert. This fusion of threat signal and asset risk dramatically reduces false positives and significantly accelerates the mean time to respond.

- Development/DevOps teams must complete the loop. They integrate CNAPP/XDR findings directly into their IDEs. If a vulnerability is exploited in production, the developer receives an immediate, contextual notification identifying the specific line of code or IaC template responsible. This integration ensures closed-loop remediation, effectively shrinking security debt and embedding security directly into the development lifecycle.

Failure to execute this convergence is not a technical oversight; it is a strategic miscalculation that fundamentally undermines enterprise resilience against the machine-speed adversary.

Conclusion

The prevailing CNAPP architecture, while highly effective for posture management and "shift-left" prevention, operates in a perilous isolation from the security operations center. This paper demonstrates that this organizational and technical silo creates an unacceptable response deficit—a fatal vulnerability when facing hyper-automated attacks driven by agentic AI. The speed of compromise, now measured in minutes, renders manual cross-checking between CNAPP and SOC systems obsolete, leading to extended mean time to respond.

To establish enduring resilience, organizations must adopt the code to cloud to SOC blueprint. This requires a mandatory architectural convergence achieved through a shared data fabric and context mapping, transforming CNAPP into a cloud context broker that feeds real-time identity and configuration data into the SOC's XDR/SIEM platforms. This unified view enables true risk-driven prioritization and, most critically, facilitates closed-loop response automation. By fusing preventative controls with real-time detection, the enterprise gains the necessary speed and context to contain threats instantly, pivoting security strategy from fragmented risk identification to a seamless, high-velocity continuum. Failure to make this shift from product-centric CNAPP reliance to architectural convergence is a strategic miscalculation.

EMA Perspective

The cybersecurity industry faces a dangerous illusion: the belief that comprehensive cloud defense is achieved primarily by deploying an advanced Cloud-Native Application Protection Platform (CNAPP). At EMA, we assert this is a strategic miscalculation. CNAPPs are essentially risk management tools—great for cloud hygiene, managing misconfigurations, and tracking vulnerabilities—but they are not complete, real-time detection and response engines.

This narrow focus has led to a structural vulnerability: the cloud security silo. Specialized CNAPP teams operate separately from the central security operations center.

This structural gap has become catastrophic with the advent of generative AI in adversarial toolkits, which radically accelerates attack velocity from hours and days to minutes and seconds. When threats move at machine speed, the traditional, manual process of an alert traveling from the CNAPP to the cloud team, then being manually escalated to the SOC, introduces an unacceptable response deficit. This human-mediated handover is the primary failure point in modern cloud defense, leaving siloed organizations incapable of containment before compromise.

The only viable countermeasure is the immediate and comprehensive integration of CNAPP capabilities directly into the SOC's operational framework. This requires a semantic context exchange in which the CNAPP acts as a cloud context broker, enriching every SOC alert with real-time data on asset criticality and identity exposure (CIEM-derived). This unified view fuses the active threat signal (from the SOC) with asset criticality (from the CNAPP), enabling true risk-driven prioritization.

Most critically, convergence must enable closed-loop response automation. An integrated SOAR engine must be able to launch simultaneous, cross-platform containment actions, such as revoking over-privileged cloud permissions (a CNAPP control) at the moment a workload is isolated (a traditional SOC control). The challenge is organizational, demanding a unified cloud SecOps model to secure the enterprise in the AI-accelerated threat landscape.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT research and consulting firm dedicated to delivering actionable insights across the evolving technology landscape. Through independent research, market analysis, and vendor evaluations, we empower organizations to make well-informed technology decisions. Our team of analysts combines practical experience with a deep understanding of industry best practices and emerging vendor solutions to help clients achieve their strategic objectives. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com**

4638.111825