Breaking Barriers in Enterprise Security

An Executive Guide to Cloud Security and SOC Convergence

Security teams face increasing complexity as they defend their organizations from advanced cloud-based threats. Operational silos divide application security (AppSec), cloud security (CloudSec), and security operations (SecOps) teams, each working with separate tools, workflows, and data sources. The resulting barriers hinder collaboration and delay incident response.

CloudSec teams, for example, detect a vulnerability in cloud infrastructure but lack the runtime context to determine its active exploitation. SecOps analysts monitor alerts without visibility into the cloud services and applications they're protecting. Meanwhile, AppSec teams remain disconnected from risks that materialize in production.

As attackers move between cloud infrastructure, enterprise systems, and application layers, these divides give them the advantage. In today's landscape—with 80% of medium, high, and critical exposures occurring in cloud environments[1]—manual workflows and disconnected tools are liabilities.

Organizations need a new approach to security—one that breaks down artificial barriers between AppSec, CloudSec, and SecOps. By unifying data, automating workflows, and leveraging AI-driven insights, security teams can gain shared visibility, enabling teams to detect, investigate, and respond to threats with the same agility that attackers use to exploit these divides. Drawing from the same intelligence, they can respond faster to incidents and reduce risk across the enterprise.

> An AI-driven security operations platform, built on unified data and automation, elevates security from reaction to prevention.

Challenges in Modern Cloud Security

Cloud-native environments introduce challenges that traditional security tools and workflows aren't equipped to address:

- **Visibility gaps**: Siloed teams and disjointed tools obscure critical data. Without unified monitoring, AppSec loses sight of postdeployment risks, CloudSec loses time attempting to correlate runtime activity, and SecOps can't consolidate signals into actionable insights.
- **Shared responsibility**: Unclear boundaries between cloud providers and internal teams delay incident response. Analysts spend valuable time identifying ownership, increasing risk during critical incidents.
- **Dynamic environments**: Ephemeral cloud resources and rapid deployments create an ever-shifting attack surface. CloudSec teams face challenges tracking assets, and AppSec teams risk introducing misconfigurations in the push for speed.
- **Risk prioritization**: Cloud environments generate thousands of alerts, making prioritization difficult. AppSec rarely prevents issues, cloud posture complexity overwhelms teams, cloud runtime remains too sparsely deployed, and SOCs lack the visibility, AI, and automation needed for near-real-time threat response.
- **Access management**: Proliferation of identities across tools and platforms leads to inconsistent policies, redundant controls, and a heightened risk of unauthorized access or privilege escalation.
- **Configuration management**: Misconfigurations remain a top cause of incidents. AppSec's insecure defaults, compounded by CloudSec's configuration drift, create blind spots that leave SecOps chasing alerts without full context.
- **Attack path analysis**: Massive amounts of telemetry obscure critical risks. Teams need tools to consolidate data and identify potential breach paths, from vulnerabilities in development pipelines to cloud runtime exploitation.

Mapping the Fault Lines in Cloud-Scale Complexity

The challenges outlined above aren't isolated. Risk prioritization failures impact all teams as visibility gaps create issues from development to runtime. Cloud ecosystems have outpaced traditional security, a shift best understood by examining its effects.

[1] *Unit 42 Attack Surface Threat Report 2023*, Palo Alto Networks, September 2023.

The Visibility Crisis

Consider a typical scenario: Your security team receives an alert about suspicious activity in a cloud workload, exposing critical visibility gaps:

- **The SOC team** reviews the alert but is unaware of how the threat originated, whether from a vulnerability in a serverless function, misconfigured API, or unencrypted S3 bucket.
- **The application security team** lacks context from the ecosystem, which prevents them from recognizing a recurring issue and addressing it in code.
- **The cloud security team** faces an overwhelming volume of vulnerabilities and misconfigurations. Without runtime data correlated with SOC insights, they can't readily differentiate exploitable risks from theoretical ones.
- **The cloud posture management team** opens a security ticket, but partitioned workflows prevent clear ownership and follow-through.
- **Development teams** deploy new code without visibility into active threats, inadvertently replicating vulnerabilities across the environment.
- **Manually coordinating between these teams** slows investigations, leaving critical gaps that attackers exploit.

Lacking intel and communication isn't just inefficient—it's dangerous. The time spent solving for inefficiencies allows attackers to move laterally, escalate privileges, and exfiltrate data before security teams act.

91%

of organizations say the number of tools they use create blind spots that affect their abilities to prioritize risk and prevent threats.[2]

The Resource Drain

The operational burden of managing fragmented security tools impacts every team:

- Tool sprawl from reactive solutions—everything from secret detection to vulnerability management—creates overlapping capabilities while compounding inefficiencies.
- Teams manually correlate data across disconnected platforms, delaying investigations and responses.
- Training requirements multiply as each tool demands expertise, straining resources.
- Redundant solutions and integration efforts consume budgets without delivering unified outcomes.
- Misaligned workflows leave vulnerabilities unresolved. SOC analysts, for example, risk application disruptions when addressing cloud issues, while development teams prioritize deploying new code to grow the business.

The Growth Paradox

As organizations use AI to accelerate software development, the limitations of siloed security tools intensify:

- Disconnected workflows fail to keep pace with AI-driven attacks and development velocity, overwhelming teams with risk alerts and uncoordinated responses.
- Tools designed for specific tasks struggle to integrate into a unified security posture.
- Fragmentation stifles innovation, sidelining secure practices and frustrating development teams who view security as an obstacle rather than a partner in progress.

86%

of DevOps view security as a gating factor hindering software releases.[3]

[2] *The State of Cloud-Native Security Report 2024*, Palo Alto Networks, May 15, 2024.

[3] Ibid.

Evolving CNAPP: Closing Security Gaps for Modern Environments

The cloud security market has progressed from cloud security posture management (CSPM) to full-suite cloud-native application protection platforms (CNAPPs). CNAPPs introduced advanced capabilities like container security, data protection, and cloud infrastructure entitlement management (CIEM).

As cloud environments grow more complex, the CNAPP must continue to evolve. Its ongoing effectiveness relies on advancements addressing three key areas:

- **Limited threat context**: Current CNAPP solutions lack integration with essential telemetry sources like endpoint detection and response (EDR), application security, and threat intelligence platforms. Without this context, teams must manually correlate signals, delaying investigations.
- **Constrained automation**: CNAPPs excel in cloud-specific tasks but can't orchestrate responses across the broader security ecosystem. The resulting gap delays containment of threats that move between development pipelines, cloud workloads, and on-premises systems.
- **Incomplete attack chain visibility**: Attacks can start outside the cloud and pivot through cloud resources to impact multiple environments. CNAPPs are purpose-built for the cloud layer and can't account for indicators of compromise occurring beyond their scope.

When investigating an active breach, security teams must manually request access and context from cloud teams—an intermediary step that is dangerously inefficient. Meanwhile, cloud teams lack the sophisticated detection, investigation, and response capabilities found in modern SOC solutions.

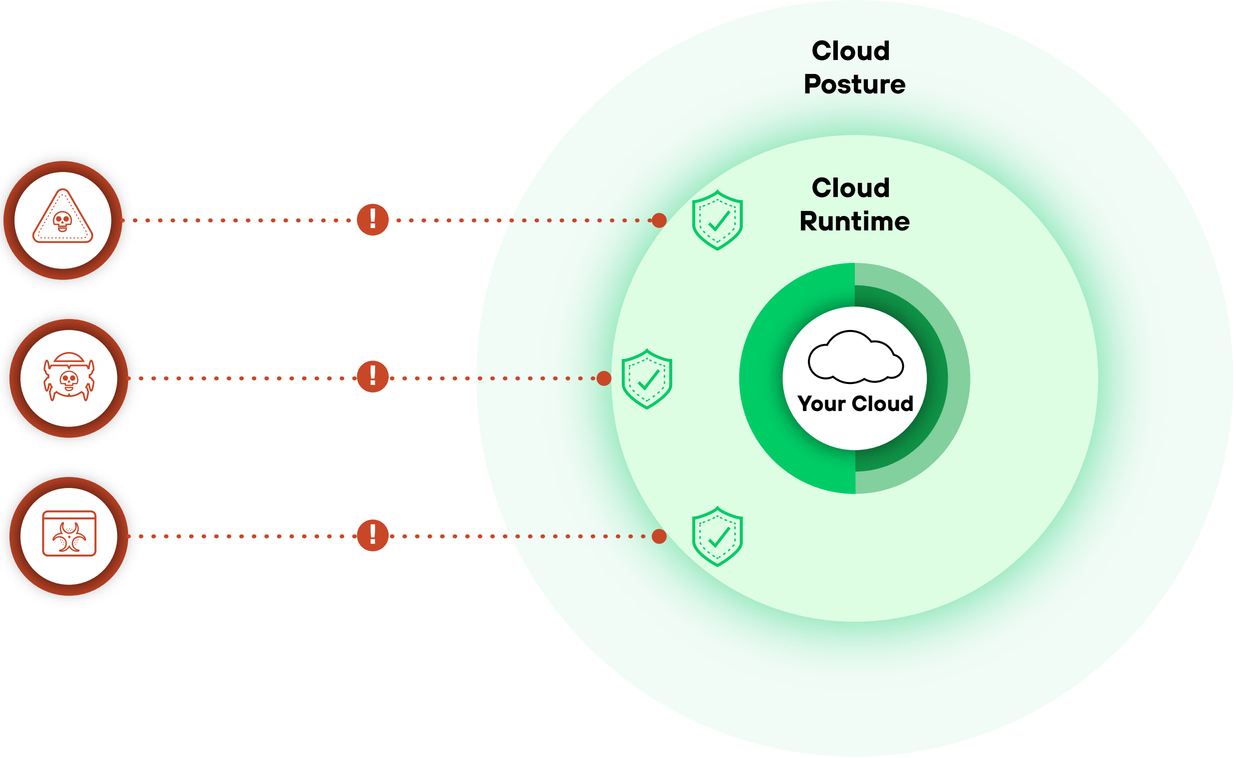

Figure 1: Dynamic cloud environment protection must go beyond posture and evolve with the threat landscape

Toward a Unified Security Foundation

Addressing today's security limitations requires a number of optimizations across three areas:

Application Security

- Strengthen contextual awareness of vulnerabilities as they progress from development to runtime.
- Improve cross-team visibility by integrating application security insights with runtime data for more accurate prioritization.
- Enhance guardrails to adapt dynamically to evolving threat patterns during development.

Cloud Posture Management

- Deepen integration of posture management tools with runtime threat indicators to better prioritize risks.
- Address gaps in misconfiguration remediation workflows to prevent operational delays.
- Strengthen the connection between posture enforcement and real-time threat visibility.

Cloud Runtime Security

- Advance detection capabilities by correlating runtime signals with upstream application and cloud data to uncover complex attack chains.
- Bridge the gap between cloud runtime threat detection and automated, ecosystem-wide remediation.
- Expand visibility into hybrid environments, capturing interactions between cloud-native resources and traditional infrastructure.

While CNAPPs are highly effective at cloud-specific security functions, they perpetuate operational silos at a critical juncture when organizations need visibility and integrated response capabilities across their entire attack surface. In fact, 94% of organizations seek a centralized security solution spanning all their cloud accounts, and almost as many (93%) want cloud and application security unified with traditional network security,[4] highlighting the urgent demand for a more cohesive approach.

A Vision for Modern Security Architecture

For security leaders, the challenge isn't choosing between features—it's designing an architecture that eliminates silos and delivers end-to-end visibility.

By unifying data from code to cloud to runtime, organizations can break down operational barriers, prioritize risks with deep context, and coordinate responses across their ecosystem.

The advances in the modern attack surface require moving beyond isolated tools toward an integrated solution that empowers teams to prevent, detect, and respond to threats with precision and speed.

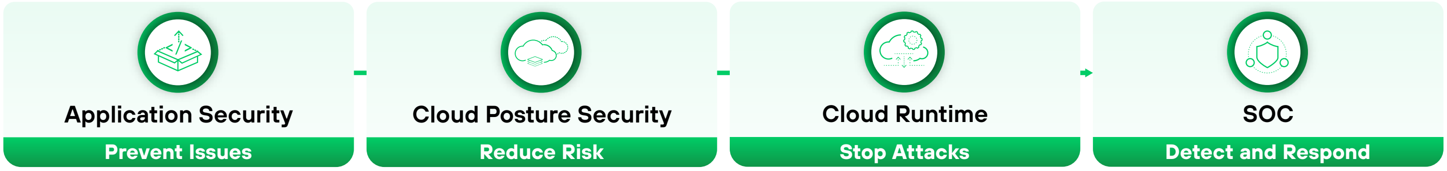

Figure 2: Cybersecurity layers offer stronger defenses, less risk exposure, and faster mitigation

[4] *The State of Cloud-Native Security Report 2024*, Palo Alto Networks, May 15, 2024.

Attack Chain Visibility from Code to Cloud to SOC

Modern security threats often begin with code vulnerabilities that manifest in cloud environments before impacting broader enterprise security. **Data, AI, and automation** present the solution to transforming operations—powering a shift from reactive defense to proactive, adaptive protection.

An AI-driven security operations solution, built on unified data and automation, elevates security from reaction to prevention. By ingesting and analyzing data across code, cloud, and security operations, AI can identify attack paths, prioritize critical risks, and recommend precise remediation actions.

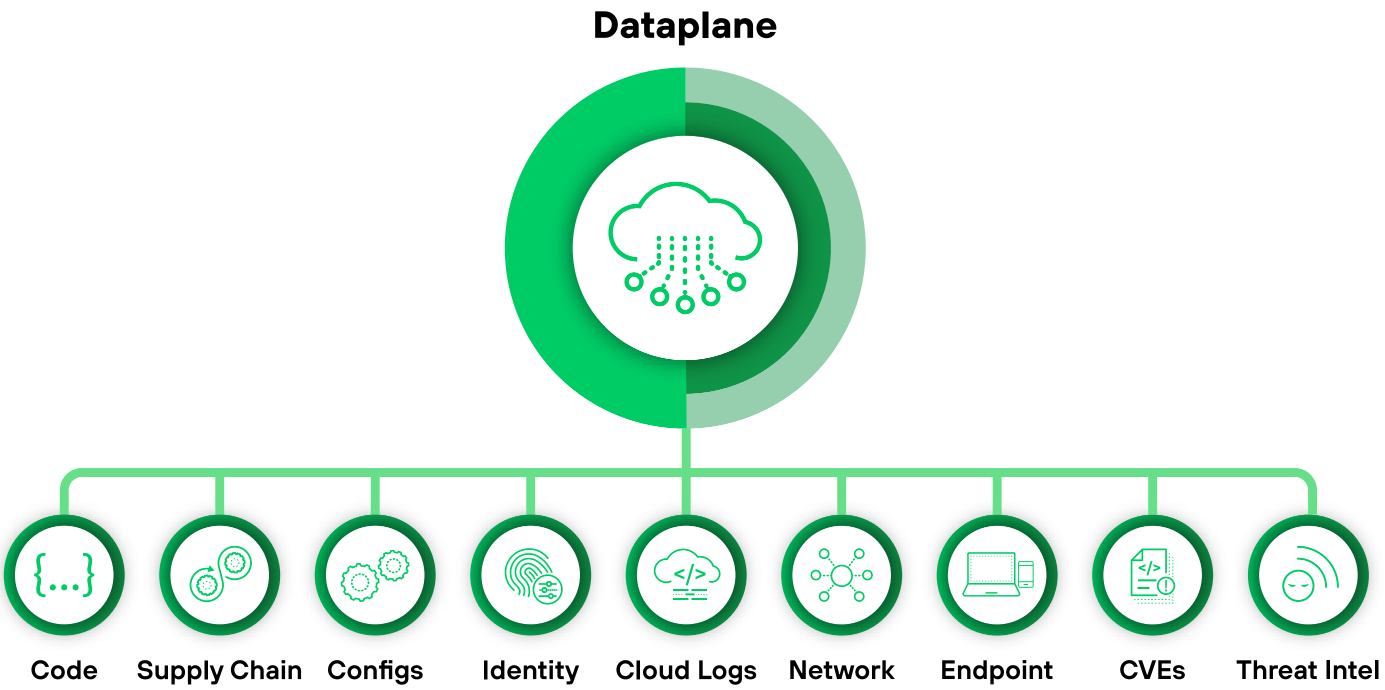

Figure 3: Dynamically stitched data enables teams to scale prevention, detection, and response

When an incident occurs, AI correlates signals across the environment to show the complete attack story—from initial code vulnerability through cloud exploitation to broader impact. More importantly, AI can predict potential attack paths before attackers exploit them.

An intelligence-driven approach fundamentally shifts security left. Rather than simply responding to incidents, organizations can prevent attacks, automatically identifying and fixing their most critical vulnerabilities.

What's more, AI continuously learns from each incident, improving its ability to predict and prevent attacks while automating routine security workflows across cloud and security operations. This represents just one of the transformative capabilities that only a unified, AI-driven approach can deliver.

1 > Code Vulnerability

Cloud Exploitation < 2

3 > Broader Impact on Org

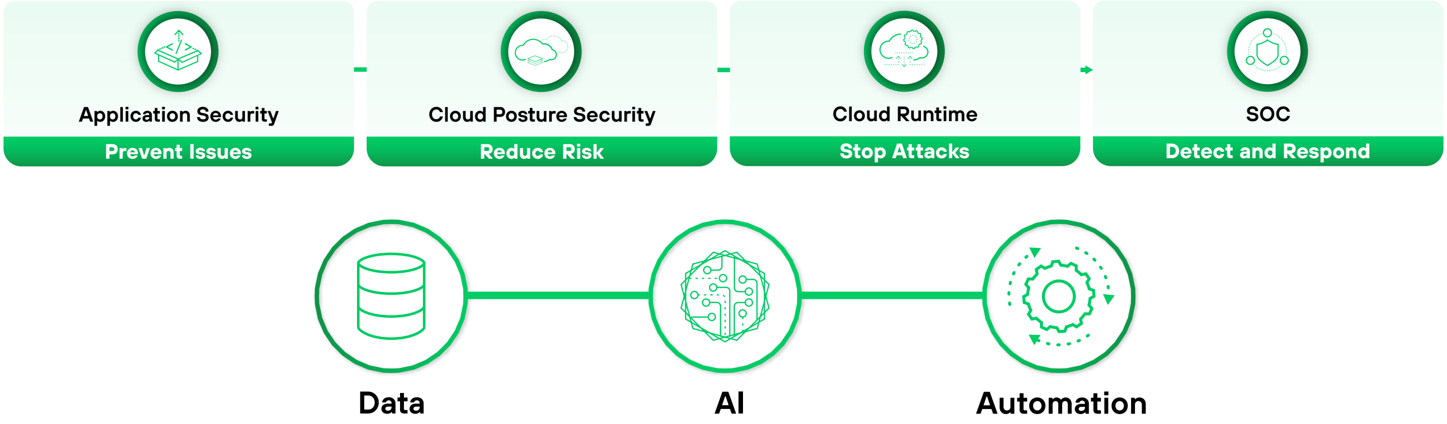

Figure 4: Centralized data powers AI-driven security, automating defense across the security lifecycle

The Automation Challenge

Traditional response playbooks don't translate to cloud environments where "containment" means code and configuration changes. Cloud security demands a new approach. While organizations have invested in security automation, they lack three strategic capabilities:

- **Intelligent incident prioritization**: Leveraging AI to stitch related alerts, attack paths, and vulnerabilities into prioritized action plans, showing teams exactly what needs attention first and why.
- **Cloud security workflow automation**: Bringing enterprise-grade security automation to routine cloud security tasks that consume DevOps' time, streamlining everything from compliance checks to configuration management.
- **End-to-end remediation orchestration**: Automating response actions across the full environment—from immediate runtime responses in cloud and SOC to fixes in code and cloud infrastructure—all orchestrated by clear prioritization and remediation guidance.

The difference between a contained threat and a full-scale breach hinges on time. Without comprehensive automation, organizations incur delays while teams shift through data and coordinate remediation across tools and teams.

Step back and reevaluate: Does your current security stack equip you to effectively respond to security incidents, or does it put your organization at risk?

90% of security teams need more automation for risk prioritization.[5]

92% say cloud security needs out-of-the-box visibility and risk prioritization filtering.[6]

93% want a solution that automatically finds interconnected vulnerabilities and misconfigs with a high potential for successful attacks.[7]

[5] *The State of Cloud-Native Security Report 2024*, Palo Alto Networks, May 15, 2024.

[6] Ibid.

[7] Ibid.

Bridging the Security Gap with Cloud Detection and Response

Emerging as a critical capability for modern security operations, cloud detection and response (CDR) provides security teams with deep visibility into cloud-native applications, automated threat detection, and coordinated response capabilities across cloud environments.

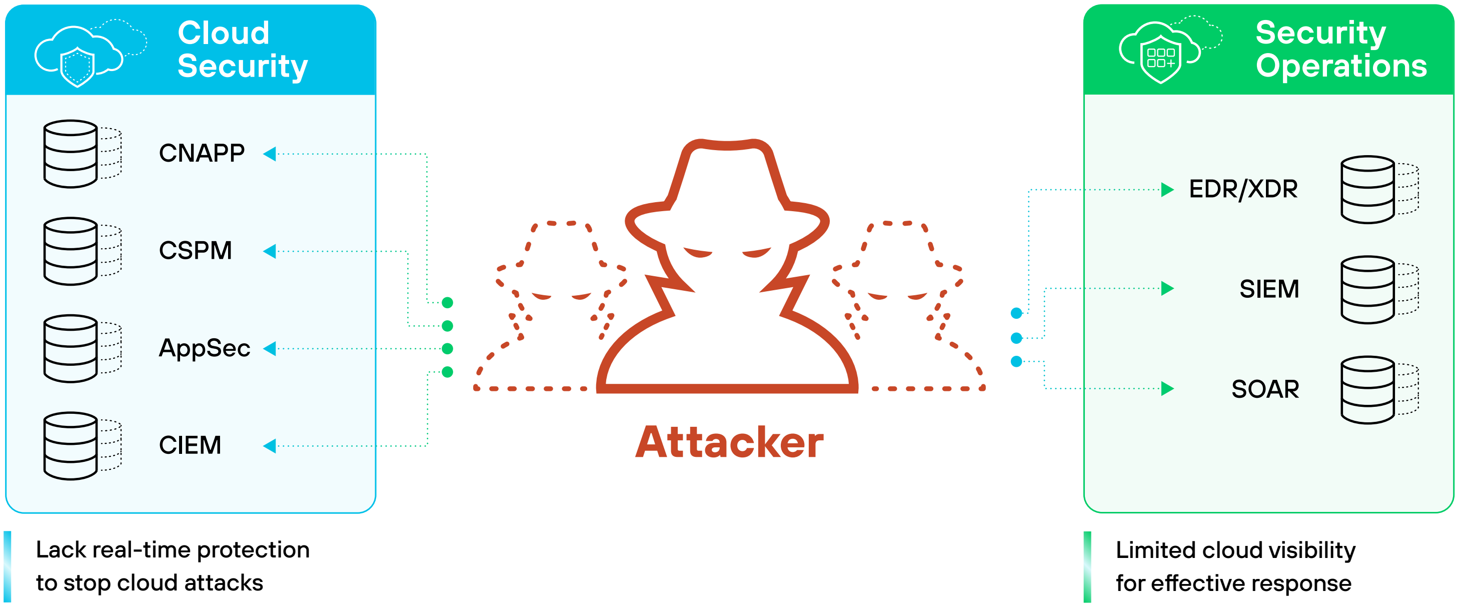
Cloud Security
CNAPP
CSPM
AppSec
CIEM
Attacker
Security Operations
EDR/XDR
SIEM
SOAR
Lack real-time protection to stop cloud attacks
Limited cloud visibility for effective response

Figure 5: Silos create blind spots and delays, leaving organizations vulnerable to cloud attacks

CDR enhances the ability of security teams to detect sophisticated threats, streamline incident response processes, and proactively defend against potential breaches. By providing a comprehensive view of cloud activities and integrating advanced analytics, CDR empowers CloudSec and SecOps to act swiftly and effectively.

Key CDR capabilities in a unified solution enable security teams to:

- Detect threats across multicloud environments in real time.
- Stop attacks with best-in-class protection across clouds.
- Prioritize and investigate incidents by correlating cloud activity with enterprise-wide security events.
- Automate response actions through prebuilt playbooks.

Consider Real-World Scenarios Where CDR Proves Transformative

Scenario 1: Detecting Credential Abuse

When unusual authentication patterns emerge in cloud workloads, CDR automatically:

- Identifies anomalous access patterns across cloud services.
- Correlates activity with known threat actor behaviors.
- Provides immediate context about affected resources and configurations.
- Triggers automated response actions to contain potential compromise.

Instead of spending hours manually gathering data from multiple sources, security teams can immediately understand and respond to the threat.

Scenario 2: Container Security Incident

When malicious activity is detected in a containerized environment, CDR enables teams to:

- Instantly trace the container's history and configuration.
- Understand the blast radius of potential compromise.
- Identify similar containers that might share vulnerabilities.
- Deploy automated quarantine actions while preserving forensic data.

The automated response prevents the "turn it off and on again" approach that often destroys valuable forensic evidence. Through these capabilities, CDR transforms how organizations detect and respond to cloud threats, eliminating the manual correlation and delayed response times that characterize traditional approaches.

The Unified Advantage: Integration as Strategy

The answer to the cloud's diffuse challenges doesn't involve more tools. It asks us to rethink security, to break down longstanding barriers between application development, cloud security, and operations. Traditional CSPM functions, while crucial for cloud hygiene, become vastly more effective when integrated into a comprehensive solution.

By stitching together data from code to runtime to SOC, a unified platform enables teams to identify misconfigurations, connect them to real attack patterns, and automate responses across cloud and traditional infrastructure.

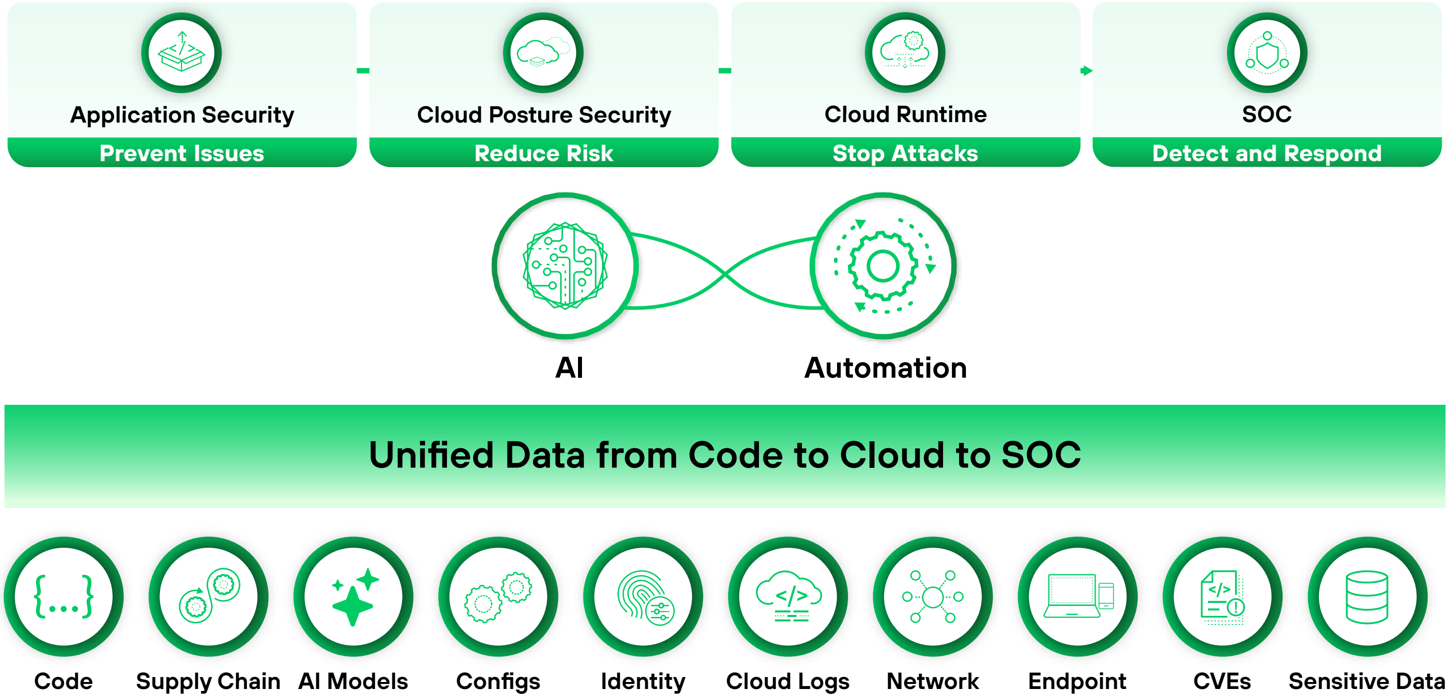

Figure 6: AI-driven security offers full context across AppSec, CloudSec, and SecOps

A unified approach transforms security operations by providing full visibility and control, operational efficiency at scale, and business acceleration.

Unified Visibility and Control

When powered by comprehensive data, AI, and automation, integrated solutions deliver:

- **Proactive application security**: Context-aware guardrails identify and prioritize vulnerabilities throughout development, reducing risk before code reaches production.
- **AI-powered runtime prevention**: Tools like the Cortex XDR® agent provide unparalleled cloud runtime protection, achieving perfect efficacy in MITRE ATT&CK® testing.
- **Cloud detection and response**: AI-driven prioritization and investigation rapidly detect and mitigate attacks, automating remediation across the enterprise.
- **Streamlined DevSecOps**: Integrated automation capabilities eliminate manual workflows and enable fixes across code, cloud posture, and cloud runtime environments.
- **Generative AI-powered productivity**: GenAI copilots accelerate workflows, boosting collaboration and efficiency across teams.

Operational Efficiency at Scale

An integrated solution delivers measurable operational benefits:

- 90% of alerts resolved through automation, dramatically reducing the manual workload.
- Lightning-fast threat detection and response: 10-second MTTD and 1-minute MTTR (respond).
- Efficient incident management with 5-hour MTTR (resolution).
- Significantly reduced training overhead as teams operate on a unified code to cloud to SOC solution.

Business Acceleration

Most importantly, a unified solution empowers organizations to move faster with less risk:

- Accelerated deployment of new cloud services with comprehensive visibility and built-in security.
- Lower total cost of ownership by consolidating tools and reducing operational complexity.
- Enhanced productivity across application, cloud, and security teams, enabling secure innovation at scale.

Making the Strategic Choice

As you evaluate your cloud security strategy, consider these key questions:

Operational Impact

1. How much time do your teams spend switching between security tools?
2. What is the real cost of maintaining multiple security tools?
3. How quickly can you respond to and remediate cloud threats?

Risk Management

4. Do you have complete visibility across your cloud infrastructure?
5. Can you correlate threats across endpoint and cloud environments?
6. How effectively can you enforce consistent security policies?

The Path Forward

The choice between cloud security point tools and an integrated solution isn't just about features—it's about your organization's future, a more secure future. While individual solutions may offer impressive capabilities, they tend to perpetuate the problems they're trying to solve: complexity, fragmentation, and inefficiency.

A strategic centralized approach enables organizations to:

- Transform thousands of alerts into prioritized incidents through AI that automatically correlates signals across code, cloud, and SOC.
- Scale security operations through intelligent automation that orchestrates workflows across both routine cloud security tasks and incident response.
- Enable AI-powered threat detection and response by leveraging telemetry across the entire attack surface.
- Drive consistent, automated remediation from a single solution spanning cloud runtime, security operations, and cloud infrastructure changes.
- Optimize security investments by consolidating tools and enabling AI and automation to handle routine tasks.

The most successful organizations are moving beyond point tools to embrace the unified security model. To evaluate whether a unified approach is right for your organization:

- Assess your current security operations and integration pain points.
- Calculate the total cost of your existing security tools and operations.
- Consider a pilot program to validate solution benefits.
- Develop a transition strategy that minimizes operational impact.

The future of cloud security isn't about having the most tools—it's about having the right strategy.

Key Takeaways

1. The expanding cloud attack surface complicates visibility challenges and security workflows, requiring organizations to reevaluate their current security approaches.
2. Comprehensive visibility and integrated response capabilities across the entire attack surface are pivotal to effective security.
3. CNAPPs excel at cloud-specific security functions but can perpetuate operational silos, limiting holistic security efforts.

Without AI and automation drawing from a single dataplane, and AI, organizations can't align AppSec, CloudSec, and SecOps teams to operate effectively. By addressing these challenges, organizations can reduce friction, improve collaboration, and secure their environments in real time—without compromising development speed.

Ready to Imagine the Possibilities?

Contact us to discover how a unified security strategy can empower your organization to outpace modern threats—or **schedule a demo of Cortex Cloud today**. Explore the power of **platformization**.

3000 Tannery Way
Santa Clara, CA 95054

Main:	+1.408.753.4000
Sales:	+1.866.320.4788
Support:	+1.866.898.9087

www.paloaltonetworks.com

cortex_breaking-barriers-in-enterprise-security_022125