FROST & SULLIVAN

Code-to-Cloud-to-SOC: Reimagining the Next-Gen Cloud Security Operations

By Anh Tien Vu, Principal Industry Analyst, Security
Supporting Analyst Jarad Carleton, Global Research Director, Security

FROST & SULLIVAN EXECUTIVE BRIEF

Sponsored by paloalto NETWORKS

frost.com

CONTENTS

SOC Transformation in the Cloud & AI-Native Era: From the Visibility Trap to Explainable Security

Executive Summary

As cloud adoption surges, cloud security has become an integral part of an enterprise's total cybersecurity strategy. However, despite significant investment in cloud security tools, such as CNAPP, CSPM, CWPP, and other seemingly vital security tools, enterprises are struggling to improve their cloud security operations.

False positives, irrelevant alerts, fragmented visibility, and alert fatigue have made it clear that today's cloud security tools are falling short, particularly for cloud threat detection and response. Research shows that despite widespread adoption of cloud security tools, the mean time to detect (MTTD) and mean time to respond (MTTR) to cloud have not meaningfully improved in the past five years.

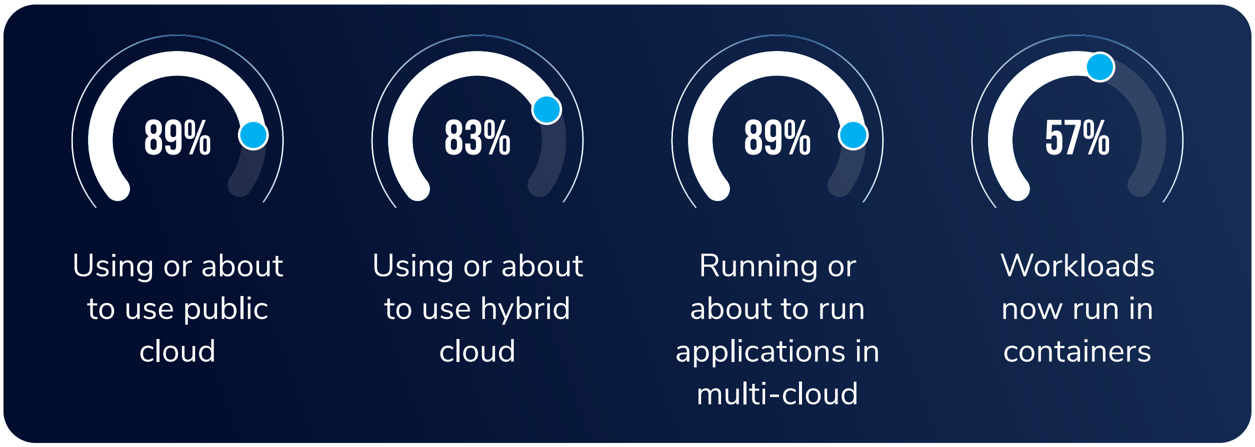
What began as an effort to improve visibility and posture management has, in many cases, delivered the opposite outcome. Large organizations now operate complex, disconnected security ecosystems where cloud security runs independently from SecOps and security operations center (SOC) activities. This separation leaves SOC analysts and SecOps teams blind to active threats in cloud environments and leads to cloud teams operating without the incident-response discipline of SecOps.

Security leaders must eliminate the outdated divide between cloud security and enterprise SecOps and SOC operations. Organizations must move beyond the trap of visibility and focus more on active threat management. The future of cloud security lies in a unified "code-to-cloud-to-SOC" model that covers security across code, cloud, and operations under a single, coherent, and explainable security architecture.

Cloud & Cloud-Native Adoption: The Market Reality

The push for stronger cloud security strategies is driven by the surge in cloud and cloud-native adoption. Cloud is no longer a trend; it is the operating fabric of modern business (Exhibit 1). Multi-cloud and hybrid cloud use has become standard practice, with enterprises running workloads across AWS, Azure, GCP, OCI and private data centers, multiplying the complexity of monitoring, compliance, and threat response.

Exhibit 1: Cloud-Native Adoption Metrics and Multi-Cloud Penetration (2025)



Source: Frost & Sullivan

In addition, the Cloud Native Computing Foundation study, titled "Cloud Native 2024: Approaching a Decade of Code, Cloud, and Change,"[1] further illuminates the acceptance of cloud native technologies and illustrates how deeply they are woven into daily operations at organizations:

90%
Cloud native adoption hit new height

91%
Organizations use containers in production

91%
Kubernetes use in production

CI/CD
Used in production for most or all applications

This landscape has introduced significant complexity into enterprise security programs, especially cloud security operations, where ownership is fragmented across teams. As a result, cloud security can no longer function as a standalone IT function focused only on posture and risk management. Ownership must shift into SecOps, integrating infrastructure, workload, and application protection into a single operational discipline.

1 https://www.cncf.io/wp-content/uploads/2025/04/cncf_annual_survey24_031225a.pdf

Current State of Cloud Security

Traditional SecOps and SOC teams are unprepared, overwhelmed, and ineffective at handling novel cloud threats because they lack the right tools and platforms.

1. In the early days, they worked within predictable, on-premises environments.
2. They handled logs that arrived in familiar formats, playbooks were reliable, and the daily queue of security tasks was more easily managed.
3. As organizations lifted workloads into the cloud, predictability vanished and turned that earlier era of security into an immensely more difficult management challenge.
4. CloudTrail JSON logs replaced firewall events, and each cloud provider introduced unique telemetry formats.
5. Security Information and Event Management (SIEM) platforms designed for thousands of events per hour now face millions of events per minute, driving up storage costs and analyst fatigue.
6. Cloud-native technologies, including containers, Kubernetes, serverless functions, and CI/CD pipelines, introduce transitory workloads and new blind spots.

Together, these changes mark a clear break between traditional SOC predictability (Exhibit 2) and modern cloud-native volatility (Exhibit 3).

Exhibit 2: The Earlier Era: Predictable SOC Telemetry and Response

Predictable Device Logs

- Logs from servers, workstations, and network devices streamed to centralized collectors
- Every asset had a predictable IP address, hostname, and physical location

Structured SIEM Analysis

- SIEM systems efficiently processed structured logs with known formats
- Correlation rules were stable, leading to manageable false positives

Clear Incident Response Workflows

- Step-by-step procedures worked seamlessly in static environments
- “isolate the infected host” often meant simply unplugging a network cable - a clear and effective action

Familiar toolkits

- EDR on endpoints, NDR for networks, SIEM for correlation, and SOAR for automation

Exhibit 3: The New Era: Cloud-Native Chaos and Transient Workloads

Ephemeral Workloads & Kubernetes

- Applications now lived in ephemeral containers that spun up and disappeared in seconds
- Traditional host-based monitoring became obsolete when the “host” was a concept, not a physical machine

CI/CD Pipeline Complexity

- Code now moves from development to production through automated CI/CD pipelines, adding speed and complexity
- Infrastructure defined in YAML files via GitOps left SOC teams unsure how to monitor IaC they couldn’t see

Emerging AI-Native Attacks

- Machine learning models, vector databases, and LLM APIs introduced entirely new categories of threats
- Prompt injection attacks weren’t in any traditional security textbook

Source: Frost & Sullivan

In addition, the “shared responsibility” model, intended to clarify cloud risk ownership, often led to shared blame due to blurred boundaries, intertwined misconfigurations, exposed APIs, and fragmented accountability, leaving SOC teams struggling to respond while attackers exploited the seams.

Meanwhile, the explosion of specialized tools—such as cloud security posture management (CSPM), cloud workload protection platforms (CWPP), cloud infrastructure entitlement management (CIEM), data security posture management (DSPM), SaaS security posture management (SSPM), static application security testing (SAST), software composition analysis (SCA), and infrastructure as code (IaC) scanners—created an alphabet soup of point solutions, trapping organizations in the misguided belief that all of it would help improve their cloud security operations through visibility, posture management, and threat detection and response.

More than 80% of organizations have at least 3 cloud security tools.[2] However, most of these were developed as separate, IT-owned functions to help developers, DevOps engineers, and risk and governance teams, all of which are disconnected or irrelevant for vital SecOps/SOC team functions.

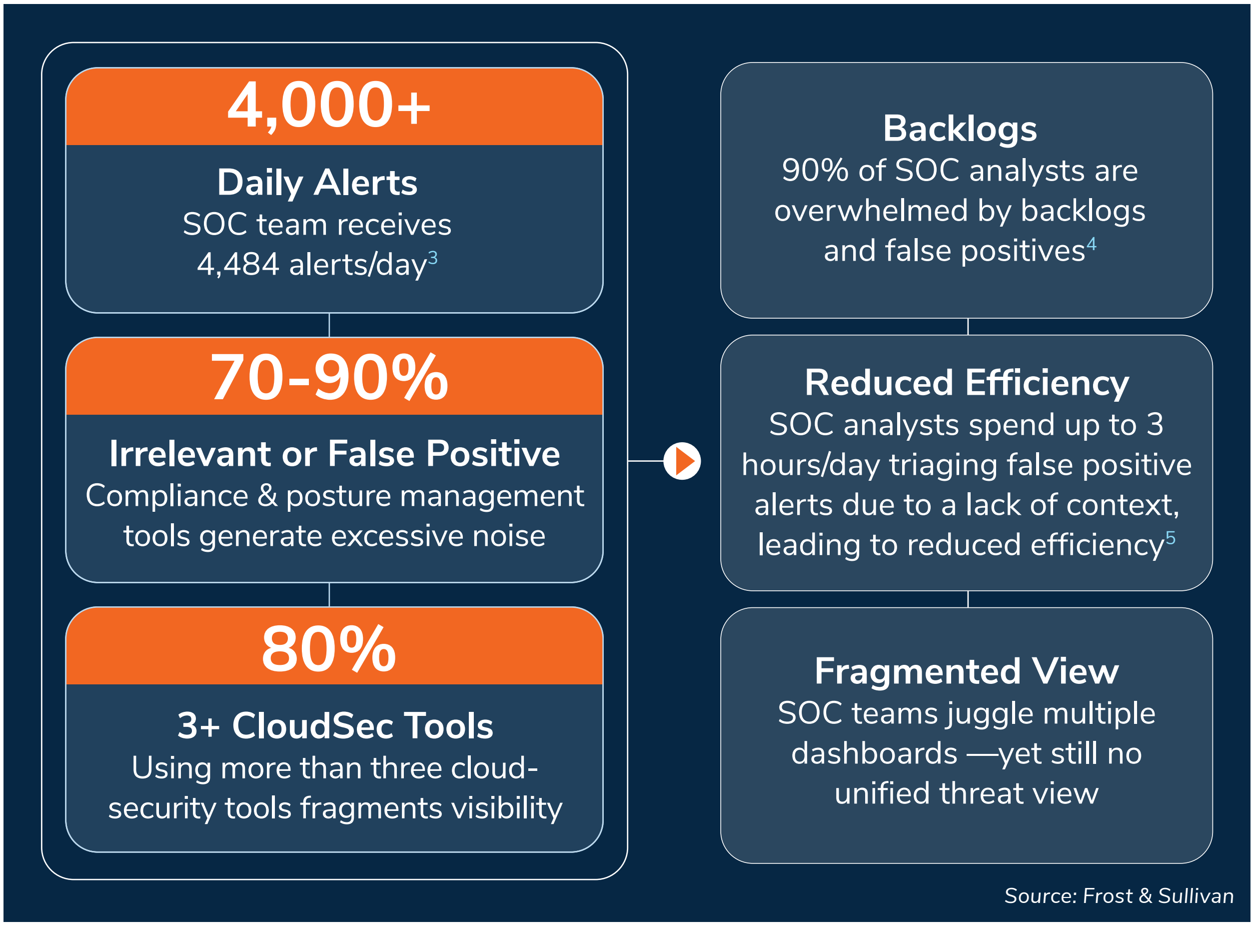
2 Source: Frost & Sullivan

The Inflection Point—Why the Legacy Approach Fails

The fundamental flaw of the legacy SOC model is architectural; traditional SIEMs and correlation engines were never designed for the scale, speed, or dynamism of cloud and cloud-native environments. Fixed IP addresses and packet captures have shifted to ephemeral APIs and short-lived workloads, yet many organizations still rely on tools built for static environments.

While posture-centric cloud security tools improve hygiene and compliance, they deliver limited value to SecOps/SOC teams and have not closed the detection-response gap. Instead of acting as solutions, they are creating more problems for SecOps/SOC teams by flooding them with false positives and irrelevant alerts that drive fatigue and slow investigations and response. Rather than unifying security, these tools leave the SOC navigating a sprawl of disconnected dashboards, each revealing only fragmented data without context and the full story. (Exhibit 4).

Exhibit 4: The Harsh Reality: Tool Fatigue and Reduced Efficiency



3 https://cdn.prod.website-files.com/64e50cbe2b6f932c04238c14/689db628db970401f2bfde5b_6630da12bd1f4ccb222dffea_2023-state-of-threat-detection_comp.pdf
4 https://www.dropzone.ai/blog/osterman-report-2024-soc-trends-challenges-and-solutions
5 https://cdn.prod.website-files.com/64e50cbe2b6f932c04238c14/689db628db970401f2bfde5b_6630da12bd1f4ccb222dffea_2023-state-of-threat-detection_comp.pdf

For years, organizations were told that the answer to cloud security was more visibility; collect every log, store every packet, and assume that volume would translate into insight. Instead, they became mired in a visibility trap: massive data intake with no contextual understanding. The results speak for themselves. Five years of IBM's Cost of Data Breach report data (2021-2025)[6] show no measurable improvement in MTTD or MTTR, as it takes organizations from 8 to 10 months to identify and contain attacks in the cloud—a clear signal that posture-centric tools are insufficient because they lack the runtime context SecOps/SOC teams actually need. Adding more tools has not solved the problem; tool sprawl without integration has fragmented visibility, inflated costs, and reduced operational efficiency, while leaving detection and response performance unchanged.

6 https://liangroup.net/blog/wp-content/uploads/2021/07/Cost-of-a-Data-Breach-Report-2021.pdf
https://www.key4biz.it/wp-content/uploads/2022/07/Cost-of-a-Data-Breach-Full-Report-2022.pdf
https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/07/25111651/Cost-of-a-Data-Breach-Report-2023.pdf
https://cdn.table.media/assets/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf
https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91

The Path Forward: Code-to-Cloud-to-SOC

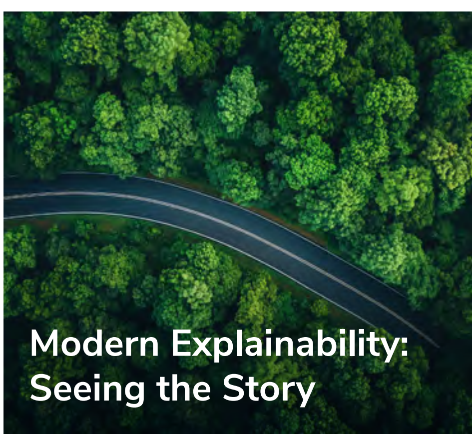
A new cloud security paradigm is emerging—one that unifies protection across the entire application development lifecycle, from development, runtime, and operations into a single SecOps framework. This code-to-cloud-to-SOC model integrates posture, runtime, and threat telemetry across identity, endpoints, networks, applications, cloud infrastructure, and data into a unified data lake spanning every layer in the cloud stack, including application code, build pipelines, cloud-native runtime environments, and SOC detection and response workflows.

Achieving this vision requires a cultural and operational shift. SecOps must move away from cataloging posture noise to identifying active threats, pivoting from risk scores to runtime validation, and from raw visibility to true explainability. Explainable context transforms alerts into coherent attack narratives that reveal not only what happened, but why it matters, how it's progressing, and how to stop it (Exhibit 5). This is the mindset required to close the detection-response gap and adapt security to the speed of modern cloud environments.

Exhibit 5: Modern Cloud Security Enables Seeing the Forest for the Trees

- Traditional SOCs maximized visibility by collecting all logs
- Raw visibility without context causes overload and hides real threats
- Data without context is like staring at trees while missing the forest

Data ≠ Answers.
Context transforms information into intelligence



- Understand why alerts matter and how attacks progress
- Turn raw logs into contextual attacker narratives
- Analysts move from seeing alerts to understanding them
- Shift from data accumulation to threat comprehension for faster, accurate response

Explainability = Alerts turned into attack stories

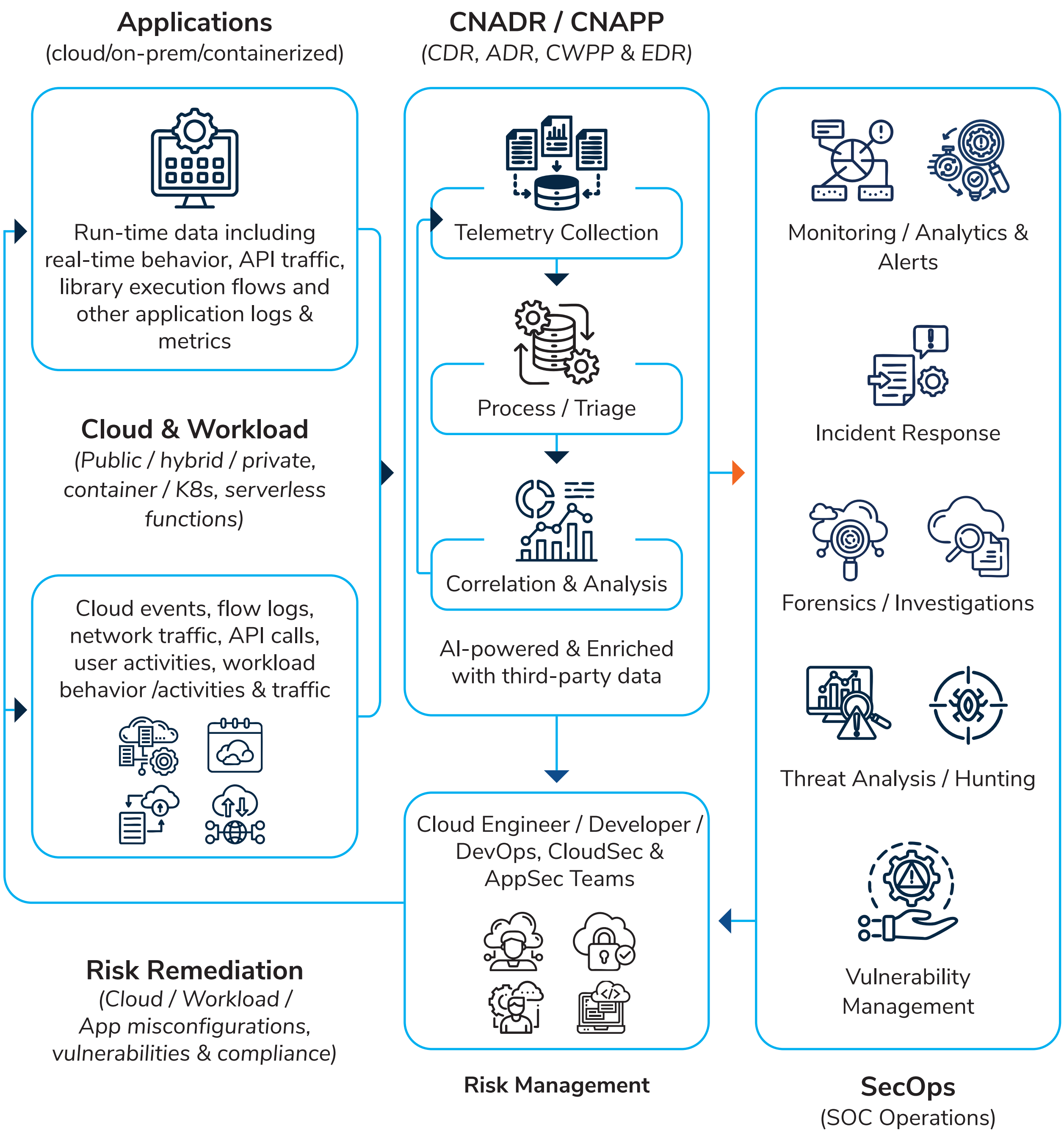
Source: *Frost & Sullivan*

This means moving beyond collecting data and stockpiling logs toward understanding attacks and telling complete attack stories. Context transforms raw information into actionable intelligence, enabling SecOps/SOC teams to focus on the threats that matter the most.

The SecOps team must evolve from reactive alert responders into proactive cloud security partners, working alongside DevOps and platform teams to not just deliver more logs, but real context, and a meaningful understanding of security events.

The centerpiece of this model is Cloud-native Application Detection and Response (CNADR), which shifts enterprises from risk management to true threat detection and response (Exhibit 6). Unlike posture tools that overwhelm analysts with lists of misconfigurations and vulnerabilities, CNADR focuses on what truly matters: active runtime threats. It correlates signals across infrastructure, workloads, and applications, unifying them into a single, real-time attack narrative. CNADR is not about what could go wrong; it reveals what is happening right now in an enterprise's cloud environment.

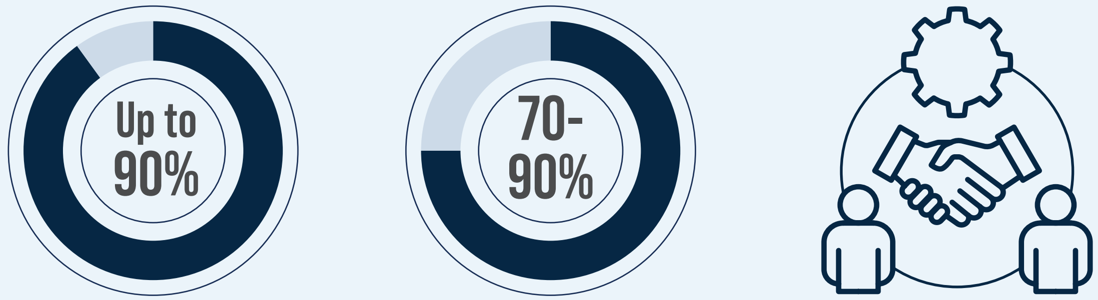
Exhibit 6: CNADR Workflow and Code-to-Cloud-to-SOC Telemetry Flow



Source: Frost & Sullivan

This enables organizations to shift gears by fundamentally changing out-of-date SOC operations drowning in logs to a unified SecOps structure that can explain attacks with the context needed to increase security resilience. The outcomes speak for themselves, as illustrated in Exhibit 7.

Exhibit 7: Runtime Context Improvements for SecOps/SOC Teams



Noise Reduction

Threat-focused alerts instead of posture findings

Faster MTTR

Contextualized attack paths accelerate investigation

Better Collaboration

Improved SOC-DevOps partnership

Source: Frost & Sullivan

The pivot to cloud threat detection and response has required a shift from posture management to runtime security. CNADR sits at the center of this shift, enabling both cloud security and the SOC to evolve from reactive, risk-cataloging functions into teams focused on the few attacks that truly matter, with context, evidence, and collaboration built in.

Strategic Implications for the C-Suite

As enterprises adopt unified SecOps architectures that bridge today's divide between cloud security and SOC operations, the impact goes far beyond technical efficiency. The shift to a *code-to-cloud-to-SOC* model is an organizational transformation that reshapes roles, accountability, and how security creates value.

By connecting security from code creation through cloud runtime to active SOC operations, organizations move beyond visibility and establish security as a continuous business function with shared ownership across the C-suite and Board.

CISOs/CIOs/CTOs:

CISOs and CIOs have become strategic integrators, leading the convergence of DevSecOps, cloud engineering, and SOC operations. Their roles expand from governance, compliance oversight, posture management to leading unified SecOps operations that deliver real-time, code-to-runtime assurance, detection, and response. They play the central role in strengthening DevSecOps culture and improving core security metrics, including MTTD, MTTR, and the speed of risk remediation.

CFOs:

Organizations can lower the total cost of ownership by consolidating platforms and eliminating point solutions, turning fragmented security spending into measurable gains in resilience. Reduced incident recovery costs and unplanned downtime, driven by proactive risk containment and faster response, further strengthen enterprise value. At the same time, integrated performance metrics make security spending more predictable and easier to plan.

Boards of Directors:

The transformation of cloud security allows organizations to shift from treating cybersecurity as a compliance exercise to positioning it as a pillar of resilience and strategic differentiation. Unified SecOps architectures bring transparency and confidence to decisions by linking security telemetry directly to enterprise risk indicators.

This unification strengthens resilience, reduces exposure, and aligns cybersecurity with broader digital transformation goals. A unified SecOps posture reinforces trust, supports compliance, and ensures business continuity.

The Final Word

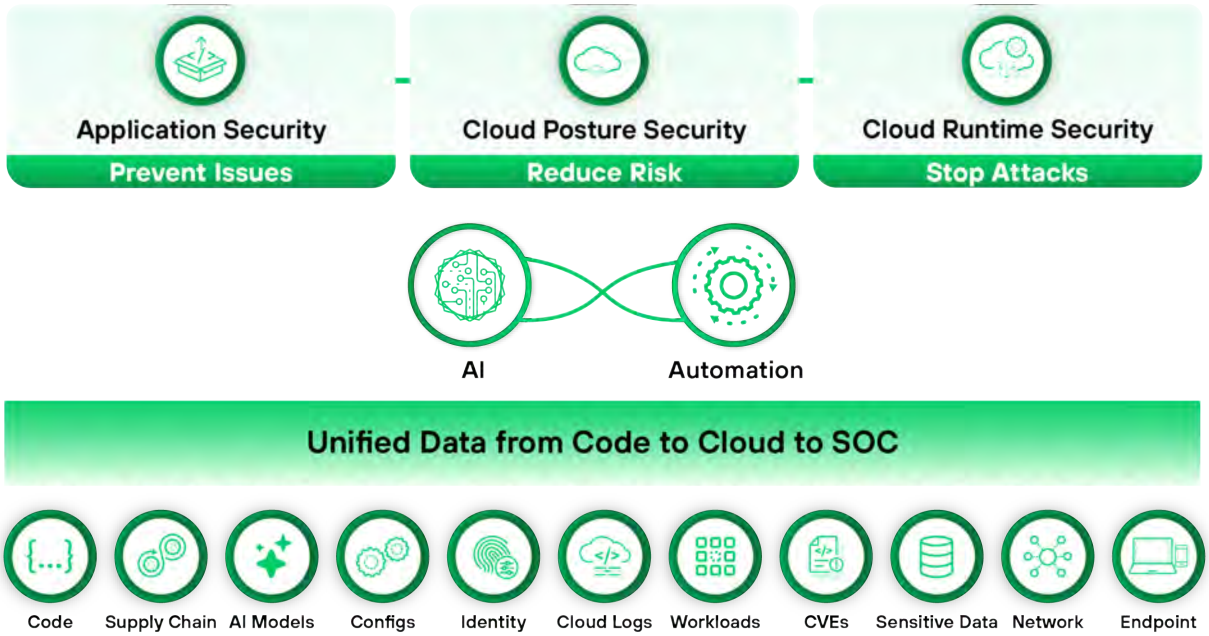
As cloud adoption accelerates, cloud security has become central to enterprise security. But organizations continue to struggle with effective cloud threat detection and response. Despite significant investment in cloud security tools, MTTD and MTTR metrics have shown no meaningful improvement.

The cloud security industry has reached an inflection point. Cloud security is converging toward a unified model that dissolves the boundaries between cloud security and SecOps, prioritizing actual threats over posture noise, explainability over visibility, and unified attack narratives over fragmented views.

Palo Alto Networks' code-to-cloud-to-SOC vision, delivered through its Cortex Cloud platform, as illustrated in Exhibit 8, represents this next stage of cloud security. It provides an explainable, contextual, AI-assisted approach that spans application, cloud posture management, cloud-native runtime security, and SOC-led detection and response capabilities.

Cortex Cloud correlates posture findings and runtime context with threat intelligence across data sensitivity, behavior identification, and external exposure to assess real exploitability. This combined perspective transforms cloud security from a passive risk-cataloguing function into an active component of the enterprise threat detection and response framework, enabling SecOps teams to move from reactive investigation to proactive threat hunting informed by posture intelligence.

Exhibit 8: Palo Alto Networks' Cortex Cloud



Source: Palo Alto Networks

As organizations adopt unified, SecOps-led cloud security architectures, Cortex Cloud reshapes how they operationalize their cloud security end to end. It aligns posture management and enterprise detection and response, spanning from code repositories, build pipelines, production infrastructure, and to SOC workflows, transforming overwhelming alert volume into clear, actionable risk narratives that help teams manage cloud threats with confidence.

YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation?

Join the journey.

FROST & SULLIVAN