kuppingercole ANALYSTS

Commissioned by:

paloalto NETWORKS

# The Future of Cloud Security

Mike Small and John Tolbert

December 19, 2025

As cloud security evolves, integrating Cloud-Native Application Protection Platform (CNAPP) capabilities into the Security Operations Center (SOC) is crucial to enhancing cyber Incident Response (IR). By converging CNAPP with traditional SOC elements, like Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and eXtended Detection and Response (XDR), organizations can streamline detection, triage, and response processes, thus reducing Mean Time To Respond (MTTR) for cloud-origin threats. A unified SOC approach not only amalgamates endpoint, network, and cloud telemetry but also correlates identity-related events, effectively closing gaps that currently hinder efficient battle against cyber threats in multi-cloud environments.

# Contents



# Figures

# Introduction

Cloud security tooling has expanded quickly as CNAPPs have consolidated Cloud Security Posture Management (CSPM), Cloud Workload Protection Platforms (CWPPs), Cloud Infrastructure Entitlement Management (CIEM), and Infrastructure as Code (IaC) scanning into a single control plane. Organizations that have adopted such tools have seen better inventory, policy as code, and misconfiguration detection, which has resulted in better cloud hygiene. Yet a persistent failure mode has surfaced in incident handling: many enterprises operate cloud security as a distinct function, often with a “cloud SOC” separate from the “enterprise SOC” that serves on-premises data centers and networks.

While telemetry from enterprise-owned assets may still funnel into the enterprise SOC for detection and response, lines of authority, personnel, and escalation paths remain fragmented. In high-tempo events, such as the well-known Log4j incident, teams that understand the cloud fabric (accounts, service permissions, workloads, and their owners) are not tightly coupled to the analysts and responders accountable for enterprise-wide containment of such threats. The result is a measurable lag between detection, triage, ownership assignment, and decisive action; MTTR to cloud-origin threats has not improved commensurately with the investment in CNAPP.

> CIOs repeatedly describe CNAPP as “another security stack,” which has led to split monitoring, duplication of case queues, and incompatible or incomplete playbooks.

In practice, this creates four systemic gaps. The first is role ambiguity: who leads when a cloud vulnerability manifests as exploitation across container clusters and identity providers simultaneously? The second is split telemetry: CNAPP findings, Identity and Access Management (IAM) risk signals, and network indicators of lateral movement reach different consoles and ticketing systems. The third consideration is workflow dissonance: cloud administrators, DevOps, SOC analysts, and incident responders do not share a common investigation model or data schema; each team doing only partial investigations and enrichment. Lastly, there are ownership hand-offs: the responsibility for containment actions such as revoking cloud entitlements and OAuth tokens, disabling users or accounts, and stopping/restarting VMs or workloads may lie within different departments. During the Log4j incident, many organizations spent critical hours negotiating who was authorized to implement temporary WAF rules, who could cycle container images, and who owned emergency IAM changes. Business processes as well as technical limitations exacerbated an already tough situation.

The direction that the cybersecurity industry has taken already hints at the remedy. The value of integrating endpoint, network, and cloud telemetry, and acting through a single response fabric is not speculative; it is the explicit trajectory of Network Detection and Response (NDR) and Endpoint Protection Detection and Response (EPDR) toward XDR. EPDR contributes process-level analysis and automated host remediation and containment. NDR brings east-west visibility via encrypted-traffic analysis and lateral-movement detection

where endpoint agents are absent. Both product types describe convergence into XDR as the best way to reduce Mean Time To Detect (MTTD) and MTTR across heterogeneous environments. XDR platforms implement this by unifying endpoint agents, network sensors, and cloud collectors behind one analyst interface and one automation surface, which is precisely the integration missing between cloud SOCs and enterprise SOCs.

In parallel, the cybersecurity industry has realized that identity is the primary attack vector, especially for cloud-origin attacks. Therefore, effective response now requires correlating IAM events such as credential misuse, token replay, role abuse, with host and network signals in the same investigative workflow. Converging identity and security operations measurably shortens investigation cycles by eliminating blind spots and duplicate triage.

This paper examines the claim that the future of cloud security is not merely a better CNAPP, but the integration of security tools and teams to incorporate detection and response to cloud-origin threats into the overall enterprise IR processes. This paper describes the current capabilities and limitations of both enterprise SOC tools and CNAPP, the organization of both types of SOCs, and the requirements for integrating the SOCs. It also examines Palo Alto Networks Cortex Cloud as an example of how to achieve this combination. The paper concludes with general recommendations for readers on how to move to this integrated SOC architecture.

CNAPP has improved control coverage, but without integrated tools and teams, shared workflows, and a centralized response surface, organizations will continue to experience slow, negotiation-heavy responses to cloud breaches. By redesigning operating models and data flows and optimizing tools to collapse the cloud SOC and enterprise SOC into a single capable organization, security leaders can convert investment in platforms into the only outcome that matters during a cloud incident: faster remediations.

# Highlights

- Enterprise SOC architectures are composed of multiple standard tool types, including EPDR, NDR, XDR, email/web gateways, SIEM, SOAR, and others. Most enterprise SOC tools were designed for on-premises infrastructure. Some of these solutions have overlapping capabilities, but many also fail to address or integrate with cloud security solutions.
- Over the years, many organizations have developed distinct cloud SOCs, which use CSPM, CIEM, and CNAPP solutions. These tools are primarily designed for posture management rather than response orchestration.
- Running dual SOCs takes more effort and results in less effective investigations and slower responses that can increase attacker dwell time, damage, and remediation costs.
- To address these limitations, a next-generation solution must include full integration between CNAPP and SOAR/XDR capabilities.

# Example Incident Scenario

> This scenario illustrates the need for the deep integration of cloud security capabilities from CNAPP into the SOC tooling and processes.

An attacker phishes a cloud administrator's account and gains limited IAM role access in AWS. This scenario is representative of real attacker behavior in well-known cloud compromise narratives (such as credential compromise → privilege escalation → lateral movement → data exfiltration).

- The attacker discovers a misconfigured IAM role "DevOpsBackupRole" allowing access to both Simple Storage Service (S3) and Elastic Compute Cloud (EC2) instances.
- They then use that role to spin up a new EC2 instance in a less-monitored Virtual Private Cloud (VPC), attach an IAM instance profile, and scan internal networks to access databases.
- They extract data from an Amazon Relational Database Service (RDS) instance using that instance's network path.

The IR team receives an alert about a suspicious S3 download from role "DevOpsBackupRole." They begin investigation but cannot see the intermediate EC2 instance route or lateral movement inside VPC because they do not have agent telemetry there.

On the other hand, the CNAPP sees:

- The misconfiguration of DevOpsBackupRole was "high risk" in the cloud security posture,
- That new usage of that role is anomalous.
- That EC2 instance relationships and network paths connect that role to RDS.
- It flags the "risk path" automatically so responders know: Role → EC2 → RDS → exfiltration.

It is only by integrating the cloud security capabilities of cloud security solutions into the SOC that incidents like this will be fully visible to the IR team.

# Enterprise SOC and CNAPP - Current Capabilities and Limitations

> Cloud security must evolve to provide the full context needed to respond to cyber-attacks in today's multi-cloud IT environments. SOCs must fully integrate with cloud services to effectively detect, triage, respond to, and recover from all cyber incidents.

## Enterprise SOC Component Capabilities

**EPDR** combines preventative controls (anti-malware, host firewall, URL, and application controls) with continuous detection and response on endpoints to spot and contain malicious code, suspicious processes, and indicators of compromise that bypass prevention. Mature EPDR platforms support threat hunting, attack timeline reconstruction, remote evidence collection, automated or analyst-driven actions (process termination, and node quarantine and rollback), alignment to MITRE ATT&CK® in the analyst UI, and integrations that stream telemetry to SIEM/SOAR for case management and orchestration. EPDR is the principal endpoint sensor within broader XDR programs.

**NDR** inspects north-south and east-west traffic in on-premises, cloud, and Operational Technology (OT) or Industrial Control System (ICS) segments in order to baseline normal communications and discover anomalies that indicate lateral movement, Command and Control (C2) communication, data staging, or exfiltration, frequently using Encrypted Traffic Analysis (ETA) methods and Machine Learning (ML) detection engines rather than signatures. Sensors can run in-line for active blocking or out-of-band for passive monitoring, with responses including alerting, case generation and enrichment, session termination, and host/subnet isolation; NDR feeds SIEM/SOAR and is usually a primary compensating control where endpoint agents cannot be deployed.

**XDR** unifies endpoint, network, and cloud telemetry and increasingly identity and deception signals into a single correlation and response plane, providing a single investigation console and a single automation surface rather than disjointed point solutions. Architecturally, XDR pairs endpoint agents, network sensors, and cloud collectors/connectors with centralized analytics to accelerate triage, reduce dwell time, and invoke direct controls (similar to what is available in both EPDR and NDR tools) from the same case record. XDR is the market trajectory for converging EPDR and NDR with cloud workload coverage, especially for mid-market companies, Managed Detection and Response (MDR) providers, and Managed Security Service Providers (MSSPs).

**SIEM** aggregates and normalizes high-volume security logs and alerts from firewalls, EPDR, NDR, cloud services, IAM systems, email and web gateways, and other security components to support correlation, historical search, compliance reporting, and SOC case creation. In most enterprises it is the central data lake and alert bus for security tools that downstream solutions such as SOAR and XDR subscribe to.

**SOAR** provides an investigative interface and can execute playbooks that integrate SIEM and other detections, open and update cases, call EPDR to isolate hosts, instruct NDR to block sessions, update firewall rules, and push tickets into IT Service Management (ITSM). Many EPDR and NDR products interoperate with, or delegate complex orchestration to SOAR platforms. Some organizations rely on SOAR and its integrations to drive responses, and in others, XDR is used for automating responses, often also via integrations, particularly in cases where “Open XDR” architectures are employed.

While SOCs have evolved to provide capabilities to detect, investigate and respond to cyber threats as they occur based on threat intelligence, telemetry and security configuration data

from on-premises systems, these are less well integrated with cloud environments and lack similar data for these.

## CNAPP Evolution and Capabilities

All the major cloud services including AWS, IBM, Microsoft Azure, and Google Cloud offer built-in capabilities and services for securing the use of their service. However, these capabilities, user interfaces, and APIs are all different. In response, a market in CNAPPs has evolved to help Infrastructure as a Service (IaaS) tenants and cloud app developers to identify and remove vulnerabilities in their apps and in their cloud configurations. CNAPP solutions help to prevent and protect against cyber threats, to measure security posture, and to demonstrate regulatory compliance. However, they are less helpful in the areas of attack detection and response.

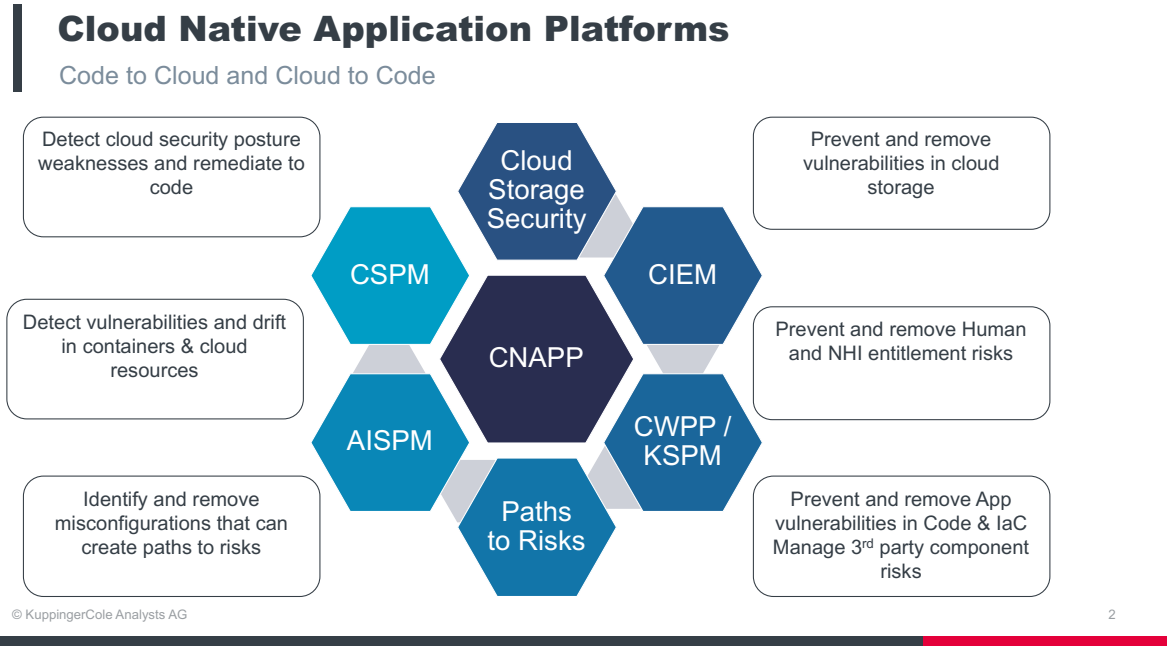


Figure 1: CNAPP - Code to Cloud and Cloud to Code

CNAPP provides capabilities that address the tactics used by cyber adversaries to attack cloud systems. As well as the application code, the cloud resources involved in delivering the application, together with their security controls, are defined in code. CNAPP focusses on DevOps' needs covering preventative security processes (Code to Cloud) as well as in responding to cloud incidents (Cloud to Code) where it may be necessary to change the code.

**Paths to Risks:** CNAPP discovers and analyzes cloud network security controls. It identifies, reports, and remediates potential paths to risks where a combination of weak network controls and excessive entitlements provides a route for an attacker.

**CIEM:** Cloud identity and entitlements represent a significant vulnerability in cloud security. CNAPP discovers and analyzes the user accounts (people and services) with access to the

cloud services and their entitlements. It identifies, reports, and remediates user accounts with excessive or abnormal privileges and other risks, such as orphan accounts (those without owners), as well as accounts with weak authentication policies.

**Cloud Storage Security:** CNAPP discovers and analyzes cloud data storage services to identify, report, and remediate excessive risk. These risks include data storage services without appropriate controls (for example, not encrypted), data storage with public access, and data storage directly exposed to the Internet for the wide range of cloud storage types (File Systems, Object Stores, Databases, and data lakes).

**CWPP:** The configuration of cloud compute services, containers and serverless functions may include excessive entitlements and other vulnerabilities. CNAPP discovers and analyzes these to identify, report, and remediate risks. It also analyzes these elements for risky patch levels, Operating Systems(OSs) and images with unmanaged vulnerabilities, and risky configurations.

**Cloud Container Security:** Cloud apps are mainly developed and deployed using container based microservices. CNAPP discovers and analyses cloud container services to identify, report, and remediate insecure container images, container registries, and deployments for common container environments such as Kubernetes.

**Cloud GenAI Security:** Organizations are increasingly using cloud GenAI services to train, develop, and deploy AI based business services. This creates risks related to the confidentiality of the data used, the provenance of the Large Language Models (LLMs) leveraged as well as technical vulnerabilities. CNAPP discovers and analyzes the technology related risks in these areas.

**CSPM:** This provides capabilities to visualize and report on the cyber risks that have been discovered. This includes surfacing paths to risks that arise from combinations of controls and connections between cloud and app elements.

While CNAPP provides capabilities to detect and respond to incidents within the cloud, it is not integrated with the tools and capabilities provided by a conventional SOC. This separation leaves a fissure in the organization’s cyber security. CNAPP does not take account of the full range of threat intelligence, investigative knowledge, and capabilities provided by the SOC. Equally, the SOC does not see the full picture for cloud-related events or correlate between clouds.

> CNAPP has become a “cloud security” silo that is isolated from the organizational response tools and teams.

## Limitations of Enterprise SOC Tools

> Legacy SIEM/SOAR systems were not built for ephemeral, Application Programming Interface (API)-driven cloud environments, making them inherently reactive rather than adaptive.

Before proposing an integrated operating model, we must acknowledge the structural limits of the current SOC stack, including EPDR, NDR, XDR, SIEM, and SOAR, which collectively expand visibility yet still leave identity-led and cloud-borne incidents stranded in triage queues. IaaS is especially vulnerable to the visibility gaps in enterprise SOC tools. Because of these gaps, IR teams often lack the context to see “which path did the attacker take from a misconfigured role, through a subnet, into a database?”

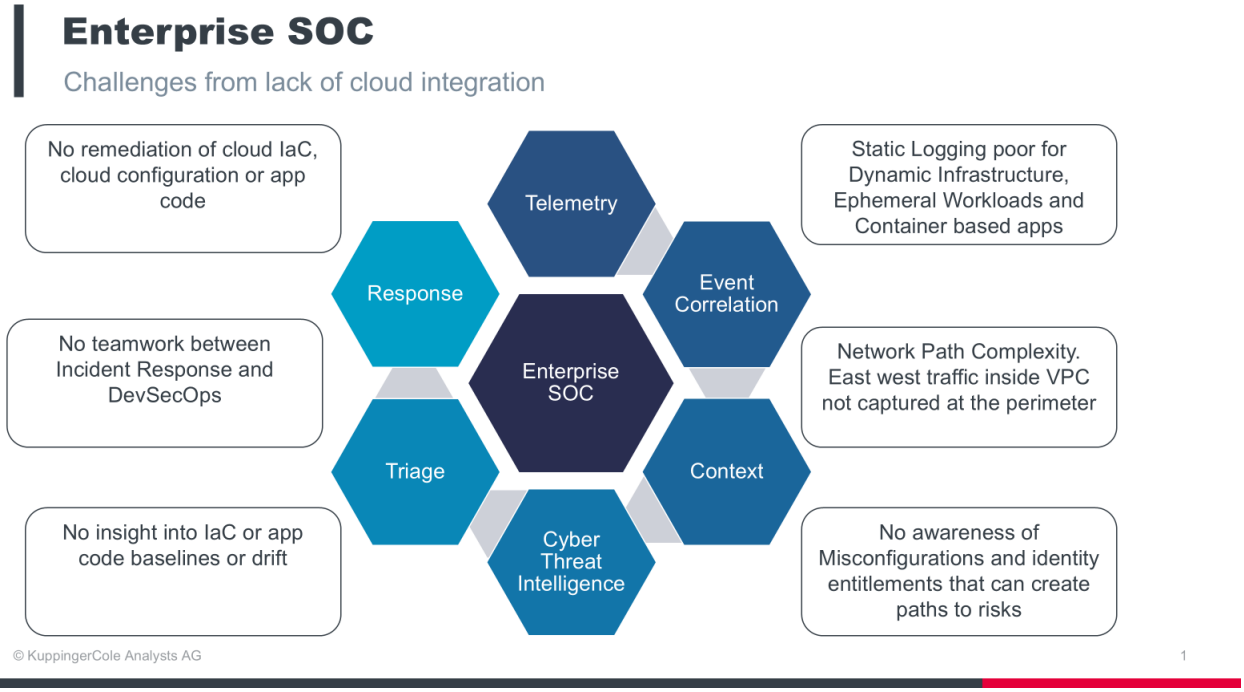


Figure 2: Enterprise SOC challenges from lack of cloud integration

Traditional SIEMs were designed for on-premises log sources (firewalls, servers, and endpoints) and rely on agents or syslog ingestion. Cloud environments generate API-based, event-driven, and service-specific logs such as AWS CloudTrail, Azure Activity Logs, and GCP Audit Logs, for example, which vary widely in format, volume, and semantics. SIEM centralizes event collection and correlation but also concentrates cost and noise in the form of high-volume, weakly contextualized alerts that generate false positives.

Cloud logs are extremely verbose. CloudTrail alone can generate terabytes per day. SIEM licensing is often based on data volume (GB/day), making comprehensive visibility prohibitively expensive. Furthermore, many of the cloud vulnerabilities are related to the entitlements of service elements which can be exploited by attackers, and these activities do not show up in the SOC.

SIEMs aggregate logs but rarely *understand* cloud context, such as the relationships between IAM roles, policies, VPCs, and resources. Most SIEM/SOAR pipelines rely on log forwarding and batch ingestion, often delayed by minutes or hours. In cloud-native attacks, lateral movement and privilege escalation can happen within seconds. Legacy SIEMs depend on static correlation rules, often tuned for on-premises Tactics, Techniques, and Procedures (TTPs) such as port scans, and brute-force logins.

While some modern SIEMs have ML modules, most were trained on network or endpoint data, not cloud telemetry.

SOAR platforms depend on good data and tight API integration with upstream components, otherwise automation fails, and it just becomes yet another pane of glass in the SOC.

SOAR tools can trigger scripted responses (often called playbooks or runbooks) to block IPs or disable accounts, for example, but struggle to act within cloud provider APIs or multi-cloud contexts. They treat each log source as separate. In hybrid architectures, attackers often traverse from cloud identity to endpoint to SaaS and back.

In the cloud dynamic infrastructure, ephemeral workloads such as instances, containers, and auto-scaled groups can appear and disappear, making static logging and fixed alert rules insufficient. Most SIEM/SOAR setups require manual onboarding of new log sources and API connectors. They cannot access telemetry from managed cloud services (such as SaaS APIs, Kubernetes control plane, and serverless).

XDR promises cross-domain correlation and unified responses, yet most offerings vary in their coverage of network and cloud controls and frequently omit the treatment of identity risk signals. Another promise of XDR is the elimination of SIEMs from customer architecture, but this is not often achievable because organizations that are subject to various regulatory compliance regimes still need SIEMs for audit trails. Traditional IR teams often rely on siloed tools: Endpoint Detection and Response (EDR), network Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS), SIEM, and Cloud Service Provider (CSP) logs. XDR integrates these sources into a single correlation layer, so if you only see part of the attacker's trail in one system, XDR can align it with other signals (for example, "IAM role used anomalously in AWS" + "new EC2 process spawn" + "unusual outbound DNS from container"). Once an incident is confirmed, XDR can trigger cross-domain response actions.

East-west traffic inside the virtual network, private link traffic, and service endpoints are often not captured by perimeter network sensors. In addition, some workloads may run without endpoint agents or in isolated networks, making lateral movement invisible to traditional EDR/XDR or network monitors.

Misconfigured security groups, IAM roles, open storage, and network ACLs are the top risks in cloud services. Because the enterprise SOC tools do not have access to this data, IR teams often lack the context to see "which path did the attacker take from a misconfigured role, through a subnet, into a database?"

Many XDR platforms started with EPDR heritage, so their cloud coverage depends on ingesting logs from providers. They do not always model the deep relationships that CNAPPs do (such as IAM graphs and network exposure maps). Licensing and log access issues persist: If the underlying cloud provider restricts audit logs to premium tiers (as in Microsoft's Storm-0558 case), XDR still will not "see" what is not provided. Additionally, EPDR cannot instrument many unmanaged, OT/ICS environments, and ephemeral cloud workloads. This is compounded by the problem that adversaries routinely erase or evade endpoint logs.

# Requirements for an Integrated Cloud and Enterprise SOC

> To address the limitations described above, next-generation cloud security must include full integration between CNAPP and SOAR/XDR capabilities.

A full cloud security solution should provide in-depth IR capabilities based on full visibility of data from CNAPP as well as other relevant sources. This is essential to provide visibility into areas that IR teams cannot get through current SOC tools.

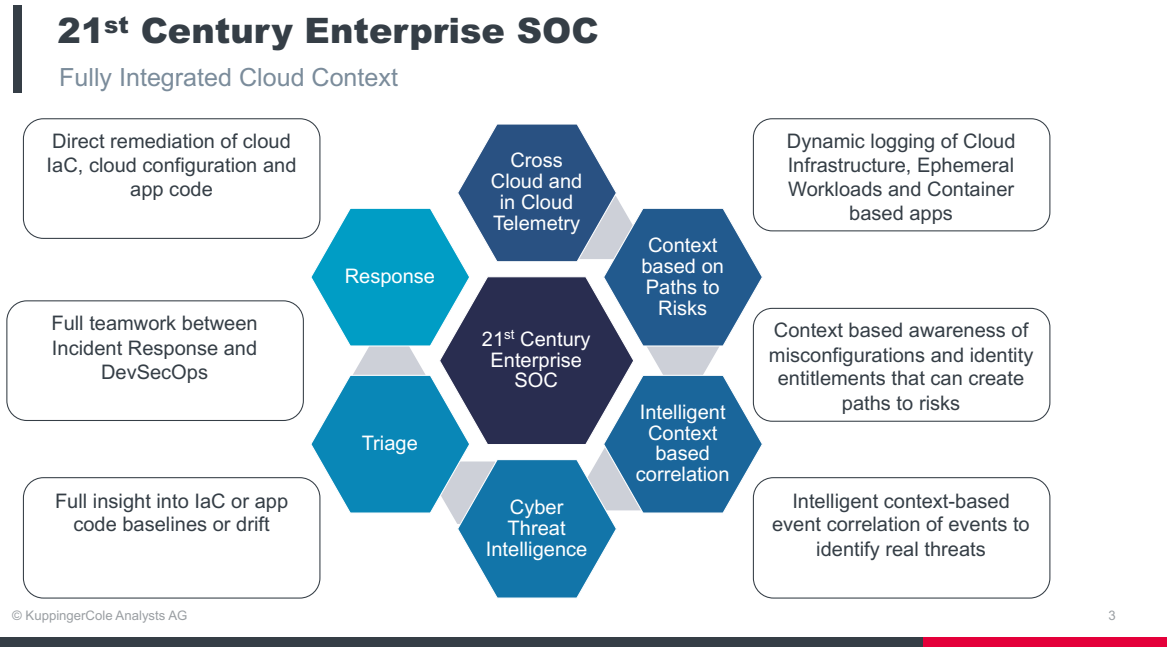


Figure 3: 21st Century Cloud SOC

A full cloud security solution should also include enhanced telemetry ingestion, contextual awareness, real-time analytics, and automated response capabilities. The following list defines key functional requirements that a cloud-ready SIEM/SOAR should meet to enable effective and scalable cloud incident detection and response.

**Unified Contextual Awareness** (Identity, Posture, Network). The solution must maintain a continuously updated asset and identity graph to correlate IAM roles, configurations, and network relationships, and integrate with CSPM/CIEM for attack-path visualization. It should provide a "contextual model" of identity, network, storage, and compute relationships. For example, to trace a path like: "role A -> instance B -> security group C -> S3 bucket D."

**Risk scoring and alert prioritization**. The solution should combine posture, entitlement, vulnerability, and runtime signals, to flag a "high-risk path" proactively before an attacker uses it.

**Cross-layer context.** It should correlate misconfigurations, identity misuse, and runtime anomalies to make the connection between configuration risk and exploit execution visible.

**Historical baselines and drift detection**. The solution should detect configuration drift or anomalous expansions of privileges to alert IR teams before compromise.

**Automated remediation or guardrails**. It should include capabilities to trigger mitigations such as revoking a risky role as well as reporting and enabling manual IR actions.

**Cloud Telemetry Ingestion**. The solution must natively ingest, normalize, and enrich telemetry from all major cloud providers and SaaS platforms. It must also support API-based and event-driven data collection, auto-onboarding of new accounts, and consistent schema mapping across clouds.

**Cost-Efficient Data Architecture**. The solution must implement tiered data storage (hot, warm, and cold) with decoupled ingestion and analytics layers; and enable policy-driven data retention and integration with cloud-native data lakes.

**Real-Time Event Correlation and Detection**. The solution must provide near real-time detection using streaming analytics pipelines with sub-minute latency and correlate ephemeral events across hybrid and multi-cloud workloads.

**Behavior-Based and ML-Driven Analytics.** The solution must use ML models trained on cloud-native telemetry to identify abnormal IAM usage, data exfiltration, and privilege escalation.

**Integrated Cloud Response Automation.** The solution must provide prebuilt SOAR playbooks to automate responses through provider APIs, and enable containment actions such as revoking IAM credentials, quarantining instances, or isolating workloads.

**Cross-Domain Correlation and XDR Integration.** It should correlate cloud events with endpoint, network, and identity telemetry. The solution must integrate bi-directionally with XDR solutions for unified detection and response.

**Cloud-Native Deployment and Elastic Scalability**. The solution must be based on microservices or serverless functions, scaling elastically with log volume, and support multi-cloud deployment with tenant isolation.

**Continuous Threat Intelligence Integration**. The solution must consume cloud-relevant threat intelligence feeds and map Indicators of Compromise (IoCs) to active assets, users, and workloads in real time.

**Compliance, Auditability, and Forensic Readiness**. The solution must support immutable log retention, automated compliance reporting, and tamper-proof evidence collection for investigations and audits.

**Adaptive and Continuous Detection Engineering**. The solution must enable detection covering code pipelines, versioned rule testing, and automated retraining based on analyst feedback or simulation exercises.

**Usable, Analyst-Centric Design**. The solution must provide intuitive dashboards, ATT&CK mappings, and guided investigations. It must also support ChatOps integrations such as Slack, Teams, and others for collaborative response.

# Palo Alto Networks Cortex Cloud

> Palo Alto Networks was founded in 2005 and is headquartered in Santa Clara, California, in the US. The Cortex Cloud platform merges Cloud Native Application Protection (CNAPP) and Cloud Detection and Response (CDR) to bridge the divide between enterprise and cloud SOCs. Cortex Cloud improves SOC efficiency through a centralized analyst interface, policy-driven automation, and prebuilt playbooks that accelerate investigation, detection, and response across customers' assets, on-premises, hybrid, and cloud.

Organizations continue to struggle with fragmented threat detection and response workflows due to the artificial separation of application security, cloud security, and security operations teams. Palo Alto Networks' strategy to unify these traditionally siloed teams under a single platform with a shared data lake and unified risk model remains a consistent architectural thesis in its transition from Prisma Cloud to the Cortex Cloud.

At the core of this integration is the **Cortex Command Center**, a centralized interface designed for situational awareness across environments. It presents animated radar-style visualizations of active threats, open issues, and open cases. Complementing this are indicators such as data ingestion rates (measured in GB/day) and a real-time view of all monitored assets, including those currently at risk.

The top screen within the Cortex Command Center organizes operational domains into discrete sections: Dashboards & Reports, Cases & Issues, Investigation & Response, Threat Management, Posture Management, Inventory, Modules, and Marketplace. These categories reflect both workflows and integration capabilities. Customers can augment native functionality via integrations from the Palo Alto Networks marketplace.

The **Case View** aggregates related security events by correlating multiple detections across sources. Each case header displays metadata (source, timestamp, status, and case ID) followed by alignment to ATT&CK techniques and explanatory narratives. An embedded "Overview" pane consolidates open issue counts, issue sources (such as an XDR agent), affected artifacts, assets (including IPs, URLs, and cloud instances), and automation recommendations derived from curated playbooks.

This case-centric model contrasts with other vendors' single-issue focus. Instead of forcing analysts to resolve 50 discrete alerts linked to one misconfiguration, Cortex Cloud encapsulates such alerts into a single case. This architecture enables analysts to view and act on root causes rather than symptoms.

The issue correlation engine relies on more than 10,000 ML detectors that monitor and analyze artifacts and assets in near real time. These detectors identify similar issues and group them into composite cases, thus reducing alert fatigue and surfacing prioritized risks.

The **Issues & Insights** tab details issue severity, domain (for example, security vs. posture), detection methods (such as IaC scanners, XDR agents, Static Application Security Testing (SAST), and CSPM), and issue categories such as configuration errors, exposed secrets, or

code weaknesses. Analysts without this capability would be required to manually export CNAPP and CSPM outputs and import them into external SOAR tools to achieve comparable visibility.

Selecting an issue within this tab invokes the **Investigation View**, which displays context-sensitive evidence. In one scenario, a misconfiguration flagged by the IaC scanner was displayed with an impact summary, asset inventory, correlated cases, and the triggering policy rule. Analysts may drill into execution steps across hosts, networks, applications, and workloads using the **Executions tab**.

The **Case War Room** facilitates inter-analyst collaboration via a chat interface, augmented by a Cortex bot that parses discussions and enriches them with context where applicable. Analysts can filter the War Room for investigative efficiency. A timeline view of all activities provides an additional layer of temporal correlation.

Switching to the **Modules view**, several specific functional domains are highlighted. Under **Data Security**, the dashboard includes asset breakdowns by type (such as databases, storage buckets, and AI datasets), top unresolved issues, geographic distribution, and pattern matches (for example, email addresses and street addresses). This view extends visibility beyond infrastructure to data-level exposures.

The **Application Security Platform Module** displays issue intake and case output pipelines. Integration points include GitHub, CircleCI, GitHub Actions, AWS, and GCP. It tracks post-guardrail persistence of issues and provides granular telemetry on secrets, IaC misconfigurations, vulnerabilities, and privilege misuse. Examples of IAM related application security issues it can detect, focusing on privilege and secrets management, include excessive permissions, user permission escalation events, and embedded credentials within source files. Additionally, it can detect classic attack vectors such as SQL injections, reverse shells, password spray attempts, and enumeration behaviors.

In isolation, CNAPP, CSPM, and IaC scanners offer value but are constrained by their “peacetime” posture. Their telemetry must be operationalized during live security incidents to realize value. Cortex Cloud addresses this by binding runtime telemetry with design-time analysis and cross-domain issue correlation, which improves detection, investigation, and response under adversarial conditions.

While other platforms operate as loosely integrated collections of tools, Cortex Cloud’s consolidated approach reduces tooling sprawl, enriches threat context, and reduces investigation time by preserving fidelity across application, infrastructure, and operational layers.

The marketplace contains integrations/content packs for more than 1,000 third-party solutions. The following table shows some of the categories and a few representative integrations.

| Category | Sample Third-Party Integrations |
|---|---|
| Messaging | Microsoft Teams, Slack, Zoom |
| Forensics & Malware Analysis | Cuckoo, Intezer, JoeSandbox |
| Threat Intelligence | Abuse.ch SSL Blacklist Feed, AlienVault OTX, Abuse IPDB |
| Endpoint Security | Carbon Black, CrowdStrike, SentinelOne |
| Network Security | Akamai WAF, AWS firewall, Azure WAF |
| Cloud Security | Microsoft Defender for Cloud, Orca Security, Wiz |
| Identity & Access Management (IAM) | CyberArk, Okta, Ping Identity, Saviynt |
| Database Security | MongoDB, Oracle, Snowflake |
| DevOps & CI/CD | BitBucket, CircleCI, GitHub Actions, GitLab |
| IT Service Management (ITSM) | BMC Remedy, Jira, ServiceNow |
| Distributed Deception Platforms | Acalvio ShadowPlex, Attivo BotSink, Illusive Networks |
| Data Lake / Analytics | Amazon Security Lake, Exabeam Data Lake, Microsoft Sentinel |
| Privileged Access Management | Admin By Request, CyberArk, BeyondTrust |
| Vulnerability Management | Nessus, Qualys, Tenable |

Table 1: Categories and samples of integrations available in Palo Alto Networks Marketplace

# Recommendations

> Integrating CNAPP capabilities with SOCs is crucial to enhance cyber incident response and operational efficiency.

A unified SOC approach not only amalgamates endpoint, network, and cloud telemetry but also correlates identity-related events, effectively closing gaps that currently hinder efficient battle against cyber threats in multi-cloud environments.

The following strategic recommendations are aimed at helping security leaders to bridge the gap between cloud security operations and traditional enterprise SOC environments to pave the way for robust security operations tailored to the dynamic nature of modern IT infrastructures. By adopting these strategic recommendations, security leaders can bridge the gap between cloud security operations and traditional enterprise SOC environments, paving the way for robust security operations tailored to the dynamic nature of modern IT infrastructures.

1) **Integrated Security Platforms**: Transition to a unified Security Operations Center with a single platform that integrates CNAPP with existing SOC tools like SIEM, SOAR, and XDR. This will help to remove incident response silos and improve cross-platform visibility and incident response times.
2) **Dynamically Identify Paths to Risks** cloud infrastructure is constantly changing in response to demand and the evolution of business applications. To respond effectively to threats in this dynamic environment it is not only necessary to set guardrails but also to interpret cyber security event data in the context of the current risk.
3) **Enhance Identity Correlation**: converging identity and access telemetry signals with those from traditional sources. Cloud services are especially open to threats that exploit non-human (service) identities as well as administrators with excessive entitlements.
4) **Connect DevSecOps and IR Teams**: responding to cyber incidents depends upon fully integrated teamwork. Neither DevSecOps nor conventional incident response can work in isolation. While integrated tools help, teamworking is essential.
5) **Adopt Common Automation in Incident Response**: Leverage prebuilt SOAR playbooks within the cloud context for automating response actions such as revoking permissions or quarantining workloads. There should be commonality of incident response regardless of context.
6) **Invest in Real-time Analytics**: The speed with which a cyber threat can take hold within a cloud environment is high. This makes it essential to deploy analytics capabilities that enable real-time detection and response. Utilize machine-learning detection and response models strengthened with cloud-native telemetry to identify emerging threats more rapidly.
7) **Optimize Telemetry Management**: Implement a cost-efficient cyber event data architecture that supports tiered data storage and real-time telemetry ingestion. Exploit API-based data collection across cloud services to ensure a consistent security posture.

8) **Strengthen Threat Intelligence**: integrate ingest cloud-relevant threat intelligence feeds. This is necessary for real-time mapping of Indicators of Compromise (IoCs) across cloud workloads and assets.

# Related Research

Leadership Compass: eXtended Detection and Response
Leadership Compass: Network Detection and Response
Leadership Compass: Endpoint Protection Detection and Response

Leadership Compass: Intelligent SIEM Platforms

Leadership Compass: Security Orchestration Automation and Response

Buyer's Compass: Endpoint Protection Detection and Response

Buyer's Compass: Network Detection and Response

Buyer's Compass: eXtended Detection and Response

Buyer's Compass: Intelligent SIEM Platforms

Buyer's Compass: Security Orchestration Automation and Response

Leadership Compass: Cloud Security Posture Management (CSPM)

Leadership Compass: Cloud Backup for AI Enabled Cyber Resilience

Leadership Compass: Privileged Access Management

Leadership Compass: Data Governance

Leadership Compass: Cloud Infrastructure Entitlement Management (CIEM)

Leadership Compass: Zero Trust Network Access

Whitepaper: Assuring Cloud Security and Compliance

Advisory Note: Cyber Risk Frameworks in 2024

Advisory Note: Securing Tomorrow - Strategic Cybersecurity Recommendations for 2024-2033

Advisory Note: Maturity Level Matrix for Cyber Security

Advisory Note: Security Organization Governance and the Cloud

# Copyright



KuppingerCole Analysts supports IT professionals with exceptional expertise to define IT strategies and make relevant decisions. As a leading analyst firm, KuppingerCole offers firsthand, vendor-neutral information. Our services enable you to make decisions crucial to your business with confidence and security.

Founded in 2004, KuppingerCole is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as technologies enabling Digital Transformation. We assist companies, corporate users, integrators, and software manufacturers to address both tactical and strategic challenges by making better decisions for their business success. Balancing immediate implementation with long-term viability is central to our philosophy.

For further information, please contact clients@kuppingercole.com..