

Cortex CDR

Stop Cloud Attacks Before They Become Breaches

The cloud accelerates innovation, transforming how businesses operate and build. This same transformation creates opportunities for cybercriminals. With over 750 million cloud-native applications supported by 38 million developers, attacks on cloud environments have surged, increasing by 66% in the past year.¹

Cloud infrastructure introduces layers of complexity that attackers exploit, compounded by fast development cycles, frequent code updates, and short-lived assets that leave vulnerabilities in their wake. With 80% of medium, high, and critical exposures occurring within cloud environments, the cloud is now the primary attack surface.²

1. *Unit 42 Incident Response Report*, Palo Alto Networks, February 2024.

2. *Unit 42 Attack Surface Threat Report*, Palo Alto Networks, September 2023.

The Need for Advanced Defense in the Cloud

Despite varied efforts to evolve, SecOps and cloud security teams operate in silos. Isolated from the SOC, cloud security misses broader attack patterns that span multiple domains. While SecOps teams strive to monitor cloud activity by ingesting logs into SIEMs alongside endpoint, network, and other data sources, they lack a comprehensive, real-time view of what's happening in the cloud. Fragmentation hinders the organization's ability to detect and respond to evolving threats.

Consider a container escape attack, a common tactic where a bad actor breaches a container to compromise the underlying host system. Without full context, the SOC team will need to manually stitch data from various sources to understand the attack story. Securing the enterprise—identifying, stopping, and responding to threats with optimal speed and precision—requires a prevention-first approach to cloud security. It requires the integration of cloud activity into the broader security ecosystem. Context equips both teams to prevent and mitigate threats faster—before damage occurs.

Introducing Cortex CDR

Protect, detect, and respond to threats in real time, with unmatched visibility and control across cloud environments. Cortex® Cloud Detection and Response (CDR) unifies security operations and cloud security in a single, powerful platform for comprehensive security—transforming how you protect your cloud environments and ensuring business continuity in an increasingly dynamic threat landscape. Cortex CDR extends industry-best cloud runtime protection with enterprise-wide visibility and response in a single source of truth for full context and workflow sharing across cloud security and the SOC.

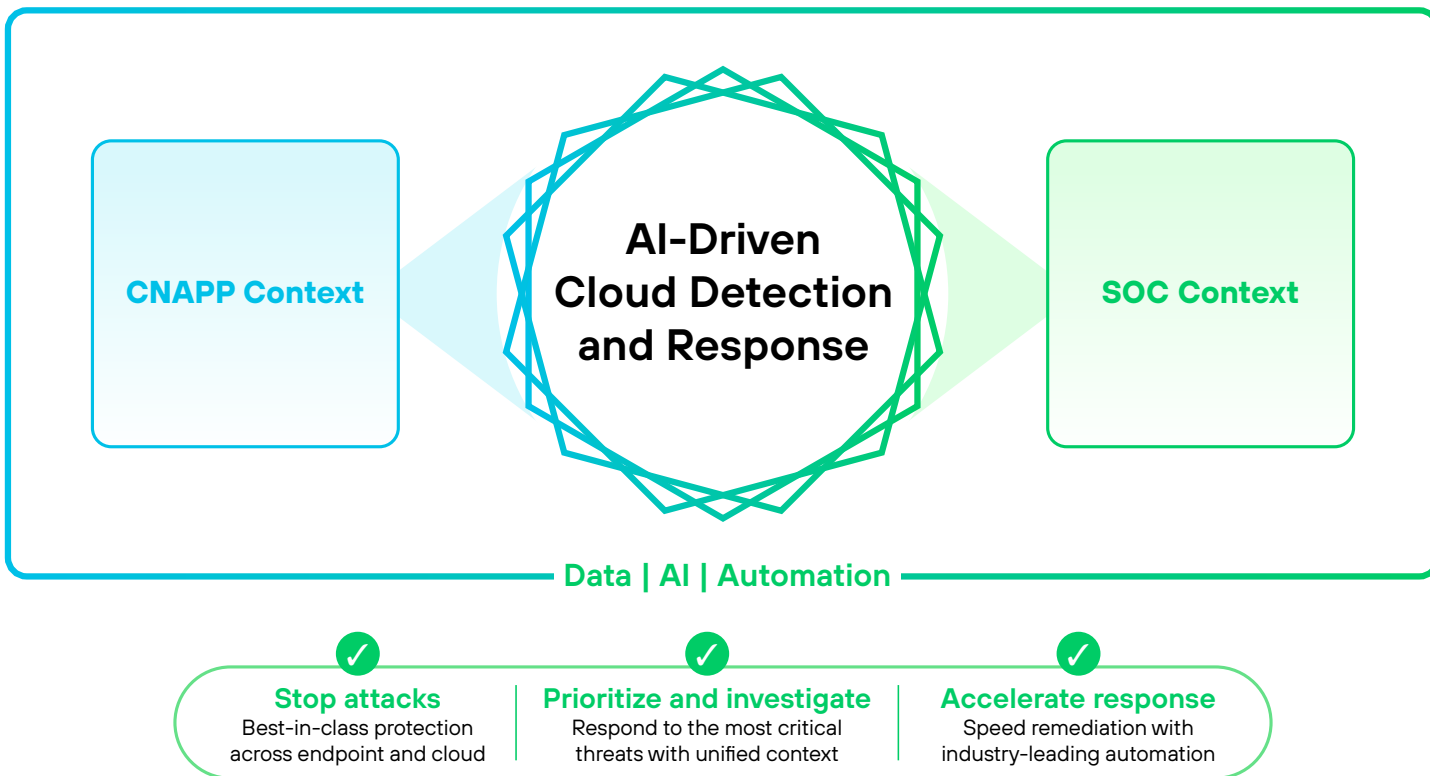


Figure 1. Bringing cloud security into the greater security ecosystem with AI-driven CDR for best-of-breed protection

Integral to the Cortex SOC platform, Cortex CDR integrates the deep cloud-native intelligence of Prisma® Cloud with the advanced detection and response capabilities of Cortex XDR®. Precision AI® powers every layer, delivering unmatched accuracy and protection for defending attacks.

Cortex CDR's Core Capabilities

Runtime Protection

Prevent known and unknown threats with elite threat intelligence and runtime protection:

- Prevent cloud attacks such as technique-based exploits, behavioral threats, malicious processes, ransomware, and cloud-based malware.
- Protect workloads across diverse environments—virtual machines (VMs), containers, Kubernetes® clusters, and serverless functions—with a lightweight agent.
- Conduct vulnerability and compliance scanning to reduce risk and manage compliance.
- Achieve industry-leading results, the highest prevention rate among vendors with zero false positives that could disrupt critical business operations in the [MITRE ATT&CK® Evaluations](#).

Real-Time Detection

Stay ahead of attackers with real-time threat detection:

- Detect threats immediately with over 10,000 detectors and more than 2,600 AI-powered models, mapping events to the MITRE framework for a detailed view of the attack tactics.
- Monitor dynamic, multicloud environments with visibility into changing attack surfaces.
- Combine CNAPP insights from the cloud control plane, dataplane, and management plane with SOC insights to generate high-fidelity detection and minimize noise.

Context-Rich Investigations

Enable security teams to act with confidence and precision:

- Turn fragmented alerts into highly prioritized incidents with context-driven insights.
- Identify the root cause of threats and incidents with cloud context, such as vulnerabilities, misconfigurations, identities, and data risks.
- Accelerate investigations with a comprehensive view into the attack lifecycle, empowering analysts to make quick and informed decisions.

Automated Incident Response

Speed up response times and reduce analyst workloads through intelligent automation:

- Accelerate remediation with over 1,000 prebuilt playbooks and integrations for seamless workflow automation.
- Remediate risks in the cloud or code to prevent future attacks.
- Continuously learn from past incidents to improve automation and future responses.

Key Cortex CDR Benefits

- **Proactive defense:** Block threats before they materialize.
- **Operational efficiency:** Reduce mean time to resolution (MTTR) by 90%.
- **Improved analyst productivity:** Decrease analyst workload by 75%.
- **Future-proof automation:** Continuous learning from incidents to enhance automation workflows.

What Sets Cortex Apart?

- A single agent for cloud and endpoint, which can be deployed in eBPF, kernel mode, or lightweight Kubernetes connector.
- The only vendor to achieve 100% technique-level detection coverage with no delays or configuration changes in the [MITRE ATT&CK Evaluations](#).
- One data lake for centralized data collection, analysis, and correlation.
- Consistently recognized as a leader by Forrester®, Gartner®, and others.

Leave No Gaps with Cortex CDR

Cyberattacks rarely stay confined to one domain. Instead, they pivot across environments, including the cloud. The most effective defense comes from a unified approach capable of detecting threats in seconds and automation-first remediation. This is the power of [Cortex Cloud™](#).

[Cortex Cloud CDR](#) seamlessly integrates code insights and cloud threat intelligence to deliver unmatched visibility and complete telemetry, enabling security teams to detect and respond to cloud incidents as they happen. Breaking down organizational silos, CDR bridges SecOps and CloudSec teams to effectively contain and remediate threats at their source.

Discover how you can stop cloud breaches and reduce your MTTR to just minutes.

[Schedule a demo today.](#)



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

© 2025 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.
cortex_ds_cortex-cdr_051225