Cortex Cloud
At a Glance

Remediate in Minutes, Block in Real Time, and Investigate and Respond in Near-Real Time

Reimagining Cloud Security

Nearly every business runs in the cloud, seeking outcomes like 65% faster delivery[1] and 4X productivity gains. The future is AI—63% name it the top cloud driver,[2] and by 2028, half of cloud resources will run AI workloads.[3]

But growth introduces risk, and peace-time security tools fail in real time. Cloud environments account for 80% of security exposures in the cloud,[4] with 45% of risks shifting monthly.[5] Attackers have doubled their speed, while security teams take roughly 145 hours to resolve an alert[6]—far too late to stop breaches.

Introducing Cortex Cloud

Cortex® Cloud changes everything. Uniting the world's leading CNAPP with the No. 1 SecOps platform, it delivers real-time security from code to cloud to SOC. Unified data, AI, and automation forge an adaptive defense that stops threats instantly at their source—empowering businesses to embrace AI-driven innovation without compromise.

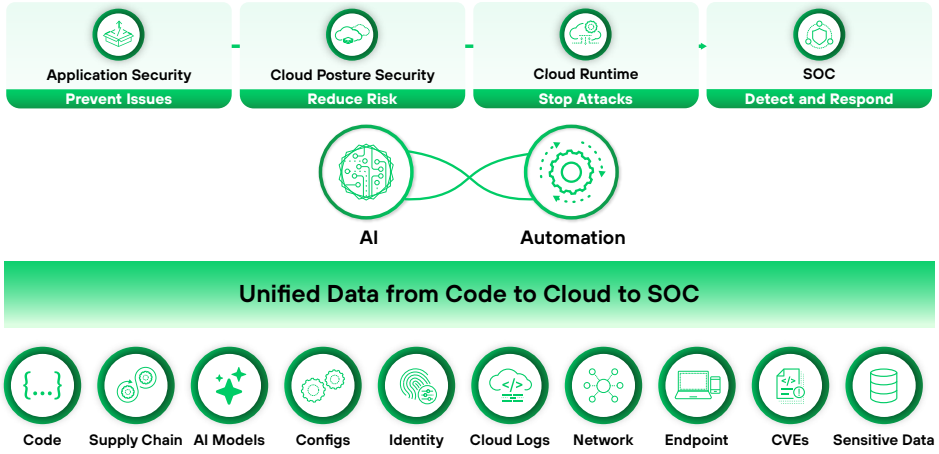

Figure 1: Unified data, dynamically stitched, enables teams to scale prevention, detection, and response

Integral to the Cortex SOC platform and purpose-built for AppSec and CloudSec teams, Cortex Cloud combines deep cloud-native intelligence with Cortex XDR's advanced capabilities for unmatched prevention, detection, and response.

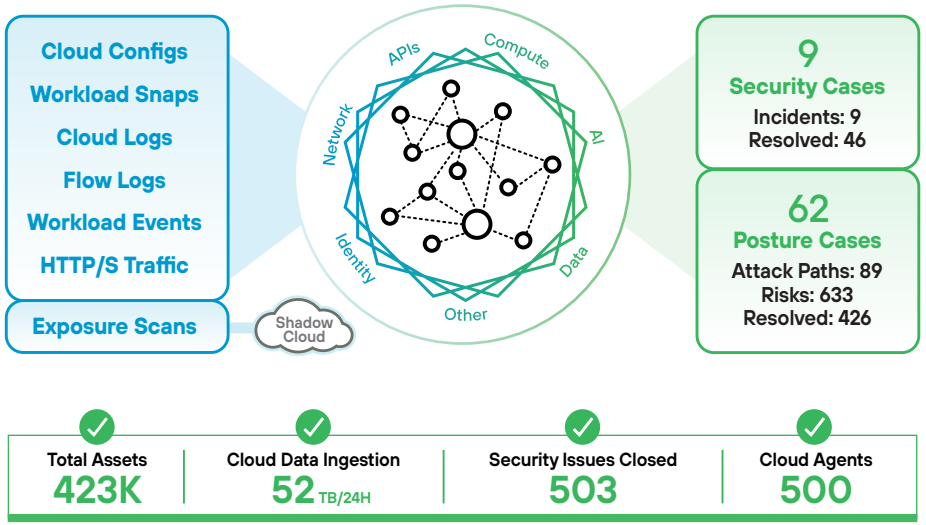

Figure 2: Petabytes of raw cloud data collected daily and transformed into actionable intelligence

The context engine in Cortex Cloud doesn't just collect and stitch data, it enriches it in real time, dynamically correlating findings with behavioral patterns and the industry's most advanced threat intelligence.

Cortex Cloud Core Capabilities

Application Security

Eliminate risk from reaching production. Cortex Cloud natively integrates with engineering ecosystems to prevent risks and secure applications by design with:

- **Centralized visibility**: ASPM provides visibility across AppSec tools and third-party scanners for consistent security across the lifecycle.
- **Ecosystem security**: Secure the engineering ecosystem—code, supply chain, and tools—from a single platform.

1. "7 Ways Cloud Computing Makes You Better at Your Job," Comcast Business, 2024.
2. *2024 Cloud and AI Business Survey*, PwC, 2024.
3. "The Future of Cloud 2028: From Technology to Business Necessity," Gartner, 2024.
4. *Cortex Xpanse Attack Surface Threat Report 2023*, Palo Alto Networks, September 14, 2023.
5. Incident Response Report 2024, Palo Alto Networks, February 20, 2024.
6. *Unit 42 Cloud Threat Report: Volume 7*, Palo Alto Networks, April 18, 2023.

Cortex Cloud
At a Glance

- **Agile guardrails**: Prevent risk from reaching production with agile guardrails that enable developers to automatically apply best practices from within native developer tools.
- **Risk management**: Manage risks with combined context from code, pipelines, runtime, and applications, prioritizing based on exploitation probability and business impact.

Cloud Posture Security

Cortex Cloud centralizes, automates, and scales cloud security to measurably improve detection, prioritization, and remediation of cloud risks by providing:

- **Comprehensive view**: Gain full view of your cloud infrastructure, compute, identities, data, and AI.
- **Attack path detection**: Detect attack paths with correlated misconfigurations, vulnerabilities, identity risks, and AI threats.
- **Intelligent risk correlation**: Consolidate alerts into fully contextualized, high-priority cases with intelligent risk correlation.
- **AI-driven resolution**: Resolve multiple alerts with AI-driven recommendations for an average 26-fold reduction in workflows.
- **Compliance and reporting**: Eliminate compliance violations, generate audit-ready reports, and monitor posture.
- **Capability consolidation**: Consolidate capabilities typically found in CSPM, CIEM, DSPM, AI-SPM, and vulnerability management tools.

Cloud Runtime Security

Stop attacks. Prevent known and unknown threats with elite threat intelligence and runtime protection, including:

- **Attack prevention**: Prevent cloud attacks, including behavioral threats, exploits, ransomware, and malware.
- **Workload protection**: Protect workloads across diverse environments—virtual machines (VMs), containers, Kubernetes clusters, and serverless functions—with a single agent.
- **Vulnerability scanning**: Scan for vulnerabilities and compliance to reduce risk.
- **Industry-leading results**: Achieve the highest prevention rate among vendors with zero false positives that could disrupt critical business operations.

Cloud SOC

Speed up response times, reduce analyst workloads, and enable security teams to act with confidence and precision through:

- **Immediate threat detection**: Detect threats immediately with over 5,000 detectors and 2,200+ AI-powered models, mapping events to the MITRE ATT&CK® framework for a detailed view of the attack tactics.
- **Rapid remediation**: Accelerate remediation with over 1,000 prebuilt playbooks as well as integrations for seamless workflow automation.
- **Risk remediation**: Remediate risks in cloud or code to prevent future attacks.

Key Cortex Cloud Benefits

- **Proactive defense** to block threats before they materialize.
- **Minimize risk** through analytics with context from code to cloud to SOC.
- **Increase efficiency**, optimizing workflows for each team.
- **Reduce cost and complexity** with tools consolidated into a single platform.
- **Innovate faster** with intelligent security guardrails.
- **Future-proof automation** with continuous learning from incidents.

What Sets Cortex Cloud Apart?

- Single agent for cloud and endpoint.
- Unified data purpose-built for AI scale, analytics, and automation.
- First to achieve 100% technique-level detection coverage with no delays or configuration changes in the MITRE ATT&CK Evaluations.
- Only multiyear leader from Forrester, Gartner, and others.

United Cloud and SOC with Cortex Cloud

Cortex Cloud rearchitects the world's leading CNAPP on the No. 1 SecOps platform for end-to-end, real-time security from code to cloud to SOC, powered by unified data, AI, and automation.

For the first time ever, get best-in-class cloud security and SecOps on a single, unified platform to shut down threats significantly faster and more efficiently.

Schedule a demo today →