Cortex Cloud
At a Glance

The World's Most Intelligent Code to Cloud to SOC Platform

Advancing the New Era of Cloud Security

An average of 1.8 million cloud security findings—the number awaiting remediation in enterprise environments.[1] With a 120-day fix-and-redeploy cycle,[2] the backlog grows 15x faster than teams can address. Detection-first workflows aren't working.

Enterprises aren't standing still. They're building faster, scaling smarter, and pushing the boundaries of what the cloud can do. The next era of cloud security demands intelligence and adaptability equal to the innovation it protects—an architecture built to scale progress safely.

Introducing Cortex Cloud

Cortex® Cloud™ unifies multicloud protection with real-time detection and response to arm security teams with unprecedented context, faster action, and better collaboration—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. Experience cloud security the way it should feel with unparalleled protection and striking simplicity.

Only Cortex Cloud merges multicloud protection with real-time detection and response to arm security teams with unprecedented context, faster action, and better collaboration.

The context engine in Cortex Cloud collects and stitches data. It also enriches it in real time, dynamically correlating findings with behavioral patterns and the industry's most advanced threat intelligence.

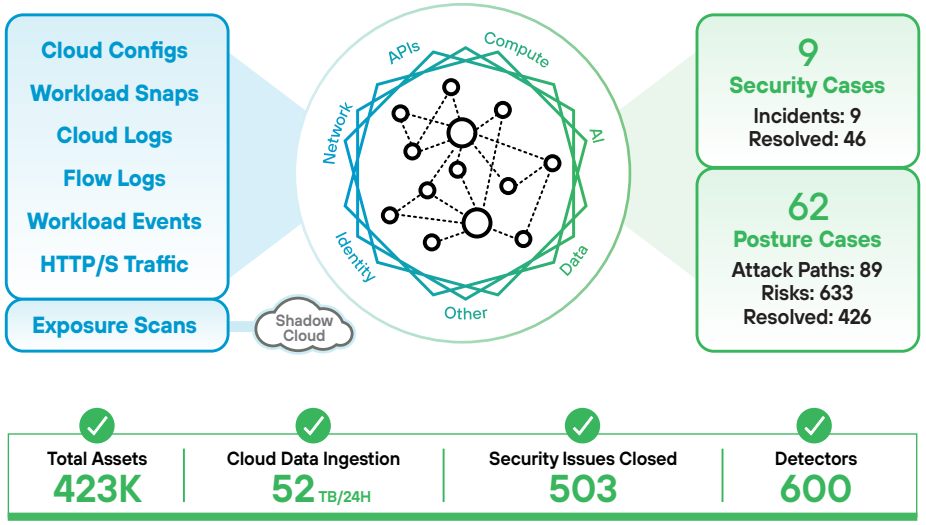

Figure 1. Petabytes of raw cloud data collected daily and transformed into actionable intelligence

Foundational Capabilities

Application Security

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

- **Centralized visibility:** Application security posture management 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.
- **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.

1. *The State of Security Remediation 2024*, Cloud Security Alliance, February 13, 2024.
2. Unit 42 Attack Surface Threat Report, Palo Alto Networks Unit 42, September 28, 2025.

Cortex Cloud
At a Glance

Cloud Posture Security

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

- **Comprehensive view:** Gain a 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 issues into fully contextualized, high-priority cases with intelligent risk correlation.
- **AI-driven resolution:** Resolve multiple alerts with AI-driven recommendations for an average 25-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:

- **Real-time protection:** 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.
- **Flexible deployment options:** Choose between the full or lightweight agent and improve performance by 50%.

Native SOC Integration

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

- **Immediate threat detection:** Detect threats immediately with over 10,000 detectors and over 2,600 AI-powered models, mapping events to the MITRE 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.
- **Agentic AI:** Eliminate threats with the most experienced AI agent workforce trained on 1.2 billion real-world responses to investigate and resolve security issues in minutes.

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 Enterprise Evaluations.
- Only multiyear leader from Forrester®, Gartner®, and others.

Unite Your 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 on a single, unified platform to shut down threats significantly faster and more efficiently.

Schedule a demo today →