Cortex Cloud Posture Security

Prioritize and Remediate Risks with an AI and Automation-Driven Platform

The demands of cloud security have evolved. Organizations face delays in identifying and mitigating cloud risks. Coupled with the increasing complexity of cloud environments and the rapid exploitation of vulnerabilities by attackers, this creates significant challenges for security teams.

- 16+ tools adopted for cloud security on average[1]
- 4,600+ new cloud security alerts each day[2]
- 11+ days average meantime to resolve (MTTR) alerts[2]

1. *State of Cloud-Native Security Report*, 2024
2. Internal Palo Alto Networks research.

Siloed Tools and Data

Relying on too many tools can complicate cloud risk management instead of streamlining it. Disparate cloud security solutions—like CSPM, CWPP, CIEM, vulnerability management, and DSPM—create inefficient workflows, forcing teams to switch between multiple products and consoles. This increases cognitive load, introduces the risk of missed priorities, and slows down effective risk management.

The lack of integration also makes it difficult to gain real-time visibility into the overall cloud security posture. Security context across code, cloud, and runtime exists in siloes—some in cloud configurations, some in workload protections, and other critical data buried in access or storage-specific logs. Without unified visibility, security teams struggle to connect the dots, leaving risks fragmented and unresolved.

Manual Work

Disconnected data and disparate tools generate an overwhelming number of alerts for security teams to address. When managing these alerts, teams struggle to prioritize which risks to address first and often need to manually correlate data across multiple sources and tools to understand the bigger picture. Without unified context, they may focus on multiple risks independently, unaware they are part of a larger issue. This redundancy and manual effort delay the ability to identify and mitigate cloud risks effectively.

Introducing Cortex Cloud Posture Security

Detect, prioritize, and remediate your biggest risks across multicloud environments. Transform the way you reduce cloud risks by unifying cloud security data and enabling AI-powered risk prioritization and automation-first remediation with Cortex® Cloud Posture Security.

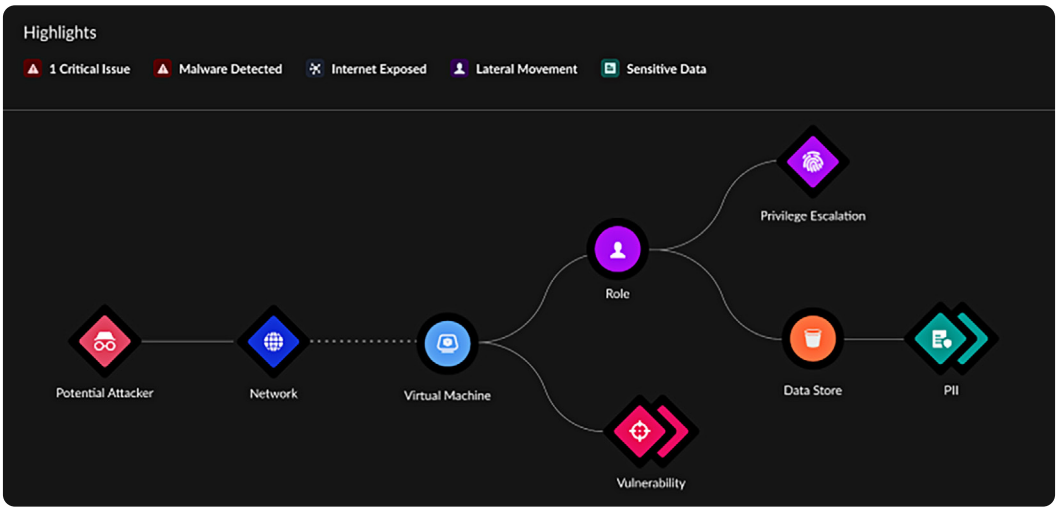


Figure 1: Multiple risk signals form an attack path

Unified Data

Unified data eliminates the inefficiency of switching between multiple tools, offering a seamless and streamlined experience and setting the foundation for AI and automation-driven outcomes. Cortex Cloud continuously collects, correlates, and normalizes data across the entire cloud environment, surpassing basic log collection. The platform brings together core cloud security capabilities—CSPM, CIEM, vulnerability management, DSPM, and AI-SPM—into a single integrated solution and combines context from code to cloud to SOC, transforming posture security.

Risk Detection and Attack Path Analysis

Detect security issues across the entire cloud environment such as vulnerabilities, misconfigurations, identity and permissions risks, public-facing exposures, sensitive data exposures, and AI risks. Cortex Cloud identifies combinations of signals that together form attack paths within cloud environments. Rich relationship graphs visualize attack paths, providing full risk context.

AI-Powered Correlation to Prioritize Risks

Out-of-the-box AI-based detections go beyond traditional approaches. Security teams can focus on their most important risks by dramatically reducing alerts and incorporating context across code, cloud, and runtime. Cortex Cloud automatically consolidates related issues and attack paths into high-priority, fully contextualized risks.

Automation-First Remediation

Resolving thousands of security issues one by one is simply unsustainable in dynamic cloud environments. That's why Cortex Cloud provides AI-driven recommendations that remediate numerous security issues with a single action. Built-in playbooks automate remediation workflows and help accelerate alert resolution. Cortex Cloud integrates with your existing technology ecosystem and workflows, driving better collaboration with teams who are responsible for resolving cloud security issues.

Key Integrated Capabilities

Cortex Cloud integrates these key posture security capabilities into a single data platform.

Cloud Security Posture Management

Gain an inventory of your IaaS and PaaS assets. Detect and remediate misconfigurations and network exposures across multicloud environments.

Workload Scanning

Discover the virtual machines, containers, Kubernetes, and serverless functions running on cloud providers. Identify and address in-workload security issues.

Cloud Infrastructure Entitlement Management

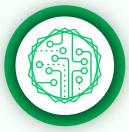
Identify the net-effective permissions across cloud infrastructure and understand which entitlements go unused. Enforce least-privileged access to reduce your blast radius.

Vulnerability Management

Identify, prioritize, and address vulnerabilities with full risk context across the application lifecycle—code, build, deploy, and run.

Data Security Posture Management

Discover, classify, protect, and govern sensitive data across your clouds. Identify risks and stop sensitive data from exfiltration.



AI Security Posture Management

Map your AI ecosystem—including models, agents, endpoints, and data flows—while monitoring sensitive data, mitigating exposure risks, and prioritizing AI threats across infrastructure and supply chains.

Kubernetes Security Posture Management

Gain visibility into resources, identify risk with context, and enforce policy at the admission controller level across Kubernetes environments.

Compliance Management

Baseline your cloud environments against industry compliance and regulatory controls. Resolve violations, monitor posture, and generate audit-ready reports.

Benefits of Cortex Cloud Posture Security

Cortex Cloud is the AI-driven platform that transforms your cloud posture, harnessing the power of AI and automation to prioritize risks, resolve issues at scale, and accelerate remediation. Reduce risk and operational complexity by centralizing multiple products into a single, converged platform purpose-built for security from code to cloud to SOC.

25X

Reduction in alerts and remediation workflows

Cortex Cloud delivers better security and productivity outcomes:

- Simplify cloud onboarding and provides full-coverage visibility without impacting operations.
- Minimize the number of alerts requiring investigation and remediation workflows.
- Reduce the time spent on configuring and tuning security policies.
- Equip security and cloud practitioners with the context and capabilities needed to reduce alert resolution times.

SEE CORTEX CLOUD IN ACTION

paloalto NETWORKS

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

cortex_sb_cloud-posture-security_020325