Cortex Cloud Application Security

Stop Risks at the Source

Development Has Never Moved Faster, Security Must Do the Same

Not long ago, deploying new code to production was a lengthy process that could take months. Today, with the rise of cloud-native development, most organizations push updates on a weekly, or even daily basis. This accelerated pace of innovation has created significant pressure on security teams, forcing them to adapt quickly to keep up with the relentless demand for speed but without compromising on safety.

The rise of DevSecOps has shifted much of the responsibility for addressing security vulnerabilities to developers, yet legacy AppSec tools fail to support their needs. Traditional AppSec tools were designed primarily for security teams, not to seamlessly integrate into cloud-native development.

Comprehensive visibility is essential to effectively secure applications. Since modern cloud-native engineering ecosystems are highly diverse and fragmented, teams often lack the required context to effectively identify, prioritize, and remediate risks.

With the speed of cloud-native development, the only way to stay on top of managing risk is by enabling developers to secure applications from the start. The problem for AppSec teams is they must strike a balance between implementing restrictive controls, which can slow development, and being lenient, which can put the organization at risk.

Cortex Cloud Application Security

Cortex® Cloud natively integrates with engineering ecosystems to prevent risks and secure applications by design. The platform unifies leading AppSec tools with third-party scanners for complete code and runtime context to prevent and prioritize risk.

Comprehensive Visibility

Cortex Cloud centralizes AppSec visibility by integrating findings across code, build, deploy, and runtime. The platform ingests data from native scanning tools, third-party scanners, and runtime for consistent security across the lifecycle. With Cortex Cloud, AppSec teams can secure the entire engineering ecosystem—code, supply chain, and tools—from a single platform.

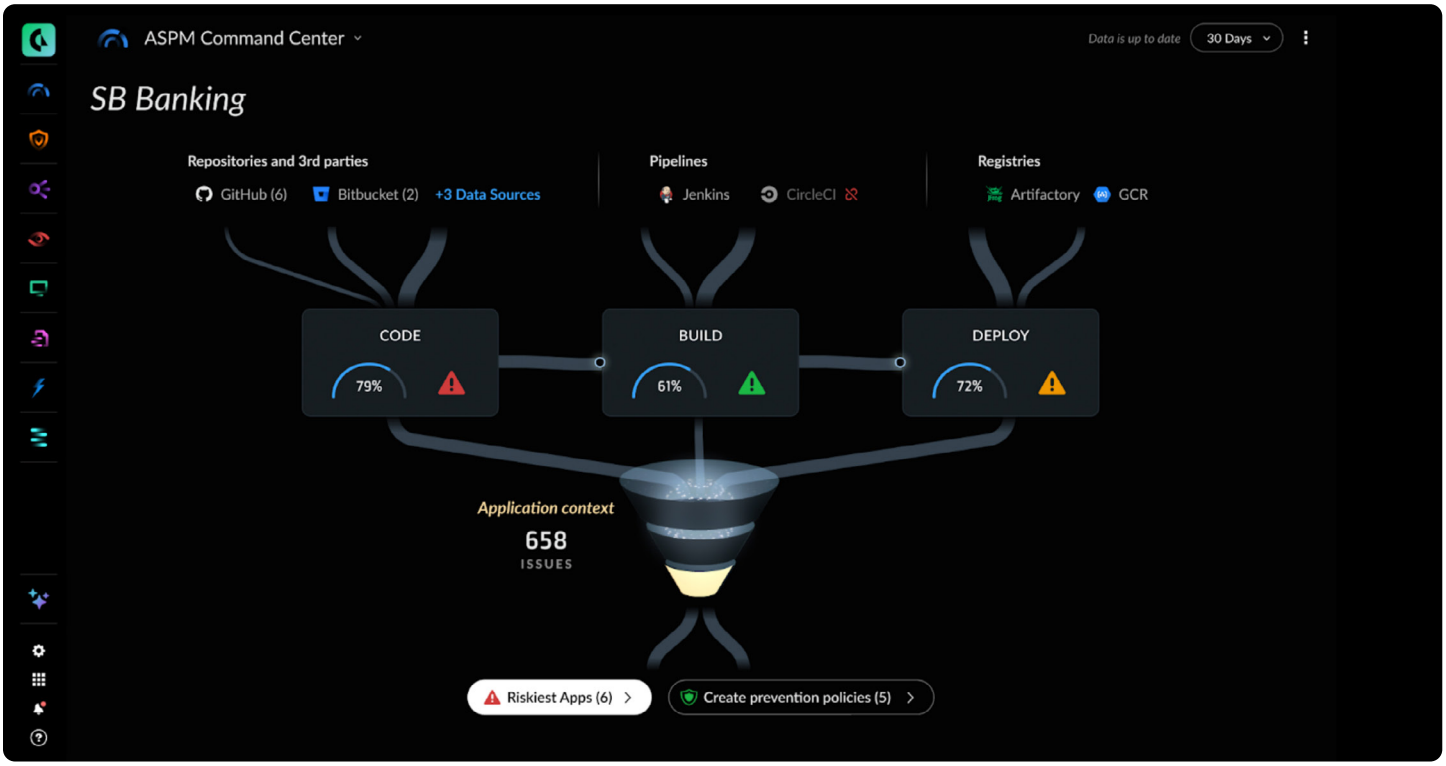

Figure 1: Cortex Cloud ASPM Command Center

Cortex Cloud Supports

Individual Development Environments (IDE):

- VS Code
- JetBrains

Version Control Systems (VCS):

- GitHub Cloud + Enterprise
- GitLab Cloud + Self-Managed
- Bitbucket Cloud + Data Center
- Azure Repos
- AWS CodeCommit

Third-Party Scanners:

- SonarQube
- Veracode
- Semgrep
- SARIF (Generic)

CI/CD Systems:

- Jenkins
- CircleCI
- GitHub Actions
- AWS CodeBuild
- Integrate Cortex Cloud CLI into any CI/CD system

AI-Driven Risk Prioritization

Maximizing risk prioritization requires runtime and application context. With this context, important information can be taken into account, such as whether:

- The package is loaded into memory.
- It is a production application.
- The application is internet exposed.
- The application is getting traffic.
- The application has access to sensitive data.

Combining code, pipeline, runtime, and application context, Cortex Cloud enables teams to prioritize risk based on probability of exploitation and potential business impact, while deprioritizing code findings that aren't reachable or are in nonproduction test environments.

Fix Risk at the Source

Cortex Cloud enables security to meet developers where they are, solving risk at the source in two ways:

1. Allowing developers to solve risk when and where it occurs from within their native environments. The platform integrates into IDE and VCS to provide immediate security feedback within a developer's native environment so they can fix issues as they occur.
2. Enabling security to trace risk to the source in code and send a pull request (PR) to a developer with context so they can easily fix security issues. Comprehensive application context enables swift ownership resolution by identifying which repository the issues stem from and which developer made the commit.

Stop New Risk from Reaching Production

Cortex Cloud enables security teams to implement agile development guardrails. Prevent risk from reaching production by applying policies that block PRs and fail builds only when context dictates. For example, failing a build when it introduces a critical vulnerability to production but allowing it in a test environment.

With runtime context, organizations can reduce friction between development and security teams by avoiding unnecessarily blocked PRs and failed builds.

Key Capabilities

Cortex Cloud integrates these key AppSec capabilities into a single platform:

Application Security Posture Management

Consolidate AppSec visibility into a single risk, policy, and automation engine, making it easier to prioritize risk and apply context-aware security policies across the entire application lifecycle.

Software Supply Chain Security

Gain deep visibility and control over the engineering ecosystem, govern pipeline tool usage and risk, manage SBOMs, and ensure secure deployments.

Infrastructure as Code (IaC) Security

Leverage comprehensive, developer-first infrastructure-as-code security with runtime tracing to fix misconfigurations at the source.

Software Composition Analysis

Proactively address open-source vulnerabilities and license compliance issues with developer integrations and context-aware prioritization.

Secrets Security

Gain comprehensive secrets security to accurately detect, prioritize, and eliminate credential exposure.

Third-Party Ingestion

Connect any AppSec tool for centralized visibility and prioritize risk based on comprehensive runtime and application context.

United AppSec, Cloud, and SOC with Cortex Cloud

Cortex Cloud rearchitects the world's leading CNAPP on the #1 SecOps platform for 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.

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

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-application-security_020525