

# Cortex Cloud Application Security Posture Management

Accelerate Secure Development with the  
Definitive Prevention-First ASPM

## Challenges

With code shipping faster than ever, security teams struggle to keep up. Production is no place to fight fires, but that's where most AppSec teams find themselves—buried in low-context alerts, chasing issues and watching backlogs pile up.

Shifting left is a step forward, but it isn't enough. Security teams continue to manage siloed scanners across sprawling cloud-native environments. Without a centralized view, it's nearly impossible to identify real risks, prevent issues early, or quickly prioritize and remediate them. Without comprehensive context, security teams can't define precise security guardrails. Overly broad policies create friction, often leading teams to remove them entirely.

# Application Security Posture Management

AppSec teams need to prevent new risks from reaching production without compromising developer velocity, and then prioritize and remediate their existing backlog—at scale. This requires an open platform that centralizes and correlates findings from disparate security scanning tools, integrates with developer workflows, and has complete context from code, application infrastructure, and cloud runtime. Armed with extensive context, teams can craft more targeted prevention policies, prioritize risk with greater precision, and automate workflows to reduce time to remediation.

## Cortex Cloud ASPM

Cortex® Cloud delivers an open, scalable platform that centralizes and correlates findings across IaC, SCA, SAST, DAST, secrets, software supply chain, application infrastructure, and cloud runtime. By integrating natively into developer workflows and pulling deep context from code, cloud, and runtime, Cortex Cloud gives teams a unified, actionable view of risk. Security can now define precise prevention policies, surface what matters, and automate remediation workflows.

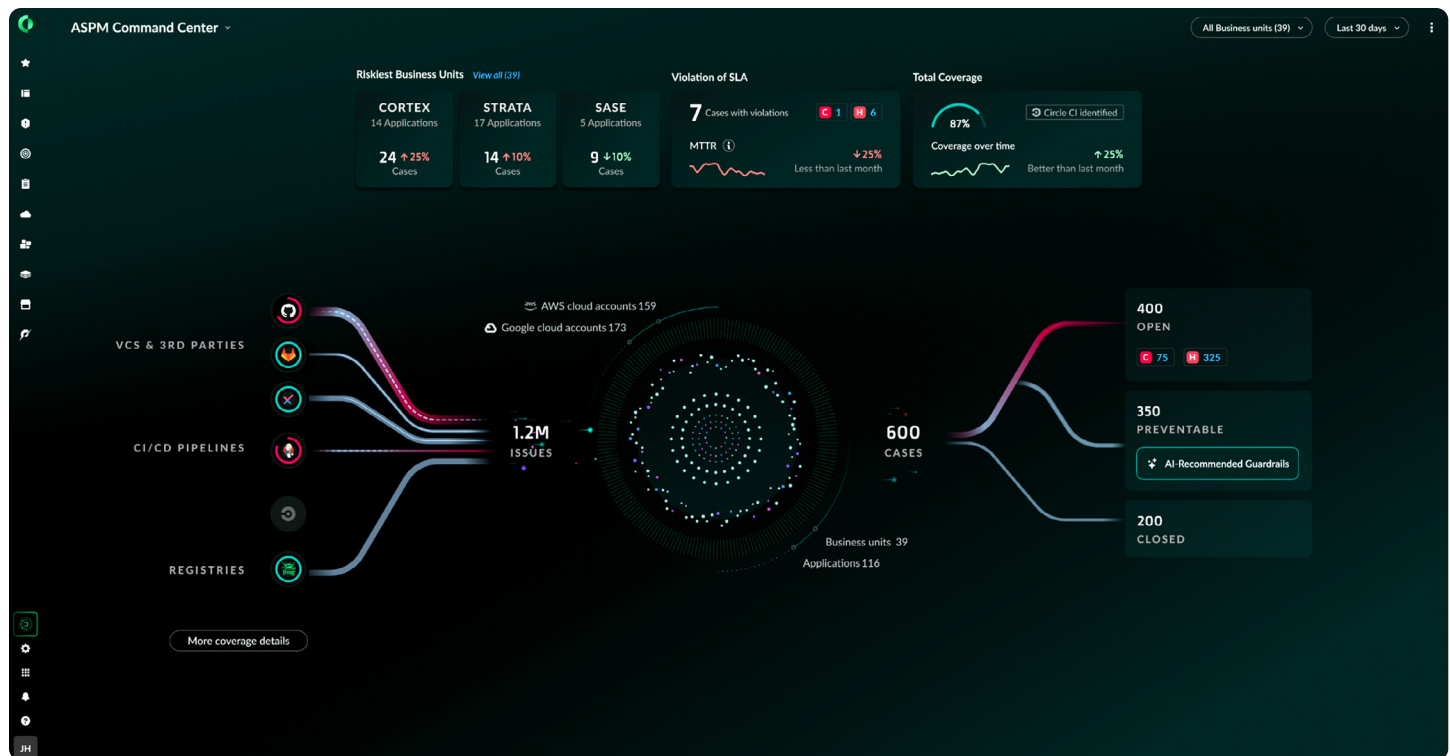


Figure 1: ASPM Command Center


## Benefits

- Proactively block up to 90% of issues from reaching production without slowing development.
- Prioritize critical, exploitable risks without requiring developers to switch tools, enhancing productivity and accelerating the remediation process.
- Eliminate manual remediation across security and development teams with industry-leading automation at every stage of the application lifecycle.

## Key Features


- **Complete visibility:** Centralize and normalize AppSec findings from the entire application lifecycle across code, cloud, and runtime.
- **Track security coverage:** Identify gaps and overlaps across AppSec tools to ensure comprehensive risk protection.
- **Risk prevention:** Enforce targeted security guardrails that distinguish between new and existing issues and use context to prevent risks from reaching production without slowing development.
- **Intelligent prioritization:** Focus on business-critical application risks with extensive code, cloud, and runtime context.
- **Automatic remediation:** Leverage automations to trigger remediation playbooks and fix issues at the source.
- **Issue attribution:** Identify the developer responsible for the security issue, the application owner to ensure remediation is assigned accurately, and reduce MTTR.
- **Consistent security from code to cloud to SOC:** Detect, correlate, and respond to active application threats across the entire lifecycle by correlating findings from code to cloud to SOC.
- **Bring security to developers:** Eliminate friction by delivering security findings and suggested fixes within native tools—so they can fix issues without slowing down or switching contexts.
- **Leverage your favorite AppSec scanners:** Integrate findings from the AppSec scanners of your choice, and maintain development workflows while boosting the value of your security tech stack.

### Integrated development environments (IDEs)

 Visual Studio Code

 JETBRAINS

### Version control systems (VCS)

 GitHub Cloud + Enterprise

 GitLab Cloud + Self Managed

 Bitbucket Cloud + Data Center

 Microsoft Azure Repos

 AWS CodeCommit

### CI/CD systems

 Jenkins

 circleci

 GitHub Actions

 AWS CodeBuild

### Native integrations

 BLACKDUCK

 CheckmarX

 GitLab

 HashiCorp  
an IBM Company

 Semgrep

 snyk

 VERACODE

 SonarQube

Plus ingest findings from any scanner using SARIF format.

SEE CORTEX CLOUD IN ACTION



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](https://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\_sb\_application-security-posture-management\_070325