Application Security Enablement — Execution Model Snapshot

Last updated: 2026-01-20

Service Identification

- Service Name: Application Security Enablement
- ISV Name: Palo Alto Networks
- Product Name: Cortex Cloud
- Service Family: Cloud Security
- Service Type: Outcome
- Service Code: PA-CC-APPSEC

How the Work Is Performed

This add-on service extends an existing cloud security foundation into the application development lifecycle by enabling visibility into application risk, code-to-cloud relationships, and pipeline exposure. It integrates application security signals into existing cloud security context so teams can identify, prioritize, and address risk earlier without replacing their development workflows.

Purpose

Defines how PA-CC-APPSEC is executed in practice, including delivery approach, customer responsibilities, dependencies, and completion criteria, to set clear execution expectations and reduce delivery risk.

Dependencies and Prerequisites

- Cloud security foundation service has been completed
- Cortex Cloud application security licenses are purchased and available
- CI/CD pipelines and repositories are accessible
- Development and security teams are available to participate

Customer Responsibilities

- Either PA-CC-POS (Cloud Security Baseline) or PA-CC-POS-RUN (Cloud Security Baseline and Runtime Readiness) completed (any variant), or a repeatable, consistent baseline posture already established in Cortex Cloud with standardized configuration and prioritized remediation
- Palo Alto Networks Cortex Cloud licenses are purchased and available
- Cortex Cloud tenant is provisioned
- Supported cloud providers are in active use
- Customer-owned teams are responsible for remediation
- Connectivity via admin credentials or API keys to supported codebases
- Approval for runtime agents or connectors
- Individuals or teams who will be responsible for implementing generated issue or case resolutions

What Happens if Dependencies Are Missing

If required inputs or prerequisites are not met, delivery may be paused until gaps are resolved. Delays caused by unmet dependencies may affect overall timelines.

Exit Criteria

- Application security capability enablement
- Integration with existing cloud security context
- Visibility into application risk and code-to-cloud relationships
- Validation and operational handover