Cloud Security Baseline and Runtime Readiness — Execution Model Snapshot

Last updated: 2026-02-03

Service Identification

- Service Name: Cloud Security Baseline
- ISV Name: Palo Alto Networks
- Product Name: Cortex Cloud
- Service Family: Cloud Security
- Service Type: Outcome
- Service Code: PA-CC-POS-RUN

How the Work Is Performed

This service establishes a governed cloud security foundation across existing cloud environments by onboarding accounts, configuring identity and access controls, enabling visibility and risk prioritization, and implementing governance, reporting, and alerting. It creates an operational baseline that supports compliance requirements and prepares the environment for runtime security capabilities.

Purpose

Defines how PA-CC-POS-RUN 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

- Administrative access to cloud environments is provided
- Qualified customer resources are assigned for decision-making
- Cortex Cloud tenant configuration is in scope
- Customer owns remediation activities
- Posture and runtime licenses are purchased and available
- Customer approves and supports agent or connector deployment
- Multiple workloads or environments may be in scope

Customer Responsibilities

- Palo Alto Networks cloud security licenses are purchased and available
- Cortex Cloud tenant is provisioned
- Supported cloud providers are in active use
- Customer-owned teams are responsible for remediation
- Approval for runtime agents or connectors

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

- Cloud account onboarding
- Security baseline configuration
- Identity and access configuration
- Governance, reporting, and alerting setup
- Validation and operational handover
- Runtime detection and protection deployed for a limited set of production workloads
- Runtime controls deployed
- Normalized runtime policies and detection behavior
- Cloud environments governed under a unified security control plane
- Security risks identified and prioritized with context
- Compliance posture measurable and reportable
- Organization prepared to adopt runtime and application security controls

entelligence™