OFFLOAD SECURITY

Cloud Security Posture Management

Module Whitepaper

Continuous multi-cloud posture across AWS, GCP, and Azure

Version 1.0 · July 2026 · Classification: Customer-Shareable

1. Overview

The Cloud Security module provides continuous security posture management across AWS, Google Cloud, and Microsoft Azure: misconfigurations, public exposure, compliance benchmarks, and cloud-provider threat signals, collected on demand and on schedule, and normalized into the platform's unified risk workflow.

2. Key Capabilities

- Multi-account, multi-cloud coverage: AWS, GCP, and Azure accounts onboarded with read-only credentials.
- Native provider signals: AWS Security Hub, AWS Config compliance, GuardDuty threats; GCP Security Command Center findings; Azure Defender for Cloud assessments and alerts.
- Open policy engines (Prowler-class checks) layered on top of native signals for provider-independent benchmark coverage.
- Region-aware scanning for AWS with parallel fan-out; global scanning for GCP and Azure.
- GCP organization onboarding with recursive project discovery.
- Scheduled scans through the unified scheduler, with staggered execution windows.
- Asset inventory correlation: discovered cloud assets tracked with lifecycle status and deletion reconciliation.
- Compliance scoring per account mapped to framework controls.

3. How It Works

Scans are orchestrated through a queued execution model: a scan request creates a tracked scan run, fans out per region and per account under concurrency caps, and dispatches to provider-specific scanners running on worker infrastructure. Credentials are decrypted only inside the worker process for the duration of the scan.

Findings from every provider are normalized into a common schema — severity, resource, region, rule, and compliance mapping — and stored as unified occurrences, so a GuardDuty threat and an Azure Defender assessment are managed through the same lifecycle as every other finding on the platform.

4. Data Handling & Security

Aspect	How it is handled
Credential protection	All connection credentials are encrypted at rest with Fernet authenticated encryption (AES-128-CBC + HMAC), decrypted in memory only at the moment of use, and never returned by APIs.
Tenant isolation	Every record is scoped to the owning team; all reads and writes filter on the tenant

Aspect	How it is handled
	identifier, enforced by database indexes.
Retention & deletion	Results are subject to configurable retention windows; data can be hard-deleted per scan and is removed by the tenant-offboarding cascade.
Deployment	Available as SaaS or fully self-hosted / on-premises — in the on-premises model no security data leaves your environment.

5. One Platform, One Risk View

Cloud findings feed the unified vulnerability management queue, mint into the enterprise risk register, contribute to compliance posture per framework control, appear in attack-path analysis, and raise centralized alerts — one data model shared with code, container, and Kubernetes findings.