OFFLOAD SECURITY

Container & Software Supply Chain Security

Module Whitepaper

Registry-to-runtime image assurance: vulnerabilities, SBOMs, signatures, and secrets

Version 1.0 · July 2026 · Classification: Customer-Shareable

1. Overview

The Container Security module scans container images across private and public registries for vulnerabilities, generates SBOMs, verifies signatures, lints Dockerfiles, and detects embedded secrets — connecting image risk to the source repositories and clusters where those images are built and deployed.

2. Key Capabilities

- Registry coverage: AWS ECR, Google Artifact Registry, Azure ACR, Docker Hub, and GitHub Container Registry, with saved-registry management and image discovery.
- Dual-engine vulnerability scanning (Trivy and Grype) with CISA KEV exploited-vulnerability enrichment.
- SBOM generation (Syft) in CycloneDX, SPDX, and syft-json formats.
- Dockerfile linting (Hadolint) and image signature verification (Cosign).
- Embedded-secret detection inside image layers (TruffleHog).
- Scheduled registry re-validation so image findings stay current.
- CI/CD integration: image and artifact scanning from pipelines via a GitHub Action and API-key-scoped endpoints.
- Registry authentication failures classified and surfaced honestly (auth vs. infrastructure vs. scan errors).

3. How It Works

Every scan runs in an isolated, single-use scanner container — the platform never installs scanning tools into its own runtime. Registry credentials are encrypted at rest, decrypted only in the backend process, and passed to scanners through a read-only authentication volume.

A single registry-authentication module owns all registry login flows, so ECR, Artifact Registry, and ACR authentication behave identically across every scan path. Results are normalized per image with severity summaries and stored with scan history for trending.

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 identifier, enforced by database indexes.

Aspect	How it is handled
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

Image findings join unified vulnerability management, link to the repositories that build them and the clusters that run them, contribute to the risk register and compliance posture, and can gate CI/CD pipelines through the release-gate integration.