OFFLOAD SECURITY

# Kubernetes Security

## Module Whitepaper

*Continuous cluster posture: configuration, workloads, benchmarks, and images*

Version 1.0 · July 2026 · Classification: Customer-Shareable

## 1. Overview

The Kubernetes Security module provides continuous assessment of Kubernetes clusters — CIS benchmarks, workload best practices, NSA/MITRE framework checks, and image vulnerabilities — from a validated, encrypted cluster connection, with results unified into platform-wide risk and compliance views.

## 2. Key Capabilities

- Cluster onboarding with kubeconfig safety validation and encrypted credential storage.
- CIS Kubernetes Benchmark assessment (kube-bench).
- Workload configuration best practices (Polaris): privileged containers, resource limits, probes, security contexts.
- Framework-based posture scanning (Kubescape): NSA-CISA, CIS, and MITRE ATT&CK aligned controls.
- Container image CVE scanning for images running in cluster pods (Trivy).
- Findings tagged with MITRE ATT&CK techniques for threat-informed prioritization.
- Automatic first scan on cluster onboarding and scheduled recurring scans.
- Per-team cluster ownership enforcement on every scan and read path.

## 3. How It Works

Clusters are onboarded with a kubeconfig that is validated for safety, encrypted at rest, and scoped to the owning team. Scans run as background jobs: the platform connects to the cluster, executes each scanner in an isolated container, parses results into a common findings schema, tags MITRE techniques, and persists per-cluster scan history.

Scan execution is instrumented end-to-end (tracing and metrics), with orphaned-scan cleanup and a reconciler so cluster scan status always reflects reality.

## 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. |
| Retention & deletion | Results are subject to configurable retention windows; data can be hard-deleted per scan and is removed by the tenant-offboarding cascade. |

| Aspect | How it is handled |
|---|---|
| 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

Kubernetes findings flow into unified vulnerability management with the same triage lifecycle as cloud and code findings, mint into the risk register, contribute to compliance posture, and are included in scheduled reports and central alerting.