OFFLOAD SECURITY

Unified Vulnerability Management

Module Whitepaper

One queue, one lifecycle, one history — across cloud, code, containers, and Kubernetes

Version 1.0 · July 2026 · Classification: Customer-Shareable

1. Overview

Unified Vulnerability Management is the platform's center of gravity: findings from every scanning module and integrated tool are normalized into a single occurrence model with deduplication, exploit-aware prioritization, governed lifecycle, SLA tracking, and full history — replacing per-tool consoles and spreadsheets.

2. Key Capabilities

- Single occurrence model across cloud, code, SCA, containers, Kubernetes, web/API, and integrated third-party sources.
- Normalization to canonical severities and stable fingerprints; duplicates collapse across rescans.
- Exploit-aware prioritization: CVSS enriched with CISA KEV (known-exploited) and EPSS (exploit probability).
- Governed lifecycle: open → triaged → resolved / risk-accepted / false-positive; risk acceptance requires an owner, justification, and expiry — expired acceptances automatically re-open.
- Ownership, SLA tracking, and vulnerability aging measurement.
- Full historical record: every occurrence retains its status history across scans.
- Resource-lifecycle awareness: occurrences auto-close when their resource is deleted, through a shared deletion cascade.
- Dashboards and executive reporting over live data — counts, trends, aging, and SLA posture.

3. How It Works

Every scanning module syncs its results through a single synchronization service that owns the canonical vocabulary — severities, statuses, and source types are defined once and imported everywhere. Fingerprinting keeps a finding's identity stable across scans, so triage decisions persist and re-scans update rather than duplicate.

Grouped-finding reads use a two-phase query pattern engineered for scale, keeping dashboards responsive as occurrence volumes grow into the millions.

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

Occurrences mint into the enterprise risk register with business context, drive compliance posture where controls require vulnerability management evidence, power central alerting, and are the substrate for attack-path and threat-intelligence correlation.