OFFLOAD SECURITY

Integrations & SIEM Connectivity

Module Whitepaper

Your existing tools, one operational layer — including Wazuh SIEM

Version 1.0 · July 2026 · Classification: Customer-Shareable

1. Overview

The Integrations module connects the platform to the tools an organization already runs — SIEM, ticketing, chat, and security scanners — with team-scoped, encrypted credential storage, verified connections, and real data ingestion, so existing investments feed the unified risk view instead of another silo.

2. Key Capabilities

- Integration marketplace: a catalog of connectable tools with connect, test-connection, sync, and disconnect flows.
- Team-scoped credential store — integrations are team resources, usable by any teammate, isolated across tenants, encrypted at rest.
- Wazuh SIEM integration: agent inventory, alert ingestion, and posture summaries bridged into platform dashboards.
- Connection tests that verify real reachability and authentication at connect time — not fire-and-forget configuration.
- Scheduled global sync keeps integration data current; per-integration data summaries are stored and surfaced on the integration cards.
- Central alerting: integration failures and high-value events raise alerts in the platform's unified alert center.
- Audit and compliance connectors so integrated-tool evidence supports control posture.

3. How It Works

Each integration stores its configuration with sensitive fields encrypted at rest. Connect and sync flows execute a real test against the target system and record classified results. Ingested data lands in a common integration-data store with per-tool adapters, giving every integration a consistent freshness and health model.

The Wazuh bridge treats the SIEM as a first-class data source: agents and alerts are ingested, summarized, and correlated into the platform's posture views rather than merely linked out.

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

Integrated-tool findings and events join unified vulnerability management and central alerting, extend compliance evidence, and appear in executive reporting — the consolidation layer that makes existing tools more valuable rather than replacing them.