

HYVE OVERLORD + RAPTOR

Security & Compliance Overview

Government-grade, post-quantum AI-agent cyber defense - for procurement & vendor security review

SECURITY ARCHITECTURE

- **Your data stays in your environment.** The OVERLORD + Raptor desktop platform runs on your machines and activates offline (Ed25519, verified locally). Nothing phones home; VSS does not collect or store your operational data, telemetry, or PHI.
- **Post-quantum encrypted control channel.** The Shield-to-Command channel is encrypted at the application layer with NIST ML-KEM-768 (FIPS 203), in addition to TLS, defeating “harvest now, decrypt later.”
- **Encryption at rest.** Local secrets and key material are sealed with OS-native key stores (Windows DPAPI / platform secure storage); never plaintext.
- **Tenant isolation.** Multi-tenant data is isolated at the database layer with row-level security; cross-tenant access denied by default. Privileged operations run server-side, least privilege, fail-closed.
- **Least privilege & audit trail.** Role-based access control with an immutable audit trail across administrative and security actions.
- **Offline-first, no lock-in.** Licenses are offline-verifiable and perpetual-capable: no license server, nothing phones home, no runtime dependency on VSS.

COMPLIANCE POSTURE

FRAMEWORK	STATUS	NOTES
SOC 2 Type II	IN PROGRESS	Readiness program underway; SOC 2-aligned controls in operation today. Report shared under NDA on completion.
HIPAA	READY	HIPAA-ready architecture; your PHI never leaves your environment. BAA available for qualified healthcare deployments.
CMMC L2 / NIST 800-171	POSTURE MONITORING	Built-in control mapping + continuous posture monitoring. Posture monitoring & alignment, not a certification of your environment.
US Data Residency	YES	US-only product; customer data resides in the United States, within your environment. EAR / ITAR export-controlled.

DATA HANDLING

The OVERLORD + Raptor desktop platform is offline-first: detection, response, and the Raptor shield channel run inside your environment. VSS does not receive, process, or store your operational data, security telemetry, or any PHI in the course of the product’s operation. The only data VSS holds is what you provide for licensing and support (e.g. the purchaser’s name/email), retained in US-based systems under least-privilege access.

This overview describes our security architecture and the control frameworks we engineer to; each framework’s status is stated explicitly above. Engineering to a framework’s controls is not the same as a third-party certification of your environment. Formal attestations (the SOC 2 Type II report) and executed agreements (BAA) are provided directly to qualified customers under NDA as part of procurement. HYVE OVERLORD and Raptor are US-only, export-controlled products (EAR / ITAR).

Vendor security review? Request the full security package: vibesoftwaresolutions@gmail.com