How is Cyber Crucible data protected in transit?

Short answer: All agent-to-server communications enforce TLS 1.3. Operational data payloads additionally use JSON Web Encryption (JWE) with unique per-agent cryptographic key pairs, so payloads cannot be intercepted or manipulated in transit. Administrative access requires key-based authentication plus OAuth 2.0 token validation.

The layers

- **Encrypted channels** — all agent-to-server communication enforces TLS 1.3.
- **Per-agent payload encryption** — operational payloads use JWE with unique per-agent key pairs. Because each agent has its own key pair, compromising one transit circuit does not expose others, and inline interception or manipulation is prevented.
- **Authenticated administration** — system access requires individual key-based user authentication and OAuth 2.0 token validation, restricting administrative actions to authorized personnel.

Why per-agent keys matter

Transport encryption alone protects the channel. Per-agent payload encryption protects the *content of the message* independently of the channel — so an attacker positioned inline, or a compromised intermediary, still cannot read or alter what the agent sent.

Shared infrastructure

Where public or virtual private cloud environments are used for backend administration, Cyber Crucible applies strict logical tenant isolation together with end-to-end payload encryption. Cloud providers and infrastructure operators have **zero visibility** into operational data payloads or customer system states.

Revision #2
Created 2026-07-21 18:59:37 UTC by Dennis Underwood
Updated 2026-07-21 19:32:48 UTC by Dennis Underwood