# Como os dados da Cyber Crucible são protegidos em trânsito?

**Resposta curta:** Todas as comunicações entre o agente e o servidor aplicam TLS 1.3. Os payloads de dados operacionais utilizam adicionalmente JSON Web Encryption (JWE) com pares de chaves criptográficas exclusivos por agente, de modo que os payloads não possam ser interceptados ou manipulados em trânsito. O acesso administrativo requer autenticação baseada em chaves, além de validação de token OAuth 2.0.

# As camadas

- **Canais criptografados** — todas as comunicações entre o agente e o servidor aplicam TLS 1.3.
- **Criptografia de payload por agente** — os payloads operacionais utilizam JWE com pares de chaves exclusivos por agente. Como cada agente possui seu próprio par de chaves, o comprometimento de um circuito de trânsito não expõe os demais, e a interceptação ou manipulação inline é evitada.
- **Administração autenticada** — o acesso ao sistema requer autenticação individual de usuário baseada em chave e validação de token OAuth 2.0, restringindo as ações administrativas a pessoal autorizado.

# Por que as chaves por agente são importantes

A criptografia de transporte, por si só, protege apenas o canal. A criptografia de payload por agente protege o *conteúdo da mensagem* de forma independente do canal — de modo que um atacante posicionado inline, ou um intermediário comprometido, ainda assim não consegue ler ou alterar o que o agente enviou.

# Infraestrutura compartilhada

Quando ambientes de nuvem pública ou de nuvem privada virtual são utilizados para a administração de back-end, a Cyber Crucible aplica um rigoroso isolamento lógico de locatários

(tenants), juntamente com criptografia de payload de ponta a ponta. Os provedores de nuvem e operadores de infraestrutura têm **visibilidade zero** sobre os payloads de dados operacionais ou os estados dos sistemas dos clientes.

---

Revision #1
Created 2026-07-24 05:53:51 UTC by Dennis Underwood
Updated 2026-07-24 05:53:51 UTC by Dennis Underwood