

What can Cyber Crucible disclose if compelled by a government or court?

Short answer: Nothing in the categories that matter most, because it never holds them. Cyber Crucible does not harvest, store, or retain decryption keys, user credentials, or customer files — so there is nothing of that kind to produce to any private party, government, or foreign power. Like any U.S. company it remains subject to applicable law, but it cannot produce data it never holds.

"Nothing to disclose by design"

This is a deliberate architectural position rather than a legal promise. Legal process can compel a company to hand over what it has. It cannot compel a company to produce what was never collected.

Because Cyber Crucible does not collect or retain encryption keys, credentials, or private content, those categories are empty by design.

Why this matters more than it used to

Centralized security architectures create a high-value aggregation point. A vendor holding thousands of customers' keys and session tokens is a target for criminal and state-sponsored attackers alike — and can be reached through legal compulsion, sometimes without the customer's knowledge.

Cyber Crucible's position on key escrow follows the same reasoning: it deliberately does not maintain a central key store, so there is no single point of failure to breach or subpoena.

An honest boundary

Cyber Crucible is a U.S. company and is subject to U.S. law. The claim here is narrow and specific: it cannot disclose data it does not hold. That is a statement about architecture, not a claim of immunity from legal process.

