What does data sovereignty mean for Cyber Crucible deployments?

Short answer: Your data stays where you put it. Analysis and enforcement happen on the endpoint, and Cyber Crucible can be deployed fully on-premises — running in physically secured server racks rather than a public cloud, with no third-party platforms, no external access, and no data sharing.

Why centralized security data is a liability

Security architectures that centralize sensitive material — encryption keys, session tokens, identity data — create a single point of failure and a high-value target for criminal and state-sponsored attackers alike.

There's a second risk that receives less attention: a government could compel access to centrally held data through a classified subpoena or national security letter, without the customer's knowledge or consent. That's a profound data-sovereignty exposure with no transparency.

The on-premises option

For organizations requiring absolute control, Cyber Crucible offers full on-premises installation, including air-gapped deployment and multi-tenant architecture suitable for managing multiple departments or agencies from a single secure instance.

Revision #3
Created 2026-07-20 19:24:07 UTC by Dennis Underwood
Updated 2026-07-21 19:32:22 UTC by Dennis Underwood