



Cyber Crucible Data Sharing, Collection, and Sovereignty Mandate

CYBER CRUCIBLE, INC.

1378 Freeport Road | Pittsburgh, PA 15139 | United States

+1.412.775.2158 | info@cybercrucible.com

To Our Valued Enterprise Clients, Sovereign Partners, and Data Protection Officers:

Cyber Crucible, Inc. produces specialized, next-generation cybersecurity software engineered to defend enterprise infrastructure autonomously and at machine speed. We recognize that legacy cybersecurity tools often rely on centralized "cloud harvesting" models that continuously exfiltrate endpoint telemetry, user account details, and file system artifacts across national and geopolitical borders.

This cloud-centric approach is technologically slow against modern automated threats, and it creates unacceptable compliance and security vulnerabilities under global privacy regulations, including the European Union GDPR, Saudi Arabia PDPL, UAE Federal Decree-Law No. 45/2021, and Kenya Data Protection Act.

Cyber Crucible operates under a **principle of geopolitical neutrality** and **architectural data sovereignty**. We build software designed to protect your organization without embedding foreign strategic backdoors, foreign state intelligence partnerships, or mandatory cloud dependencies.

To guarantee complete alignment with your operational privacy and regulatory requirements, Cyber Crucible, Inc. formally adheres to the following binding mandates:

1. Content Privacy & Zero Content Collection

- **No Content Harvesting:** Cyber Crucible, Inc. does not collect, store, or transmit customer decryption keys, user passwords, session tokens, refresh tokens, private messaging keys, or proprietary files.
- **No Commercial Data Monetization:** Customer data is strictly not for sale. Cyber Crucible does not share, trade, license, or monetize customer identity or telemetry data with any third party.
- **Nothing Disclosed by Design:** Because Cyber Crucible does not collect or retain customer encryption keys, credentials, or private content, there is nothing in these categories for Cyber Crucible to produce to any private or government party. Like any U.S. company, we remain subject to applicable law, but we cannot disclose data we

1378 Freeport Road Pittsburgh, PA 15139

+1.412.775.2158 • info@cybercrucible.com • www.cybercrucible.com



never hold.

2. Local Execution & Sovereign Deployment Capabilities

- **Autonomous Edge Prevention:** Threat evaluation and process interdiction occur locally on the endpoint in typically under 200 milliseconds, operating independently of external cloud connection.
- **100% On-Premises Air-Gapped Option:** For clients requiring total data isolation and residency, Cyber Crucible offers an On-Premises deployment model. All backend management software runs entirely within your physically secured server racks, guaranteeing that **zero telemetry or data ever leaves your sovereign network boundary**.
- **Encrypted Transit Controls:** In cloud-assisted configurations, administrative communications are protected using JSON Web Encryption (JWE) over HTTPS with unique per-agent key pairs and key-based authentication.

3. Supply Chain Integrity & Geopolitical Neutrality

- **Proprietary In-House Engineering:** Our kernel drivers, sensors, and Genetic AI models are engineered and maintained in-house. We do not embed unverified third-party libraries, foreign SDKs, or state-sponsored code components.
- **Microsoft WHCP Validation:** Cyber Crucible kernel drivers undergo internal quality assurance and are submitted for certification under Microsoft's Windows Hardware Compatibility Program. .
- **Strict Personnel Controls:** All Cyber Crucible personnel with potential administrative system access are required to execute binding mutual Non-Disclosure Agreements ([<https://www.cybercrucible.com/mutualNDA>])(<https://www.cybercrucible.com/mutualNDA>)). System access is granted strictly on a role-based, need-to-know basis only when required for explicit business operations.
- **Supply Chain Risk Zero-Tolerance:** If any supplier, vendor, contractor, or employee poses a potential risk to Cyber Crucible customers or customer intellectual property, we actively manage that risk or immediately terminate the resource engagement.

Our software is engineered to defend your operations autonomously, quietly, and entirely within your legal and geographic boundaries.

Sincerely,

[Digital Signature]

1378 Freeport Road Pittsburgh, PA 15139

+1.412.775.2158 • info@cybercrucible.com • www.cybercrucible.com



Dennis Underwood

Chief Executive Officer

Cyber Crucible, Inc.

dennis@cybercrucible.com