Industry Vendor-Risk Guides

Security due-diligence answers for specific regulated industries — healthcare, education, government, defense, utilities, financial services, retail, legal, and insurance — framed for the vendor-risk reviewer. States plainly what Cyber Crucible holds and does not hold.

How does Cyber Crucible support HIPAA, and will it sign a Business Associate Agreement?

Short answer: Cyber Crucible supports a covered entity's HIPAA obligations primarily by never collecting protected health information (PHI). Analysis happens locally on the endpoint, so PHI is not uploaded to a third-party cloud for security processing. Because Cyber Crucible does not create, receive, maintain, or transmit PHI on a covered entity's behalf, it does not typically meet the definition of a business associate — but where a customer's risk process requires one, a Business Associate Agreement can be executed.

Why the architecture fits healthcare

- **PHI never leaves the device for security analysis.** Many vendor-hosted SOC/MDR arrangements upload files, keys, or telemetry to a third-party cloud; Cyber Crucible analyzes on the endpoint, so that exposure is avoided.
- **Clinical continuity.** Only the malicious process is suspended — no full-system isolation or forced reboot — so connected devices and clinical systems keep running while an attack is neutralized.
- **Ransomware without a 24/7 SOC.** Autonomous prevention stops attacks pre-execution without requiring analysts a hospital may not be able to staff.

The honest boundary

Cyber Crucible is not "HIPAA certified" — there is no such certification. It supports your compliance program; your privacy and security officers make the determination for your environment. A BAA is available on request from **dpo@cybercrucible.com**.

How does Cyber Crucible support FERPA and student-data privacy for schools and universities?

Short answer: Cyber Crucible helps educational institutions two ways: it stops ransomware autonomously without a 24/7 security operations center, and — through FortressAI — it evaluates AI-tool data access on the device so student records and family data do not reach a public AI system by accident. Because analysis is local and no student records are collected, protected educational records stay within the institution's boundary.

The two education problems it addresses

- **Ransomware without a SOC.** Kernel-level prevention stops attacks in under 200 milliseconds with no analysts to hire and no round-the-clock monitoring contract to fund.
- **AI governance for the classroom.** FortressAI checks each prompt on the device, so protected educational records and personal family data are not sent to a public AI system — including as training data.

Vendor-selection notes

- Cyber Crucible acts as a school official / service provider under the institution's direction and does not use student data for any secondary purpose.
- State student-privacy laws (for example, in California, New York, and Colorado) layer additional vendor obligations; the local-processing, no-collection design supports them. Documentation is available under NDA.

Is Cyber Crucible FedRAMP authorized, and how does it serve government agencies?

Short answer: No — Cyber Crucible does not currently hold a FedRAMP authorization, and it does not imply otherwise. FedRAMP authorizes cloud service offerings that hold agency data; Cyber Crucible's model is different. It runs locally on the endpoint and can be deployed fully on-premises or air-gapped inside the agency's own boundary, so agency data never leaves that boundary for a third-party cloud.

How the architecture fits government

- **On-premises / air-gapped deployment.** The platform can run entirely within an agency's secured infrastructure, with no external data flow — suitable for classified, disconnected, and high-security environments.
- **No agency data collected.** Customer content, credentials, and keys are never collected, which removes much of what a cloud authorization is designed to protect.
- **US-made and export-controlled.** The software is subject to U.S. Department of Commerce EAR (not ITAR), and is internationally patented following USPTO review that included Department of Defense review.

The honest boundary

Where an agency requires a specific authorization (FedRAMP, StateRAMP), Cyber Crucible does not currently hold it; the on-premises deployment model is the path that keeps data inside the agency boundary. Deployment and control detail is provided under NDA.

Does Cyber Crucible meet CMMC and DFARS requirements for the defense industrial base?

Short answer: Cyber Crucible is not CMMC-certified, and it says so plainly. It supports a defense contractor's obligations under DFARS 252.204-7012 and CMMC primarily by not collecting Controlled Unclassified Information (CUI) and by supporting on-premises or air-gapped deployment inside the contractor's own boundary, where CUI stays under the contractor's control.

How it supports the contractor's obligations

- **No CUI collected.** The endpoint agent analyzes behavior locally without extracting the files it protects, so CUI is not transferred to Cyber Crucible.
- **Boundary-preserving deployment.** On-premises and air-gapped models keep all data within the contractor's assessed boundary.
- **Endpoint protection controls.** Malware/ransomware prevention and monitoring map to the relevant CMMC practices and NIST SP 800-171 controls the contractor must implement.
- **US supply chain.** US data is handled by US-based resources; offshore contractors do not handle US data or develop the agents. The software is EAR-controlled, not ITAR.

The honest boundary

CMMC certification is held by the contractor's environment, not by an individual security tool; Cyber Crucible is a control that supports several 800-171 requirements, not a substitute for the contractor's assessment. Mapping detail is available under NDA.

How does Cyber Crucible fit NERC CIP and critical-infrastructure security?

Short answer: Cyber Crucible suits critical-infrastructure and utility environments because it protects endpoints autonomously and can run offline or air-gapped, with no cloud dependency in the protective path. That fits BES Cyber Systems and other environments where connectivity is restricted and availability is paramount.

Why it fits utilities and critical infrastructure

- **Offline / air-gapped capable.** Full protection with no internet connection, suitable for isolated OT networks and substations.
- **Availability-preserving response.** Only the malicious process is suspended, so operational systems keep running — no full-system lockdown during an incident.
- **Local, deterministic decisions.** Detect–Decide–Respond runs on the device with no cloud round trip and no live AI model.

Vendor-selection notes

NERC CIP obligations sit with the registered entity, not with an individual vendor; Cyber Crucible is a control that supports several CIP objectives (malware prevention, monitoring, incident handling). It is not a registered entity and does not represent itself as CIP-certified. Supporting documentation is available under NDA.

How does Cyber Crucible align with IEC 62443 for industrial control systems?

Short answer: Cyber Crucible supports the IEC 62443 defense-in-depth model for industrial automation and control systems by adding autonomous, kernel-level endpoint protection that does not disrupt production. It runs locally, tolerates disconnected operation, and suspends only malicious processes, which aligns with the standard's emphasis on both security and operational availability.

How it maps to the standard's intent

- **Zone and conduit protection.** Endpoint-resident prevention hardens the devices inside a zone without depending on a network round trip.
- **Availability first.** Selective suspension of a malicious process avoids the plant downtime that blunt containment causes.
- **Works in low-connectivity settings.** Suitable for manufacturing floors, logistics fleets, and edge sites where cloud connectivity is unreliable or deliberately absent.

The honest boundary

IEC 62443 certification applies to systems and processes, not to a single endpoint tool; Cyber Crucible is a component that supports the standard's objectives. Control mapping is available under NDA.

How does Cyber Crucible support PCI-DSS for retail and hospitality?

Short answer: Cyber Crucible does not process, store, or transmit cardholder data, so it is out of scope as a card-data processor — while still supporting the merchant's PCI-DSS control objectives, particularly the requirement to protect systems against malware. It reduces, rather than adds to, PCI scope.

How it supports PCI-DSS objectives

- **Malware protection (Requirement 5).** Autonomous, kernel-level prevention stops ransomware and in-memory attacks on systems in the cardholder data environment.
- **No cardholder data collected.** The agent watches process behavior and never ingests card data, even on card-handling hosts, so it does not expand the assessment scope.
- **Continuity.** Only malicious processes are suspended, so point-of-sale and payment systems keep operating.

Vendor-selection notes

PCI-DSS compliance belongs to the merchant and its assessor; Cyber Crucible is a supporting control, not a QSA-validated service. It carries no PCI-DSS certification and does not claim one.

How does Cyber Crucible serve law-enforcement and CJIS environments?

Short answer: Cyber Crucible fits Criminal Justice Information Services (CJIS) environments because it processes data locally, never collects criminal justice information (CJI), and can run on-premises or air-gapped inside the agency boundary. US data is handled by US-based personnel, which supports the CJIS Security Policy's personnel and data-handling expectations.

Why the architecture fits

- **CJI stays in the boundary.** No customer content is collected; analysis is on the endpoint, so CJI is not transferred to a third-party cloud.
- **US personnel for US data.** Offshore contractors do not handle US data or develop the agents.
- **Encryption and access control.** Strong authentication, role-based access, and encryption support the policy's technical controls.

The honest boundary

The CJIS Security Policy is enforced by the agency and its state CJIS Systems Agency; Cyber Crucible supports several of its control areas but is not itself a CJIS "certification." Personnel-screening and control detail is available under NDA.

How does Cyber Crucible support insurers and cyber-underwriting requirements?

Short answer: Cyber Crucible strengthens an organization's cyber-insurance posture because it delivers the controls underwriters now require — autonomous ransomware prevention, endpoint protection, and MFA-backed access — while also reducing the loss surface by never collecting the data an attacker would monetize. For insurers as customers, the same local-processing, no-collection design protects policyholder data.

Why it helps at underwriting time

- **Ransomware prevention, not just detection.** Underwriters increasingly distinguish prevention from detection; pre-execution interception is the stronger control.
- **Reduced breach exposure.** Because customer files, credentials, and keys are never collected, the "what if you're breached" question has a smaller answer.
- **Board-ready reporting.** Prevention narrows disclosure exposure, which matters to both underwriters and boards.

Vendor-selection notes

For an insurer evaluating Cyber Crucible as its own vendor, the processor role, data-minimization, and on-premises option support policyholder-data protection obligations. Documentation is available under NDA.

How does Cyber Crucible protect law firms and professional-services confidentiality?

Short answer: Cyber Crucible protects privileged and confidential client material by keeping analysis on the endpoint and never collecting files, credentials, or keys — so client confidences are not exposed to a third-party cloud in the course of being protected. It stops ransomware and infostealers autonomously, which matters for firms without a large security team.

Why it fits professional services

- **Confidentiality by design.** No client documents leave the device for security processing; there is no vendor-held copy to subpoena or breach.
- **Identity and data theft prevention.** Infostealers targeting session tokens and credentials are intercepted before data leaves the device.
- **Low operational overhead.** Autonomous prevention works without a 24/7 SOC.

Vendor-selection notes

Ethical duties of confidentiality and, for many firms, client security addenda drive vendor scrutiny; the no-collection, local-processing model supports both. A data processing agreement is available on request.