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.

Revision #2
Created 2026-07-23 15:18:27 UTC by Dennis Underwood
Updated 2026-07-23 18:19:57 UTC by Dennis Underwood