How does Cyber Crucible make a decision in under 200 milliseconds?

Short answer: It runs a three-step loop — Detect, Decide, Respond — entirely on the endpoint at the kernel level, using a patented edge computing analytics engine. Because nothing has to travel to a cloud service and back, and no human is in the loop, the whole cycle completes in under 200 milliseconds.

The loop

1. **Detect** — novel kernel-level sensors identify malicious behavioral patterns in memory, process activity, and file access.
2. **Decide** — the AI-enhanced behavioral model assesses the intent of the program's data access instantly.
3. **Respond** — if intent is malicious, the program is intercepted and suspended.

Why local processing is non-negotiable

Sending telemetry to a cloud server, waiting for analysis, and receiving a response back adds milliseconds the attack will happily use. For context on the scale involved: this decision happens faster than a nerve impulse travels from your eye to your brain. Any architecture with a network round trip in the critical path has already lost that race.

Raw telemetry is still copied to servers afterward for evidence and enrichment — but the protective decision never waits for it.

Revision #3
Created 2026-07-20 19:23:49 UTC by Dennis Underwood
Updated 2026-07-21 19:32:05 UTC by Dennis Underwood