Is Cyber Crucible an EDR, XDR, MDR? Or Something Else Like Agentic AI?

Short answer: It has elements of both EDR and XDR, but the category question is the wrong one. What matters is *where the decision is made*. Cyber Crucible's response logic runs entirely on the endpoint using only information available there at the moment of attack — because remote analytic servers introduce two fatal weaknesses: latency and fragility.

The honest answer to the label question

- **As an EDR:** if an EDR uses endpoint telemetry to make decisions, then Cyber Crucible's automated response is an EDR. It clamps down on extortion behaviour in milliseconds, using only local information.
- **As an XDR:** telemetry is also sent to a database (customer appliance or central) for correlation, threat hunting, insider-threat work, and IT audits. By the XDR marketing definition, that qualifies.

The team is comfortable with "EDR for extortion defense," even though edge computing is seen as last-generation in some circles. The reasoning below is why that view is backwards.

Why remote analytics became a liability — latency

The "X" in XDR represents moving analytical computing power to remote servers. That buys power and costs time, and attackers built their tradecraft around the gap:

- **Speed:** attacks were accelerated so irreversible actions complete before an analytic server can respond. This is especially visible with small, high-value items like passwords.
- **Parallelism:** many endpoint tools inspect one program, wait, then move to the next. Attackers run multiple extortion programs at once — 5,000 files accessed in parallel instead of 500.
- **Distribution:** extortion runs across many machines simultaneously. Cyber Crucible has observed roughly 75 machines at once. A tool then faces 50 programs across 75 machines — 3,750 programs to inspect.

- **Commander processes:** some attackers run a local controller that instantly re-spawns any extortion tool that gets killed.

Detection-and-response strategies wait, by their nature, for the attack to be underway. The better analogy is stopping bank robbers at the door rather than after a certain amount of cash has left the safe.

Why remote analytics became a liability — fragility

Around 80% of EDR and XDR solutions need access to remote analytic servers to function optimally, and are barely functional without that cloud "brain."

Attackers exploit this directly: gain enough access to change firewall rules, block the endpoint tool from reaching its analytic servers, and the tool loses its ability to analyze or respond. It remains unexploited, installed, running — and almost completely ineffective.

What Cyber Crucible does instead

Because latency and fragility make cloud dependency untenable for extortion defense, Cyber Crucible invented a detection and response capability whose behavioral analytics use **only information available on the endpoint at the time of attack**. Interdiction happens locally in typically under 200 milliseconds, with no cloud round trip in the critical path.

The telemetry that does flow to the database supports investigation rather than protection — threat hunting, insider threat detection, IT audits — and an open API lets it feed open XDR platforms, SOAR, or RPA tooling. That work is valuable, but it is never what stands between you and an attack in progress.

Revision #5
Created 2026-05-18 20:26:57 UTC by Dennis Underwood
Updated 2026-07-21 19:31:57 UTC by Dennis Underwood