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

Cyber Crucible’s data extortion prevention software is, strictly speaking, a Windows kernel driver and Windows service. The software communicates with our remote servers for ingestion (mostly using REST). Upon ingestion to the Cyber Crucible servers (whether as a Kubernetes' based end user deployment, or our cloud presence), multiple data sources are combined to provide additional capabilities to advanced security users.

Locally to the machine (the **Endpoint**), behavioral analytics are used to **Discover** data extortion attack behaviors, and **Respond** by suspending the associated programs, making Cyber Crucible an EDR. The use of cloud analytics to provide additional data would, by the definition of the marketers of XDR (eXtended Discovery Response) products, means Cyber Crucible is an XDR product.

So, what’s the answer, then?
The team is OK with Cyber Crucible being called an EDR for extortion defense due to the edge computing, even though that’s seen as “last generation” in some circles The reason is that the X in XDR represents an evolution of an endpoint tool strategy in place in EDR’s as well, in that analytical computing power has been moved to remote servers (usually in a cloud of some type). With that additional power, comes two drawbacks: latency, and fragility.

Remote Analytic Latency as a Liability

Extortion criminals first focused on the speed of their attack, to turn the latency into a liability. This is expressed during attacks in a couple ways. The first being that, the attackers sped up their efficiency to ensure that irreversible attack actions were completed before the analytic server could respond. We see that a great deal with small pieces of very important data such as passwords.

It is really important to note here that we are discussing detection and response strategies which, by their nature, wait for the attack to be underway. A non-cybersecurity analogy would be the more desirable detection of bank robbers outside the bank, and locking the door, versus a less desirable stance of the bank taking action to stop the robbers after a certain amount of cash was stolen from the safe.

Longer running tasks like encryption required a combination of speed with 2 other tactics - parallel and distributed computing. The attackers realized that running multiple extortion programs meant that any endpoint security tool had to inspect the behavior of each process, which takes time. So, if 5000 files could be accessed on the network at one time in parallel on a system instead of 500 with one program, that's much better for the attacker. In fact, many of the endpoint security solution are setup to inspect one program, wait for that inspection to finish, then move onto the next one.

The extortionists do not have 10, 25, or 50 malware programs running just on one machine though. They leveraged distributed computing methods to have the extortion run on many machines all at the same time. The most the Cyber Crucible has seen at once was around 75 machines. Now any type of security tool has to inspect 50 programs, across 75 machines - so 3,750 programs.

As if this isn't bad enough, some attackers began implementing a strategy, in which the extortion tools were monitored and controlled locally by a "commander" program. This commander would re-spawn extortion tools if they were killed. Like in a lot of science fiction, killed "enemy soldiers" (extortion software) were instantly replaced by fresh "troops".

By this point in the extortion tool and tradecraft evolution, any tool that relied on remote analytic computing, are simply overwhelmed. Modern attacker tactics also no longer encrypt every piece of data in a business. By the time defenders "catch up", the attacker's goals are likely already accomplished.

We'll discuss what Cyber Crucible does to correct this matter at the end.

Remote Analytic Fragility as a Liability

Previously, we discussed exploiting the latency of remote analytics infrastructures through the use of parallel and distributed computing. In this section, we'll discuss the fragility of building endpoint security tools remote analytics.

Around 80% of EDR and XDR solutions require access to remote analytic servers to function optimally. The norm is that these tools are barely functioning without access to the remote (usually cloud-based) "brain".

Attackers have combined the latency vulnerability discussed earlier, to conduct fast attacks on the EDR and XDR software.

A common attack now seen is that the attackers gain access to adjust firewall rules, and block the endpoint security tools from accessing their analytic servers. The net effect is that the EDR/XDR tools lack the ability to analyze and respond to the extortion attack activities, making the attackers' job that much easier.

Exploits against EDR and XDR software are certainly seen against endpoint software. In this case, though, the EDR or XDR can remain unexploited, installed, running - and almost completely ineffective.

What All This Means to Cyber Crucible - *IS* it an EDR or XDR?

The vulnerabilities concerning the latency and fragility of remote analytic server strategies, mean robust data extortion simply cannot rely on cloud computing. Cyber Crucible has elements of both EDR and XDR.

Cyber Crucible as an EDR

If we reduce an XDR to enable a combination of endpoint and other (usually things like network) telemetry, and define and EDR as strictly using endpoint telemetry to make decisions…

Then the millisecond-fast “clamping down” of extortion attack behaviors, that has to be resilient to the frailty of remote analytic engines…

Then Cyber Crucible’s automated response portion of the software is an EDR.

Due to the latency and frailty of remote analytic servers, Cyber Crucible had to invent a detection and response capability whose behavioral analytics use only information available on the endpoint at the time of attack.

Cyber Crucible as an XDR

The collection of endpoint telemetry for edge (endpoint) detection and response is valuable for a variety of other strategic investigatory activities such as threat hunting, insider threat detection, and IT audits. All telemetry is transmitted to the database (either customer appliance, or central Cyber Crucible database) for correlation and analysis. Data sources are combined and collated for rich data presentation.

Cyber Crucible’s open API means that analytical platforms (such as open XDR platforms like this, SOAR, or Robotic Process Automation) may combined this data with other data sources, to produce advanced automated capabilities.

Thus, this portion of Cyber Crucible’s capabilities, while not as time critical as the sub-second response required by our software’s EDR capabilities in times of impending extortion crisis, represents an value add to customers.

Revision #2
Created 2026-05-18 20:26:57 UTC by Dennis Underwood
Updated 2026-07-13 20:07:24 UTC by Dennis Underwood