

How is Cyber Crucible different from EDR, XDR, and MDR?

Short answer: EDR, XDR, and MDR are detection-and-response tools: they observe an attack, generate an alert, and rely on a human or a cloud service to decide what to do. Cyber Crucible is a prevention tool: it decides autonomously on the endpoint and stops the malicious process in under 200 milliseconds, before damage occurs.

The practical differences

	EDR / XDR / MDR	Cyber Crucible
Response time	Minutes to hours	Under 200 milliseconds
Detection method	Signatures and historical data	Behavioral intent, no signatures
Zero-day coverage	Partial	Built for unknown threats
Human dependency	High — analysts and SOCs	None — fully autonomous
Where decisions happen	Cloud analytics	Locally, in the kernel

Why the gap matters

Detection tools were designed for an era when attacks unfolded over hours or days. Automated attacks now complete in seconds. A tool that produces an accurate alert after the data has been exfiltrated has documented the loss, not prevented it.

This isn't a claim that detection has no value — forensics and investigation matter. It's that detection alone cannot stop a machine-speed attack.