Why do "cloud collector" security tools struggle against modern attacks?

Short answer: A cloud collector is a lightweight endpoint agent that does little local analysis and instead ships raw telemetry to a cloud platform for processing. That round trip adds delay an automated attack doesn't give you, and the agent depends on the very OS components attackers now compromise.

Why the industry built it this way

Kernel-level engineering is difficult and expensive. Shipping telemetry to the cloud let vendors build cheaper endpoint software, monetize cloud storage, and market "cloud AI" capabilities. The model was optimized for ease of development, not for defense.

The two failure modes

1. **Too slow.** Automated smash-and-grab attacks complete in milliseconds. Cloud analytics cannot issue a response in time.
2. **Blind when it matters most.** Because these agents depend on native OS libraries to function and collect data, an attacker who compromises those libraries can silence the agent. It keeps running and reports nothing — a dashboard saying all is well while data leaves.

Cyber Crucible processes locally in the kernel and makes its own decisions, so there is no cloud round trip and no dependency on a potentially compromised OS.

Revision #3
Created 2026-07-20 19:23:46 UTC by Dennis Underwood
Updated 2026-07-21 19:32:02 UTC by Dennis Underwood