What happened to the security industry's "dumb collector" model?

Short answer: For years vendors advised that local endpoint processing was obsolete and pushed lightweight agents that forward raw telemetry to cloud analytics. Modern in-memory attacks against core OS libraries have exposed that model — the agents keep running but go effectively blind and mute.

Why the model was adopted

It was cheaper to build. Kernel-level engineering is difficult and expensive; shipping telemetry to the cloud let vendors ship inexpensive endpoint software, monetize large cloud storage pools, and market cloud AI capabilities. The model optimized for development economics, not defense.

Why it's failing now

These agents depend entirely on native operating system components to function and gather data. When attackers compromise those components in memory, the agent doesn't crash — it stays running and reports nothing, leaving a dashboard that says everything is fine while data is exfiltrated.

There's also documented deliberate interdiction: attackers, and in some verified instances competitors seeking to mask their own flaws, actively exploiting these library dependencies to force-terminate or sabotage endpoint defenses.

The architectural dead end

Fixing this would require legacy vendors to abandon cloud-first telemetry pipelines and rebuild for local, kernel-level edge computing — a multi-year effort. Recent acquisitions and venture investment show the industry moving further toward cloud analytics and centralized data lakes instead.

Revision #3
Created 2026-07-20 19:24:19 UTC by Dennis Underwood
Updated 2026-07-21 19:32:33 UTC by Dennis Underwood