What is a fileless (in-memory) attack?

Short answer: A fileless attack is one that never writes a program to disk. The attacker injects malicious code directly into the memory of a legitimate, trusted process and builds their payload there. Because no file is ever created, security tools that scan files — including most EDR — have nothing to find.

Why it defeats file-based tools

Traditional endpoint protection is built around a simple assumption: malware is a file, so inspect files. Fileless tradecraft removes the file entirely.

In one real deployment, a financial services firm ran three industry-leading EDR products (Microsoft, CrowdStrike, and Sophos) alongside a Top-50 managed SOC. Attackers compromised a trusted remote monitoring tool, injected code into Microsoft SQL Server management processes, and compiled their ransomware and data-theft malware directly in server memory. Because nothing touched the hard drive, all three EDRs, the MDR, and the SOC were entirely blind. Cyber Crucible autonomously intercepted nearly 10,000 malicious processes — 98% of them on the SQL server farm — without a single alert from the legacy stack.

How Cyber Crucible sees it

Cyber Crucible watches behavior and intent at the kernel level rather than scanning files. A process acting maliciously is stopped in under 200 milliseconds whether or not a file was ever written.

Revision #3
Created 2026-07-20 19:23:35 UTC by Dennis Underwood
Updated 2026-07-21 19:31:49 UTC by Dennis Underwood