USE CASE

SAVING A FINTECH
from the Invisible Attack

Why 3 EDRs, an MDR, and a Top-50 MSSP completely missed a 10,000-attempt ransomware event—and how Cyber Crucible stopped it autonomously.

The Illusion of Security

A major financial services firm had built what looked like an airtight security posture. They deployed three different industry-leading EDR tools (Microsoft, CrowdStrike, and Sophos) across their endpoints. They outsourced their 24/7 monitoring to a Top-50, private-equity-owned MSP and MSSP.

Despite this massive investment, leadership felt a blind spot existed in the noise of low-confidence alerts. They deployed Cyber Crucible to see what their stack was missing.

Sixty days later, they found their answer.

The Discovery

Without generating a single alert from the legacy EDRs or the SOC, Cyber Crucible had autonomously intercepted and suspended almost 10,000 malicious processes. 98% of these attacks were executing directly on their highly privileged Microsoft SQL server farm.

Anatomy of a Fileless Hack

How do 10,000 attacks go completely unnoticed by millions of dollars worth of security software? By never touching the hard drive.

1. **The Hijack:** Attackers bypassed the perimeter by compromising the MSP's highly trusted remote monitoring tool (Kaseya).
2. **The Injection:** Because Kaseya is both highly privileged and trusted, the hackers used it to inject malicious code directly into the MS SQL Server management processes.
3. **In-Memory Compilation:** Hackers built their ransomware and data-theft malware directly in the server's memory. Because no files were ever written to disk, the EDRs, MDR, and SOC were entirely blind.

Camera vs. Guard

Legacy EDR acts like a security camera—it records the disaster so a human can investigate it later. Attackers know this, so they wear an invisibility cloak (in-memory execution) and walk right past the cameras. Cyber Crucible is the armed guard. We don't just watch; we tackle the thief the millisecond they touch the vault, intercepting and stopping the threat in under 200 milliseconds.

sales@cybercrucible.com | www.cybercrucible.com

The Conflict: Denial & Vindication

When the internal team presented the 10,000 blocked attacks, the outsourced SOC dismissed them as false positives. Why? Because their legacy tools saw nothing. Even after running simulated "war games," the incumbent EDRs were incapable of detecting the in-memory injections.

Cyber Crucible engineering traced the root cause to a likely compromised RMM credential. Fifteen days after this was communicated, the attacks mysteriously stopped.

The Global Vindication

For months, the industry had no knowledge of this new attacker tradecraft. It wasn't until the fall of 2022 that global security news outlets exploded with reports of a new wave of ransomware (TargetCompany/FARGO/Mallox) backdooring MS SQL servers worldwide. The financial sector suffered devastating breaches and massive data extortion.

The Cyber Crucible client? **They were never a victim.**

Real ROI for the CISO

Resilience tools accept the breach as inevitable; defense means stopping it before execution. Because Cyber Crucible operates autonomously at the kernel level, detecting intent in under 200 milliseconds, the CISO delivered four massive wins to the board:

The Bottom Line

Zero Business Takedown
Attacks were suspended in memory; operations continued without disruption. Legitimate SQL transactions never stopped.

Zero Regulatory Disclosure
Because the attack was stopped pre-execution and no data was touched, there were no required notifications to customers, vendors, or government regulators.

Zero PR Nightmare
There were no headlines, preserving complete customer trust and avoiding PR disasters.

Massive ROI
A fraction of the cost of their legacy stack did all the heavy lifting, proving that more tools don't equal better security.

Stop the attacks your EDR is designed to miss.

In a world of automated, machine-speed attacks, human-driven SOCs and file-based EDRs cannot keep up.
Cyber Crucible delivers pure, autonomous prevention.

Let us prove it. Contact us today for a technical briefing.

sales@cybercrucible.com | www.cybercrucible.com