

We were breached recently. Can Cyber Crucible be deployed into an environment that may already be compromised?

Short answer: Yes. Cyber Crucible evaluates what programs are doing right now rather than searching for known-bad files, so it begins stopping malicious behavior on deployment — including from an attacker who already has a foothold.

Why prior compromise doesn't blind it

Because prevention is based on behavioral intent at the kernel level, an attacker who is already resident still has to *act* — accessing identity data, injecting into processes, beginning encryption, or moving data. Those actions are exactly what triggers interception.

This is how the financial services deployment surfaced an active, ongoing intrusion the existing stack had never alerted on. Cyber Crucible wasn't brought in to investigate a known breach; it was deployed to look for a blind spot, and it found nearly 10,000 malicious processes already in progress.

What to expect

Deploying into a compromised environment often produces immediate, high-volume interception activity. That is the tool working as intended, and it is frequently the first hard evidence an organization has that something was already underway.

Revision #3

Created 2026-07-20 19:24:15 UTC by Dennis Underwood

Updated 2026-07-21 19:32:29 UTC by Dennis Underwood