# Sufrimos una brecha recientemente. ¿Se puede desplegar Cyber Crucible en un entorno que ya podría estar comprometido?

**Respuesta breve:** Sí. Cyber Crucible evalúa lo que están haciendo los programas en tiempo real, en lugar de buscar archivos que ya se sabe que son maliciosos, por lo que comienza a detener el comportamiento malicioso desde el momento de su despliegue, incluso frente a un atacante que ya cuenta con un punto de apoyo.

## Por qué un compromiso previo no lo deja ciego

Dado que la prevención se basa en la intención conductual a nivel del kernel, un atacante que ya está presente en el entorno de todos modos tiene que *actuar*: acceder a datos de identidad, inyectarse en procesos, iniciar el cifrado o mover datos. Esas acciones son precisamente las que activan la intercepción.

Así fue como el despliegue en el sector de servicios financieros reveló una intrusión activa y en curso sobre la que la pila de seguridad existente nunca había generado una alerta. Cyber Crucible no se implementó para investigar una brecha ya conocida; se desplegó para buscar un punto ciego, y encontró casi 10,000 procesos maliciosos ya en marcha.

## Qué esperar

Desplegar la solución en un entorno comprometido a menudo genera actividad de intercepción inmediata y de gran volumen. Eso es la herramienta funcionando tal como está diseñada, y con frecuencia constituye la primera evidencia sólida que tiene una organización de que algo ya estaba en curso.

---

Revision #1
Created 2026-07-24 01:52:51 UTC by Dennis Underwood

Updated 2026-07-24 01:52:51 UTC by Dennis Underwood