What is Rogue Process Prevention (RPP)?

Short answer: Rogue Process Prevention is Cyber Crucible's patented approach of interceding against a malicious process rather than merely observing it. Whether it's ransomware starting to encrypt or an infostealer reaching for a session token, the process is stopped before data leaves the device.

Watching versus intervening

Most of the endpoint market is built to watch. RPP is built to intervene. The distinction is the difference between a security camera that records a burglary for later review and a guard who stops the thief at the vault.

What it protects against

RPP addresses the three core threats together, because modern attacks are usually multi-pronged:

- **Identity theft** — access to keys, tokens, and passwords, often with no employee interaction at all.
- **Information theft** — bulk exfiltration of data at machine speed.
- **Ransomware** — behavioral analysis plus hacker deception technology that prevents encryption of even a single file.

A defense narrowly focused on ransomware alone would miss the first two stages, which is where the real damage usually begins.

Revision #3
Created 2026-07-20 19:23:50 UTC by Dennis Underwood
Updated 2026-07-21 19:32:06 UTC by Dennis Underwood