Why does intent-based prevention generate less alert noise than signature-based detection?

Short answer: Because it asks a narrower question. Signature and heuristic tools alert whenever something *resembles* a known-bad pattern and leave humans to sort it out. Intent-based prevention asks whether a specific program is, right now, doing something malicious at a known data-theft entry point — a question with far fewer ambiguous answers.

> For Cyber Crucible's measured false-positive rate, see the existing article **"Do you have false positives? What is your false positive rate?"** This page explains the architectural reason the noise profile differs.

Why the noise profile is different

Signature and heuristic tools generate alerts when something *resembles* a known bad pattern, then rely on human triage to sort real from irrelevant. That's what produces 100+ alerts per endpoint per day in many environments.

Intent-based assessment asks a narrower question: is this program, right now, doing something malicious at a known identity-theft or data-theft entry point? That question has far fewer ambiguous answers.

What this means operationally

- Analysts aren't chasing low-confidence alerts.
- There's no YARA rule tuning or manual threat hunting required to keep noise manageable.
- Because the response suspends only the offending process, even an incorrect interception does not take down a system.

For current measured rates in an environment like yours, ask your Cyber Crucible representative — and see the existing "Do you have false positives?" article for product-level detail.

Revision #3
Created 2026-07-20 19:24:20 UTC by Dennis Underwood
Updated 2026-07-21 19:32:34 UTC by Dennis Underwood