What role does memory analytics play across the platform?

Short answer: Memory analytics is the foundation everything else is built on. It is the sensor and analytic source feeding all behavioral modeling — data protection, identity protection, and FortressAI alike. Every decision those capabilities make rests on knowing what a program's memory is actually doing.

One foundation, three capabilities

Cyber Crucible tracks the state of a program's memory across its entire lifecycle, from start to end, including its in-memory interactions with other programs. That single stream of analysis is what makes the rest possible:

- **Data protection** — is this process behaving like something about to encrypt or exfiltrate?
- **Identity protection** — is this process the legitimate owner of the credential it's reaching for, or has it been taken over?
- **FortressAI** — is this AI tool still itself, and is its data access within policy?

These aren't three separate engines with three separate sensor sets. They are three policies expressed on top of the same memory behavioral model.

Why memory is the right foundation

Modern attacks increasingly leave no file to inspect. Code is injected into trusted processes and built in memory, so the only place the activity is visible is the memory state of a running program. A defense that can't see there is blind to the entire class.

Memory analysis also answers the question that matters most before granting access to anything sensitive: **is this program still what it claims to be?** A trusted application whose process or libraries have been tampered with is no longer trustworthy, and only memory-level inspection reveals that.

Not memory scanning

This is live behavioral tracking, not periodic scanning. Scanning copies a block of memory and analyzes the snapshot — a photograph rather than live footage. On a busy machine the program's state may be entirely different a moment later, which makes snapshots useful for controlled forensics and much weaker for real-time defense.

> See also the existing *Memory Analytics* articles for the technical detail on how this differs from memory scanning, and what happens when a memory attack is found.

Revision #3
Created 2026-07-20 19:23:51 UTC by Dennis Underwood
Updated 2026-07-21 19:32:07 UTC by Dennis Underwood