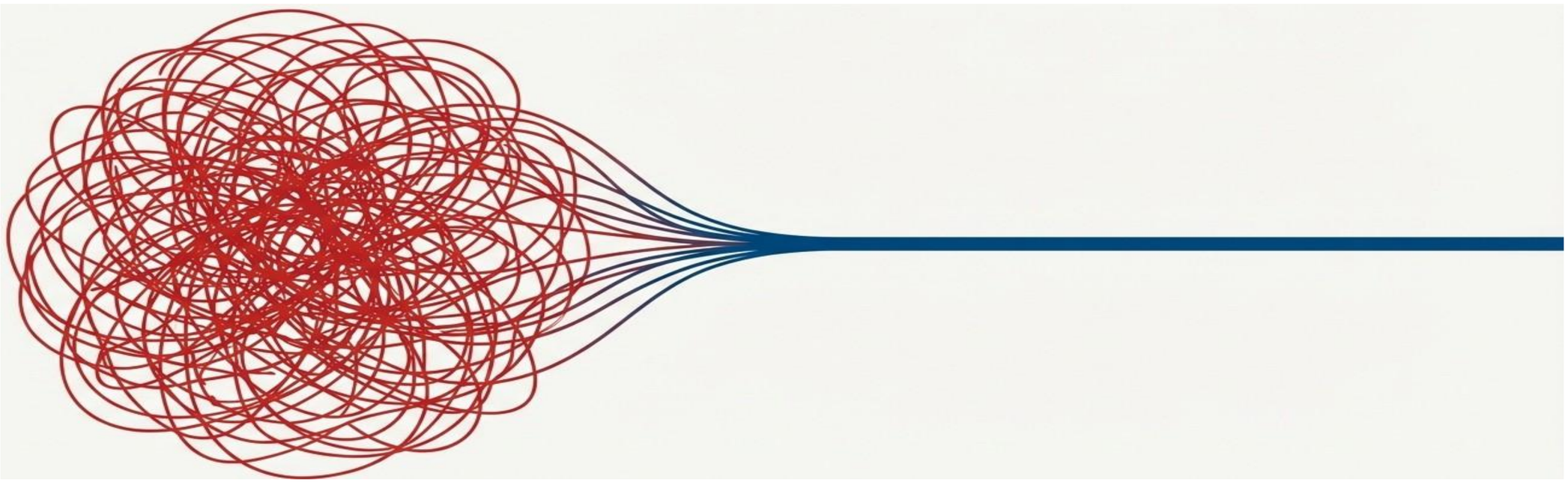
OnSystem Logic™

Security is an Infinite Problem, Until Now.

OnSystem Defender: From Probabilistic Detection to Deterministic Enforcement.



Modern Security is Built on a Losing Premise: Chasing Infinite "Bad."

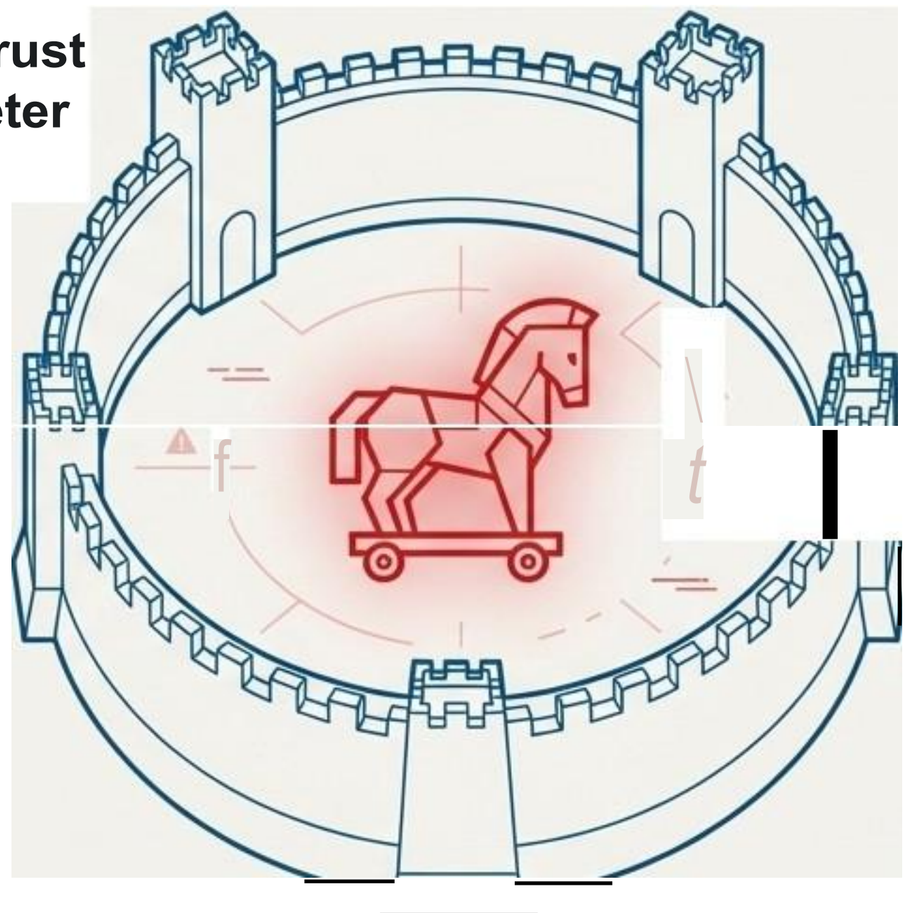
Traditional solutions assume an effectively infinite attack surface, leading to a predictable set of failures.

Trusted Software Becomes a Weapon: Signed and trusted applications are routinely abused to bypass defenses.

Memory is the True Battlefield: Fileless and memory-only attacks bypass conventional file-based controls.

Alerts Create Noise, Not Clarity: Security teams are overwhelmed by low-confidence alerts, replacing prevention with detection, response, and cleanup.

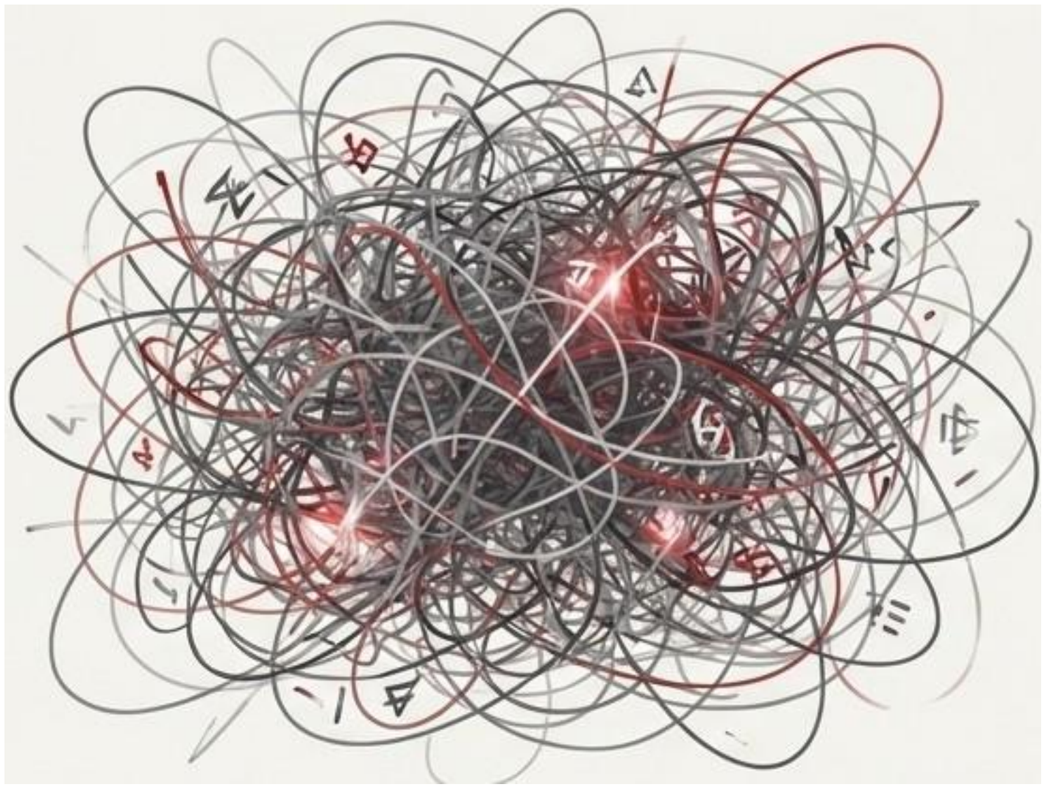
Zero Trust Governs *Authorization*, Not *Execution*.



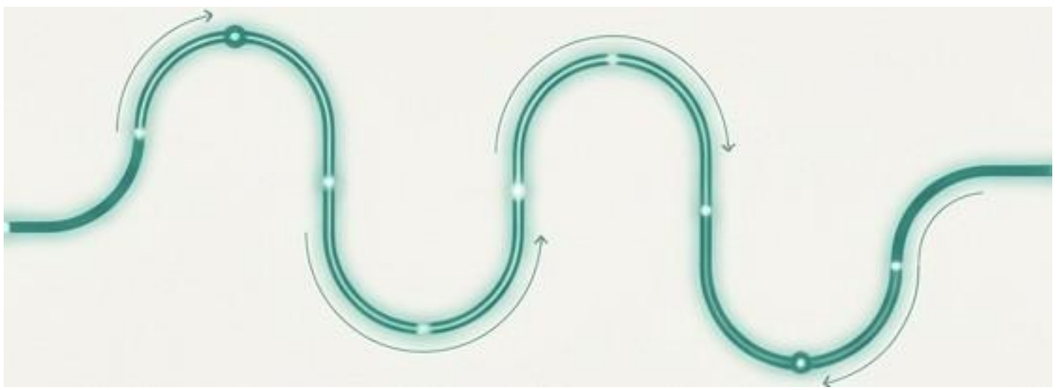
A compromised endpoint renders identity and access controls irrelevant. The device itself is the last line of defense.

- Any data that device can access becomes accessible to the attacker.
- The device becomes a launch point for lateral movement, fully compliant with identity controls.

Legitimate Software Follows a Finite Number of Paths



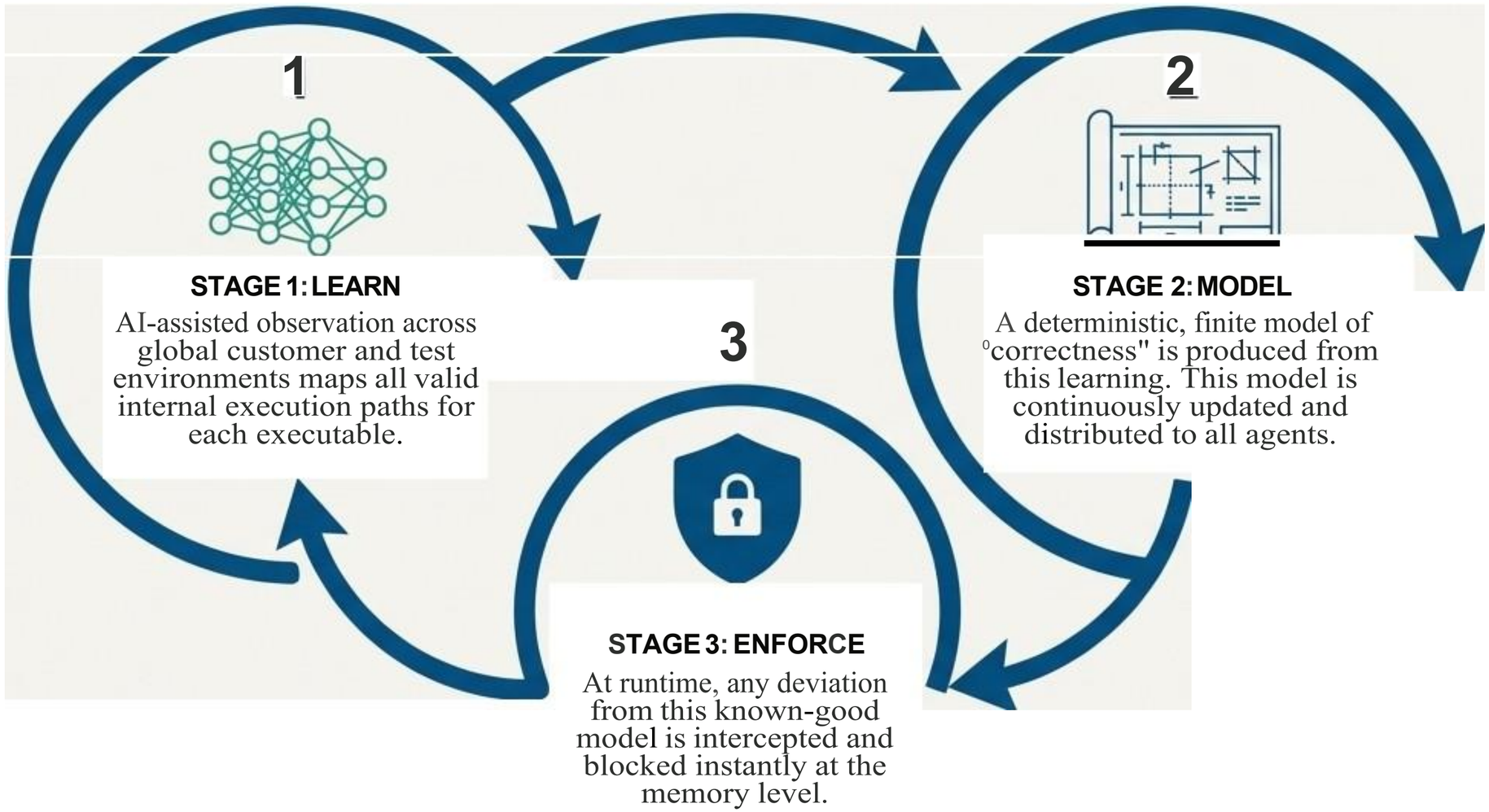
INFINITE ATTACK VECTORS



FINITE EXECUTION PATHS

While there are infinite ways to attack software, legitimate software only executes through a finite set of correct internal code paths. What if security wasn't about finding a needle in a haystack, but simply ensuring the needle stays on its known thread?

We Learn and Enforce the Finite "Good."



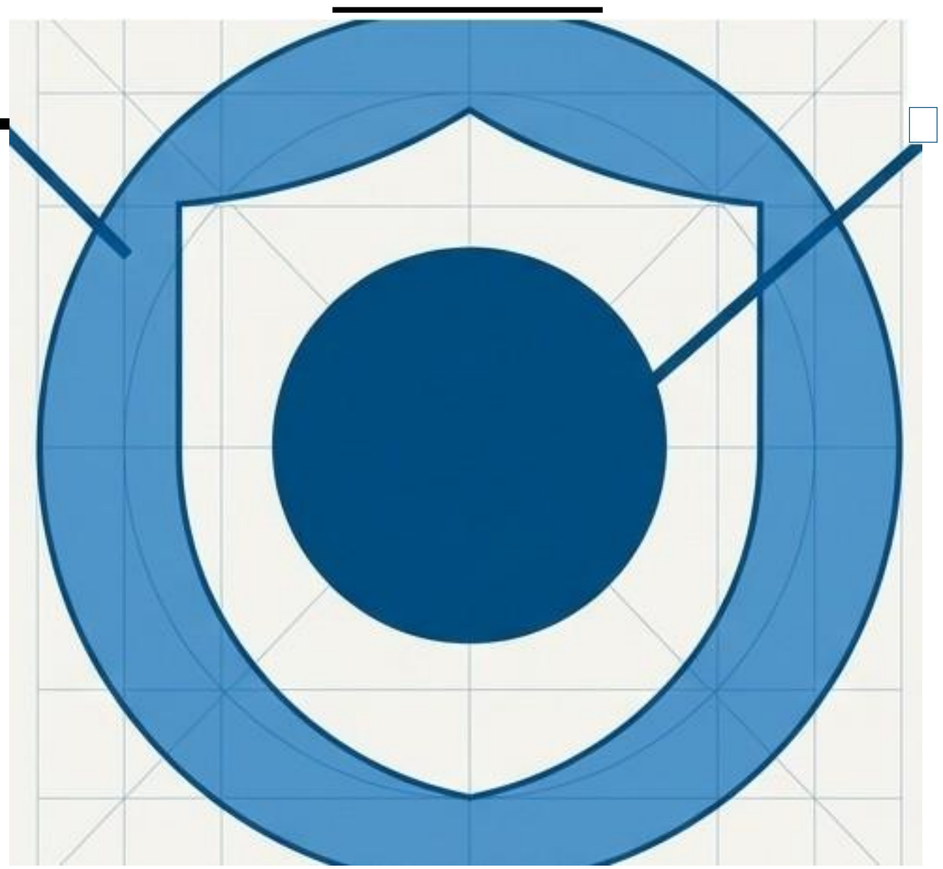
This process reduces the attack surface from infinite to a small, known, and enforceable set.

Two Layers of Deterministic Control

Outer Layer: Simple Application Control

Controls *what starts*. Drastically reduces the initial attack surface with minimal admin effort.

- Relies primarily on digital signatures and software publishers, not manual rules.
- Allows routine updates to work without constant tuning.
- Low operational overhead.



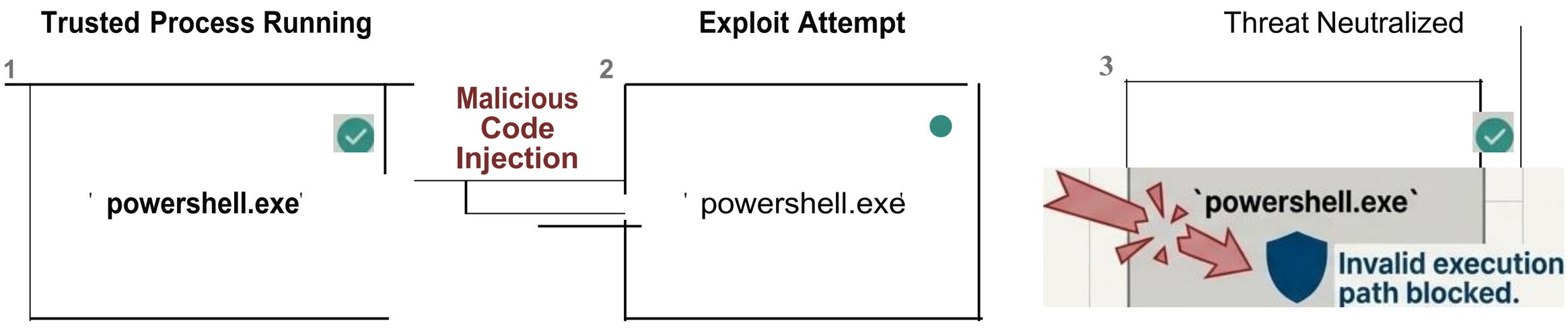
Inner Core: Deterministic Memory Protection

Controls *how it runs*. Stops exploits inside trusted applications that Application Control has already allowed.

Stopping Attacks *Inside* the Process

Allow-listing only controls *what starts*. It does not control *what happens next.*

OnSystem Defender closes this critical gap by enforcing deterministic memory protection across **all processes,** including trusted, signed applications. If a trusted application is exploited, OSD neutralizes the threat by blocking the invalid execution path within its memory.



The SolarWinds Case: Why Ring-Fencing Fails and Internal Enforcement Succeeds.

Ring-Fencing
“Old Way”

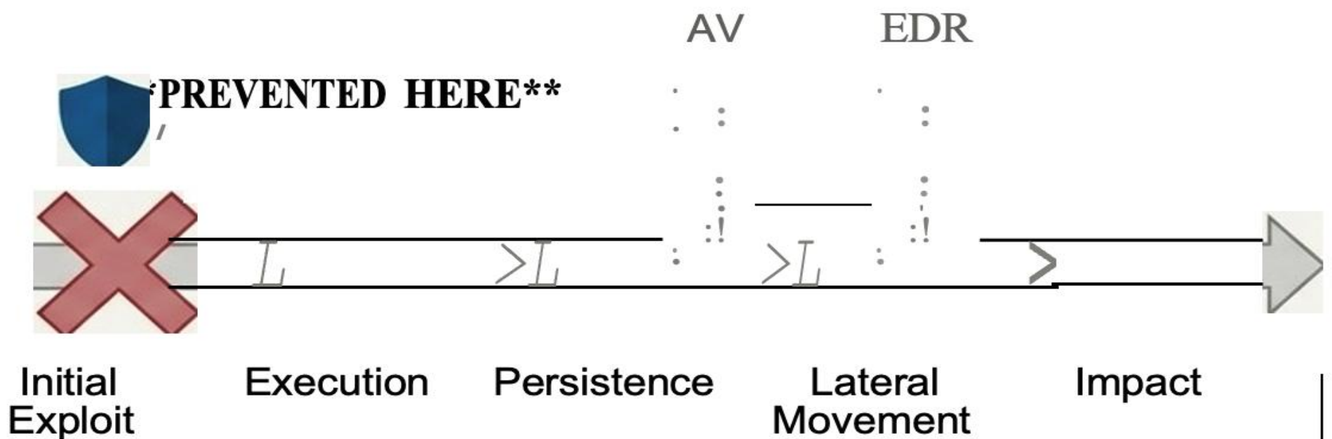
Requires predicting all future external behavior. Brittle, complex, and doesn't scale operationally.

OSD Internal Enforcement
“New Way”

Stops the malicious code at its source, independent of external behavior. Protection is automatic and absolute.

The Result: An Attack Stopped at the First *Invalid Instruction*.

- Zero-Day & N-Day Exploits (including unpatched vulnerabilities)
- Fileless & In-Memory Attacks
- Software Supply-Chain Attacks (like SolarWinds)
- Living-off-the-Land (LotL) Techniques & Abuse of Trusted Software



Block with Confidence or Detect with Certainty

Prevention Mode

Instantly blocks any invalid execution.

The attack never progresses.

Result: No damage, no cleanup, no incident response cycle.

Detection-Only Mode

Generates extremely high-confidence attack indicators.

Confirms *actual exploitation,* not just theoretical risk.

Result: Ends alert fatigue and provides SOC/MDR teams with zero-noise, actionable intelligence.

Powerful Security, Designed for Enterprise Reality.

Effortless Rollout

Deploy in detection-only mode first to ensure seamless integration and verify no system incompatibilities.

Negligible Footprint

Minimal impact on system resources. (Negligible CPU/memory usage, 360 MB storage requirement).

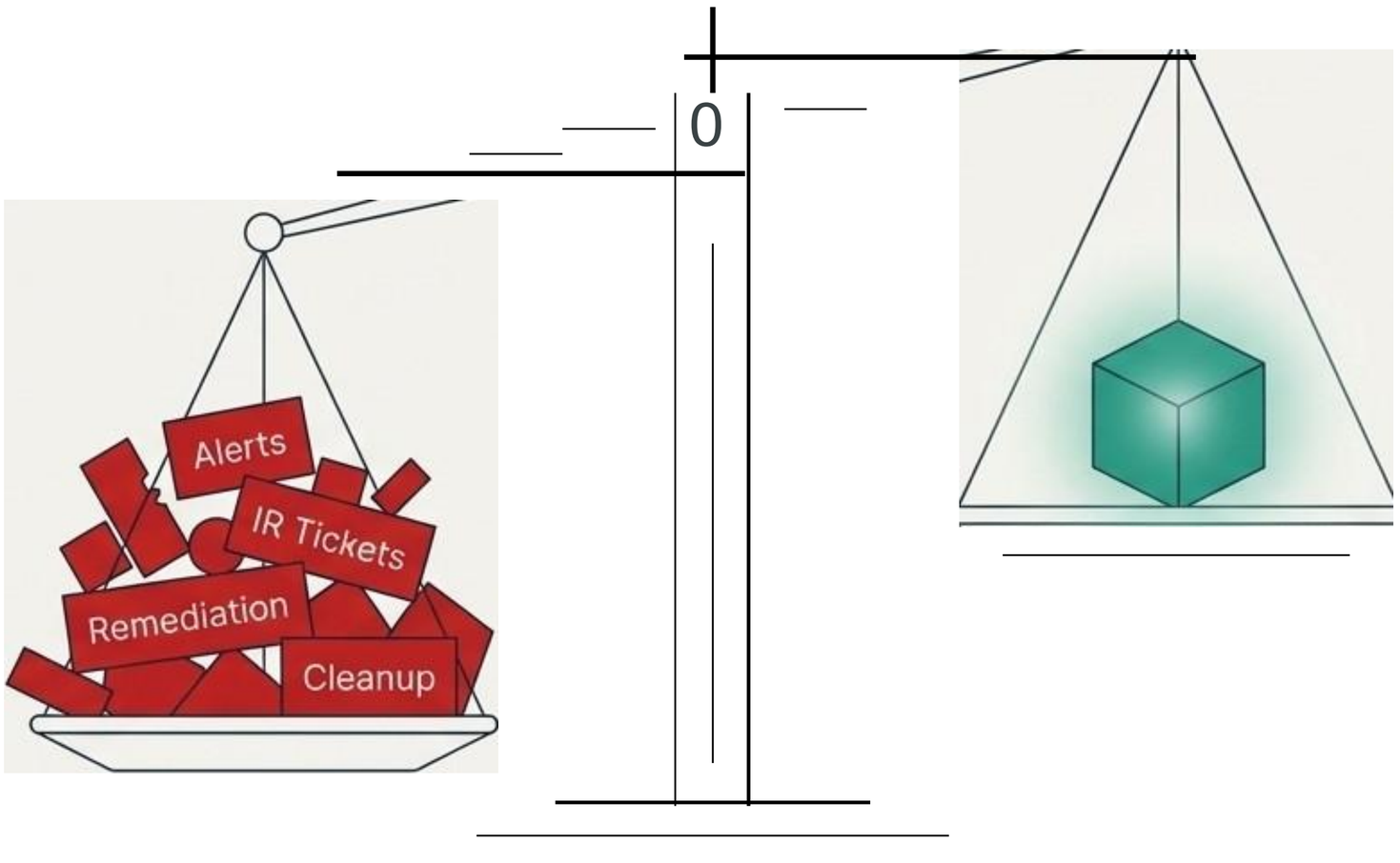
Automated Protection

Centralized learning by OnSystem Logic for memory events means no manual rule authoring is required from administrators.

Flexible Architecture

Natively supports both connected and fully air-gapped environments.

Move from Probability-Based Detection to Enforced Correctness



Reactive Response

Enforced Correctness

The Strategic Benefits:

Dramatically reduced risk from novel and zero-day attacks.

Increased operational efficiency for security teams.

A fortified Zero Trust architecture where execution is as trusted as identity.

The OnSystem Defender Difference.

1. **The Premise:** Enforce the finite set of 'good' execution paths, don't chase an infinite list of 'bad' behaviors.

2. **The Technology:** A simple, publisher-centric Application Control layer combined with deterministic Memory Protection that secures trusted processes from within.

3. **The Result:** True prevention of modern attacks, zero-noise detection signals, and minimal operational overhead.

See Deterministic Enforcement in Action.

Request a Live Demo

Start a Proof of Concept (POC)

info@onsystemlogic.com
www.onsystemlogic.com

OnSystem Logic™

A Final Perspective.

- Zero Trust without runtime enforcement leaves the endpoint exposed.
- Traditional Application Control limits what runs, but not how trusted software is abused.
- ***OnSystem Defender*** uniquely enforces correct execution *inside* every process, preventing modern attacks while allowing legitimate software to operate normally.

This is deterministic security, built for real enterprise environments.