Kernel-Level Enforcement for Enterprise Resilience

MIMIC NETWORKS · $50M SERIES A · GV & MENLO VENTURES · KEVIN MANDIA & TED SCHLEIN, BOARD

RANSOMWARE DEFENSE	VIRTUAL PATCHING	CHANGE CONTROL
Blocks encryption at the kernel. RPO-Zero triggers a backup of protected critical applications from a verified clean state.	Deploys a kernel-enforced mitigation within hours of disclosure. No vendor patch required.	Evaluates every production change against the known-good baseline in real time.

The Threat Has Changed

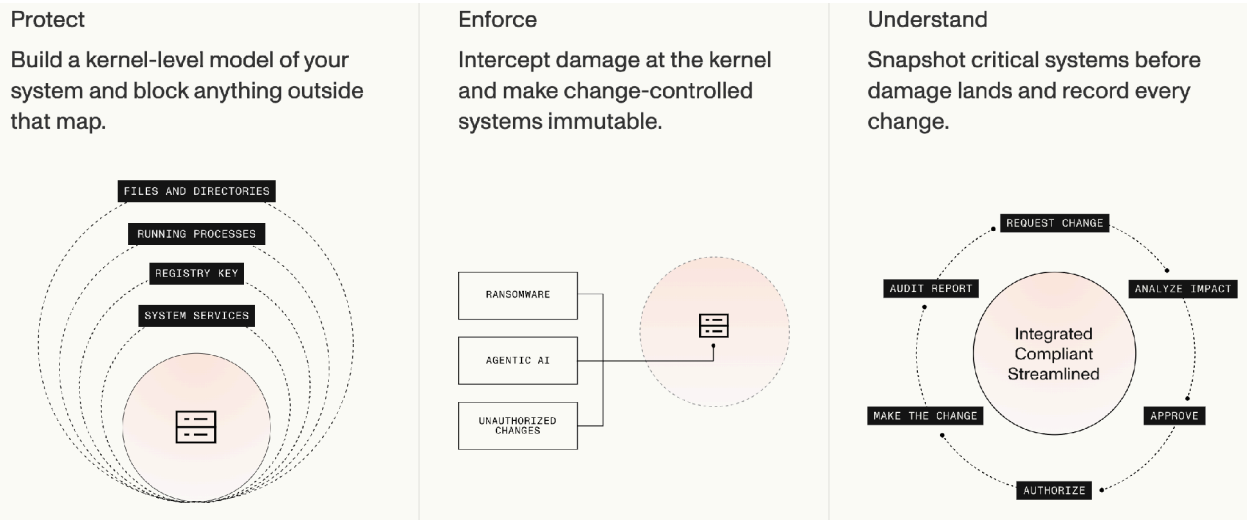
Every successful attack resolves to the same requirement: *something in the system must change*. A file written, a registry key modified, a process altered, a configuration drifted. Ransomware, supply chain compromise, insider misuse, and AI-driven intrusion all depend on it. The only question is whether that change is governed at the moment it happens.

Detection was built to observe behavior and flag what looks wrong. It assumes malicious behavior is observable, that indicators persist, that security tools stay operational when attackers target them, and that human response keeps pace. Agentic AI breaks all four. It runs inside the enterprise on valid credentials and approved tooling, generating change faster than human review was built to handle, while frontier AI discovery has collapsed disclosure-to-exploit from weeks to hours. More signatures and playbooks don't close that gap. Governing change before it executes does.

Known-Good Enforcement: A Different Question

Mimic's foundational principle is known-good enforcement. Systems are profiled in their approved operational state, and that profile becomes the enforcement policy. Every subsequent change attempt is evaluated at the kernel layer before it executes. Authorized changes proceed normally. Changes outside the known-good baseline do not, regardless of source.

This is structurally different from detection-based approaches in one respect: *it doesn't require knowing what the attack looks like, only what the approved state looks like*. A novel exploit with no CVE number, a signed binary performing unauthorized actions, a compromised AI agent with valid credentials, a misconfigured administrative script: *all present the same enforcement question, was this change authorized*? If not, it stops at the kernel, before damage lands.



PROTECT, ENFORCE, UNDERSTAND · THE THREE OPERATIONAL PHASES OF KERNEL-LEVEL ENFORCEMENT

Where Mimic Sits in the Stack

NETWORK & SIEM
Sees traffic between hosts. To an AI-driven attack moving through an authorized session, that is encrypted standard-port traffic with valid credentials: nothing to flag until after impact.

EDR, XDR & ENDPOINT AGENTS
Sees process behavior and matches against known attack patterns. A signed binary, valid credentials, and a novel exploit with no signature all pass through clean. The agent itself can be disabled or tampered with.

KERNEL: MIMIC (RING 0)
Sees and evaluates file writes, registry changes, driver loads, and process actions before they execute. Blocked before it lands, regardless of how it arrived or what credentials carried it.

Each layer above the kernel can be blinded, bypassed, or outpaced. The kernel is the layer every change must still pass through.

Mimic doesn't replace EDR, SIEM, SOAR, or BCDR. Sitting below them keeps their configurations, agents, and data intact even while those tools are the attack's target.

Three Defenses, One Enforcement Layer

Ransomware Defense

Ransomware is a change problem. Encryption modifies files, persistence modifies registry keys and services, lateral movement modifies configurations and credentials. Mimic intercepts each at the kernel in under 50 milliseconds, before damage lands. RPO-Zero triggers a backup snapshot of protected critical applications to a verified clean state, not a time-based snapshot that may already be corrupted. Recovery starts from a state the attack never reached.

Agentic AI operates at machine speed with valid credentials and approved tooling. The risk isn't obvious malware. It's the volume of legitimate-looking actions moving toward an outcome nobody approved. Mimic binds each agent's declared intent to its approved scope before any change executes, evaluates each action against that intent and the known-good baseline in real time, then assesses system state for drift.

Virtual Patching

Enterprise patch cycles run 30 to 45 days. Frontier AI discovery has compressed the interval from disclosure to working exploit to hours, so the entire patch cycle is now the exposure window. Mimic deploys a kernel-enforced mitigation to affected hosts within hours of a CVE disclosure, before the vendor patch exists and without a maintenance window. For high-profile CVEs, Mimic publishes vetted mitigations to a curated catalog, so teams get a deployable fix without authoring a rule. Before enforcement, Mimic replays each candidate rule against a host's recorded behavior and shows what it would block on that system, so teams commit with a known blast radius and roll back in seconds. End-of-life platforms with no patch path get the same enforcement as systems under active maintenance.

Change Control

Every change to the production environment is evaluated against the known-good baseline in real time. Authorized changes proceed. Unauthorized changes are blocked and logged with the context of what was attempted, by which account, against which system. ITSM integration routes those events into existing ServiceNow workflows, so change control operates inside the process teams already run. Enforcement continues through maintenance windows, the period when most change control frameworks relax and unauthorized change is hardest to distinguish from authorized work.

THE STRATEGIC OUTCOME

Across all three, the position is the same. Mimic governs change at the layer where ransomware, AI agents, frontier AI exploits, and configuration drift all eventually have to act: the kernel, where change either happens or it doesn't.

We'd welcome the chance to walk through how Mimic operates in environments like yours, where it fits alongside your current stack, and the questions your team would want answered before moving forward.

BOOK A DEMO AT MIMIC.COM