ArmorxAI

PRE-DEPLOYMENT VISIBILITY PLATFORM

RansomObserver™

See Before You Enforce. Deploy RansomObserver with Confidence.

RansomObserver is the passive evaluation companion to RansomArmor. Deploy it across your Windows fleet for ~2 weeks — no blocking, no disruption, no user awareness — while ObserverDirector streams every would-be threat event in real time. Then export a verified allow list and activate RansomArmor on Day One with zero surprises.

AWS SAAS CLOUD · PASSIVE MODE ONLY · WINDOWS AGENT · NO COST · NO OBLIGATION TO BUY

KERNEL-LEVEL VISIBILITY · ZERO DISRUPTION

The RansomObserver Agent is a silent Windows endpoint service running the identical AI detection engine as RansomArmor — same kernel driver, same behavioral heuristics, same AI/ML pipeline — without blocking or quarantine of binaries. It generates the real-world threat visibility your team needs before RansomArmor goes live.

"The security equivalent of placing an audit-only camera inside the vault — watching everyone without slowing down daily business operations."

THE CHALLENGE

THE BLIND SPOT EVERY CISO DREADS — AND WHY RANSOMOBSERVER EXISTS

Your team is considering RansomArmor — the kernel-level AI that stops ransomware and cyberattacks; but there's a hard question: **Which potential vulnerabilities and offensive binaries exist that your current security tool missed?**

Medical imaging software. CAD tools. Legacy ERP systems. Custom scripting engines that exhibit supicious or malicious behavior identical to ransomware. Nobody knows — until enforcement is live and users start calling.

There could be suspicious or malicious binaries/processes that your existing tools may not be flagging. These could be LOLBins, sideloaded DLL injections or non-sanctioned corporate software. That's the problem RansomObserver was built to eliminate.

SUPPORTED PLATFORMS

Windows 10 & 11 · Windows Server '19 - '25

RANSOMOBSERVER PERFORMANCE

~2wk	**0**
Evaluation Period Average fleet runtime required	**Process Blocks** Enforced at architecture level
<30 mins	**100%**
Deployment speed Applied to hundreds of devices under 30 mins	**Detection Parity** With RansomArmor engine

WITHOUT RANSOMOBSERVER

- × Blind to false positives on Day One
- × Reactive exceptions made under intense pressure
- × Security posture could compromise by rapid workarounds
- × No visibility into existing suspicious or malicious binaries
- × Executive confidence eroded by unexpected downtime

WITH RANSOMOBSERVER

- ✓ Full visibility into would-be suspisious & malicious blocks
- ✓ Pre-built, verified allow list before going live
- ✓ Day One enforcement is completely clean and quiet
- ✓ Zero rollback risk — everything already pre-validated
- ✓ Executive security confidence fully intact

Ready to validate your enterprise security posture?
Deploy passive validation in less than 5 minutes.

Test Drive Demo Portal →

ObserverDirector & Agent Capacities

Enterprise-grade passive endpoint instrumentation for risk-free ransomware enforcement planning.

Live Event Stream
Every would-be block streamed from agent to ObserverDirector in <1 second. Live telemetry feed details file paths, SHA-256 hashes, and device identities.

100% RansomArmor Detection Parity
Runs identical kernel-level AI behavioral heuristics, threat models, and classification routines. Perfectly tests exactly what RA would intercept upon activation.

Ultra-Low Footprint (<3% CPU)
Optimized kernel driver operations designed to run continuously throughout the evaluation window with low system impact, validated against heavy production environments.

Enterprise-Ready Deployment
Standard Windows MSI framework. Directly distribute and manage fleet deployment via standard infrastructure like Intune, SCCM, GPO, or CLI flags.

Silent & Invisible to End Users
No tray icon, popups, or notifications of any kind. Silent deployment & decommissioning occurs entirely background-level with zero desktop friction.

Architectural Zero-Block Guarantee
Quarantine pathways are entirely absent from the kernel driver code. Accidental blocks are mathematically and architecturally impossible.

EVALUATION LIFECYCLE

RansomObserver Workflow

DEPLOY → OBSERVE → EXPORT → ACTIVATE

01

1. Deploy Agent
Deploy silently via GPO, MSI or Intune. Silent rollout.

02

2. Observe (2w)
Logs would-be blocks transparently with 0 user impacts.

03

3. Export Allow List
1-click schema matching .xlsx export directly generated.

04

4. Activate RA
Transition to enforcement with verified safe execution.

ARCHITECTURAL ZERO-BLOCK GUARANTEE: Quarantine mechanisms are absent. Accidental blocks are impossible.

TECHNICAL SPECIFICATIONS

Metric	Specification
CPU Overhead	< 3% sustained avg
Event Latency	< 1 sec (Agent → SaaS)
Enforcement	**Architecturally absent**
Export Schema	1-click deduplicated .xlsx

OBSERVERDIRECTOR PORTAL

- **Real-Time Live Feed:** Instant log of file paths, SHA-256 signatures, detection classes.
- **Mandatory Warnings:** Persistent, non-dismissible observer warning status banner.
- **Fleet Organization:** Group agents by site, domain, environment type.

INNOVATIVE · TRUSTED · RECOGNIZED

NSA CRADA
Co-operative Research & Development

NSF SBIR II
Phase II Federal Innovation Grant

SIEM-Ready
Splunk

AWS
Cloud Marketplace Partner

About ArmorxAI

ArmorxAI delivers kernel-level security architecture utilizing Windows kernel instrumentation and eBPF technology. The RansomObserver agent enables risk-free deployment preparations without active blocking, backed by NSA research support and certified Microsoft driver execution pipelines.

armorx.ai
info@armorx.ai