ArmorxAI

RANSOMARMOR

Preemptive Ransomware Protection

Overview

Despite massive investments in security solutions, organizations remain vulnerable to ransomware. Ransomware has evolved from simple file encryption to sophisticated multi-stage attacks involving fileless payloads, script abuse, backup deletion, DLL injection and double extortion tactics.

Traditional endpoint security solutions often detect ransomware too late, after damage has already started. By the time they respond, files are encrypted, backups are gone, and attackers are demanding payment.

Preventive Ransomware Protection

RansomArmor is a **Patent Protected,** AI-powered platform, purpose-built to stop ransomware before it executes. Rather than relying solely on signatures or post-exploit telemetry, **RansomArmor** observes low-level signals, models attacker behavior, and prevents malicious actions in real time.

RansomArmor integrates seamlessly with your existing EDR solutions, applying preemptive methods and countermeasures to detect, identify and inoculate, ransomware-specific behaviors.

Key benefits

- Stops ransomware payloads before they start encrypting files.
- Adds a dedicated ransomware prevention layer to EDR/XDR.
- Lightweight agent with minimal system performance impact.
- Installs in minutes, no reboot required.
- Protects cloud, on-prem, or hybrid — no constant connectivity needed.
- Instantly kills suspicious processes and binaries, alerts central console.
- Integrates ransomware alerts and activities into existing SIEM.

Key capabilities

Core Ransomware Prevention

- **Pre-Execution Detection**
  Blocks malware before execution using AI and behavioral analysis.
- **Crypto Activity Monitoring**
  Monitors file access patterns and blocks unauthorized encryption attempts.
- **Fileless Ransomware Defense**
  Detects and stops script and memory-based ransomware methods.
- **DLL Sideloading Monitoring**
  Flags suspicious DLL loads that may indicate ransomware activity.

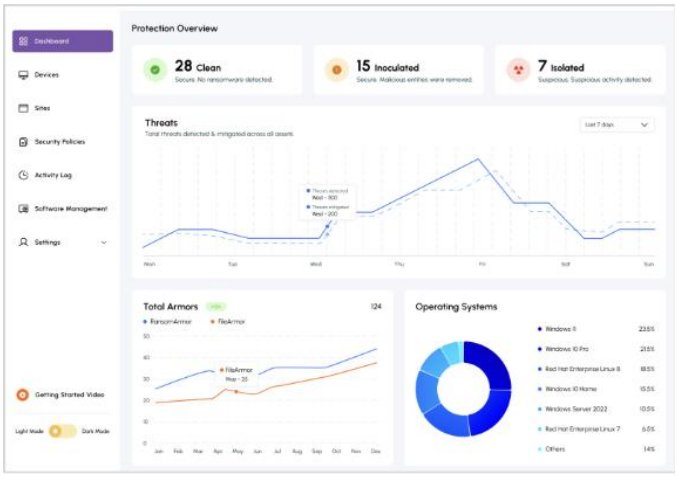
Advanced System-Level Protection

- **Kernel-Level Telemetry**
  Monitors critical OS functions for malicious process, file and registry operations.
- **Offline Protection**
  Maintains full prevention capabilities without relying on continuous cloud connectivity.

Usability & Deployment

- **Simplified User Experience**
  Protects your devices without user intervention.

Live Protection Dashboard



AI-Powered Ransomware Shield

- Stops ransomware **before it begins encrypting files** — even zero-days.
- Deploys in **minutes, no reboot, no slowdown** — protection that just works.

Why ArmorxAI?

RansomArmor isn't just another endpoint security product—it's purpose-built to do one thing exceptionally well: **prevent ransomware by providing preemptive protection.**

By narrowing the focus, **RansomArmor** provides:

- **Faster** detection and response than legacy solutions
- **Lower** system **impact** compared to bulky agents
- **Resilience** in offline and cloud-restricted environments

Support platforms

Windows 10 | Windows 11
Endpoints

Windows 2016 | Windows 2019 | Windows 2022
Servers

About ArmorxAI

ArmorxAI's vision is to stop ransomware and cyber threats before they disrupt businesses, with AI-powered protection that learns and evolves.

ArmorxAI (Kapalya Inc.) is a proud recipient of the National Science Foundation's SBIR Phase I & SBIR Phase II awards.

To learn more about how **RansomArmor** can preemptively defend ransomware threats before they impact your business: Contact us via: https://www.armorx.ai | info@armox.ai and schedule a demo or get a free trial.