ArmorxAI

DATA SHEET

RANSOMARMOR

Preemptive Ransomware Protection

Neutralize threats in real-time, minimizing downtime or disruption to business operations.

THE CHALLENGE

Enterprise security teams face increasing challenges in preventing ransomware attacks, which can lead to data breaches, operational disruptions, and financial losses. Existing security solutions often struggle to detect ransomware early, leaving organizations vulnerable.

ArmorxAI is a cutting-edge anti-ransomware solution that detects ransomware threats, inoculates or isolates affected devices, and protects organizations against data exfiltration. Unlike general-purpose cybersecurity platforms, ArmorxAI is laser-focused on **ransomware protection** to provide **real-time defense with AI-driven intelligence**.

RANSOMARMOR BENEFITS

- ✓ **Automated Containment & Kill-Switch**
  Instantly shuts down ransomware processes, even unknown or evasive ones.
- ✓ **Real-Time Monitoring & Response**
  Continuously watches Windows endpoints/servers and stops malicious actions like shadow copy deletion or privilege escalation.
- ✓ **Seamless Integration with Existing Security**
  Works alongside EDR/MDR/AV or standalone, aligned with MITRE & NIST frameworks.
- ✓ **Minimal Performance Impact**
  Runs as a sub-50MB nano-agent with low CPU/memory usage, ideal for cloud or air-gapped workloads.
- ✓ **Prevention-First, Not Alert Fatigue**
  Built for operational continuity with decisive prevention, not overwhelming alerts.

Supported systems

Windows 10 PCs

Windows 11 PCs

Windows Server 2019/2022 or higher

Support Clouds & Virtualization Environments

aws · Microsoft Hyper-v · openstack. · vmware

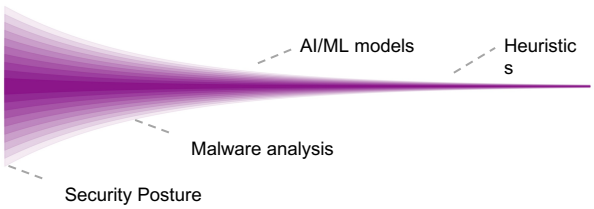
Minimum system requirements

Minimum storage at 50MB

Intel Xeon or i3 higher Minimum 1GB RAM

KEY FEATURES

- ✓ **Protection Before and During an Attack**
  Combines heuristics, behavioral, poly-rational and statistical analysis with AI-powered defenses to guard against known and zero-`day threats.
- ✓ **On device AI learning**
  Utilizes unique AI models for device and user behavior patterns.
- ✓ **Multiple Indicators of Compromise Methods**
  Security posture analysis with ML models for early detection and proactive remediation.
- ✓ **Detection & Inoculation in Milliseconds**
  Threats are detected and neutralized in real time, ensuring systems remain safe and continuously monitored.
- ✓ **Kernel-Level Integration for Real-Time Detection**
  Microsoft certified kernel driver monitors Operating System I/O functions and flags suspicious or malicious activity.



HOW IT WORKS

PRE-LAUNCH PREEMPTIVE MEASURES

- ✓ **Initial access and execution**
  (Beacon download via PowerShell, File-based and fileless thread hijacking.)
- ✓ **Post-exploitation activities**
  (Credential dumping, Self and remote DLL injection, DLL sideloading.)
- ✓ **Lateral movement**
  (SMB based payload deployment, Remote process injection.)

POST-LAUNCH PREVENTIVE MEASURES

- ✓ **Static ML model**
  (Blocks known and unknown ransomware payloads before execution).
- ✓ **Crypto detection engine**
  (Blocks unauthorized file encryption attempts in real-time.)
- ✓ **Heuristic engine**
  (Detects ransomware based on behavioral patterns.)

info@armorx.ai · /armorxai/ · armorx.ai