ArmorxAI

DATA SHEET

RANSOMARMOR

Prevent Ransomware breaches

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

The Ransomware 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 uses AI to detect and prevent ransomware threats in real-time. It isolates affected devices to prevent propagation and spread of cyberattacks 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

+ **AI-Powered Threat Detection**
  Identifies and neutralizes ransomware threats before they execute.
+ **Automated Containment & Inoculation**
  Prevents ransomware from spreading across your network.
+ **Real-Time Monitoring & Response**
  Provides continuous monitoring of known and zero-day exploits on Windows endpoints and Windows Servers.
+ **Seamless Integration with Existing Security**
  Complements existing solutions by adding another layer of protection.
+ **Minimal Performance Impact**
  Small footprint with minimal CPU/Memory usage, ensuring low performance impact on endpoints or servers.

Supported systems

Windows 10 PCs

Windows 11 PCs

Windows Server 2019/2022 or higher

Support Clouds and Virtualization Environments:

aws · Microsoft Hyper-v · openstack. · vmware

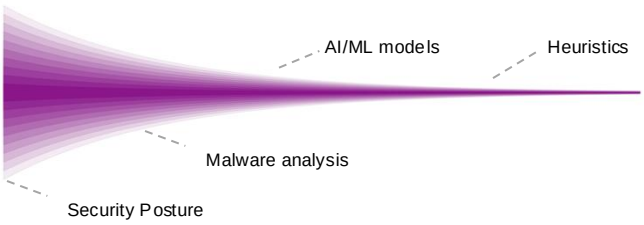
Minimum system requirements

Minimum 50MB storage

Intel Xeon, i3 processor or 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.
- **Kernel-Level Integration for Real-Time Detection**
  Microsoft certified kernel driver *constantly monitors I/O functions and flags suspicious or malicious activity.*
- **Detection & Inoculation in Milliseconds**
  Threats are detected and neutralized in real time, ensuring threats don't propagate to other systems.
- **Multiple Indicators of Compromise Methods**
  Security posture analysis with ML models for early detection and proactive remediation.
- **On device AI learning**
  Utilizes unique AI models for device and user behavior patterns.



HOW IT WORKS

- **Comprehensive Threat Assessment**
  Conducts Multi-layered security checks and advanced Ai/ML based behavioral analysis for detecting ransomware and malicious code injection threats.
- **Early Detection**
  Real-time detection and inoculation of suspicious activities
- **Proactive Protection**
  Actively neutralizes threats by isolating and quarantining malicious files and shutting down compromised systems, if a zero-day threat is detected.
- **Behavioral Analysis**
  Detects anomalies in user and system behavior, identifying potential risks.

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