



White Paper

STAYING AHEAD OF RANSOMWARE

*Minimizing Business Downtime & Data Loss
Through Intelligent Threat Containment*

Table of Contents

Executive Summary 3

Emerging Threats for Businesses 4

High Cost of Downtime and Cyber Claims 5

ArmorxAI: Complementing EDR with Real-Time Containment 6

Use Case: Preventing Ransomware Loss in Healthcare 7

EXECUTIVE SUMMARY

Incidents begin at the endpoints and servers.



Yet today's cyber threats are faster, more evasive, and increasingly business-disruptive—ransomware, data exfiltration, and identity compromise often unfold *in minutes*. Despite investing in traditional **Endpoint Detection and Response (EDR) platforms**, organizations still face real limits in speed, visibility, and operational efficiency.

The rising scale of attacks—more than **1,600** per organization *per week globally*—has turned EDR tools and SOCs into *overwhelmed systems, constantly chasing alerts and struggling to keep up*.

Most EDRs rely on *post-execution signals* or *predefined indicators*, leaving opportunities for attackers to encrypt data or pivot deeper into the network.

For many organizations, the result is a **slow, costly** game of catch-up.



Figure 01:
Layered Endpoint Defense with ArmorxAI and EDR

ArmorxAI addresses this imbalance;

It doesn't compete with your EDR—it complements them by providing an additional layer of security with a defense-in-depth methodology.

Powered by **AI-based behavioral models** at the kernel level, **ArmorxAI** detects and contains threats in real time, before damage is done. It acts as a proactive filter, not a reactive responder—stopping attacks at sub-second speeds, cutting down alert volume, giving your SOC time to react.

This paper **explores the shift in modern threat dynamics, the operational cost of response latency**, and how businesses can **reduce insurance claims, avoid downtime, and build resilience**—by rethinking what's possible at the endpoints and servers.

EMERGING THREATS FOR BUSINESSES

Cyber threats have evolved beyond perimeter-based intrusions.



Ransomware-as-a-service (RaaS)

Automate attacks



Double extortion

Encryption & Data exfiltration



Fileless malware

Hides in memory & evades signature detection

Industries commonly targeted by ransomware:

- Healthcare
- Manufacturing
- Insurance
- Financial services
- Education
- Federal/State/Local governments

Even companies with EDRs in place face gaps. These tools are often tuned for known indicators of compromise (IOCs) and require significant analyst oversight.

→ Alert fatigue, delayed triage, and blind spots from behavioral evasion all contribute to risk.

Small to mid-sized businesses (SMBs) are now primary targets

73%

Of ransomware attacks in 2024 targeted SMBs (IBM, 2024)

21 days

Average ransomware recovery time (Veeam, 2024)

Ransomware continues to succeed because most organizations focus on recovery after the damage is done. **Downtime stretches from days to weeks, costing revenue, trust, and operational continuity.**

Security teams often lack the speed and tools to contain threats in real time, forcing a **reactive cycle** of cleanup and restoration.

58% *of victims paid ransoms*

& the successfully recovered data is **65%**

*Verizon. (2024). Data Breach Investigations Report (DBIR).

*Veeam. (2024). 2024 Ransomware Trends Report.

*IBM. (2024). Cost of a Data Breach Report 2024. IBM Security.

HIGH COST OF DOWNTIME & CYBER CLAIMS

Cyber incidents cause more than data loss. They create cascading business challenges, each compounding the impact

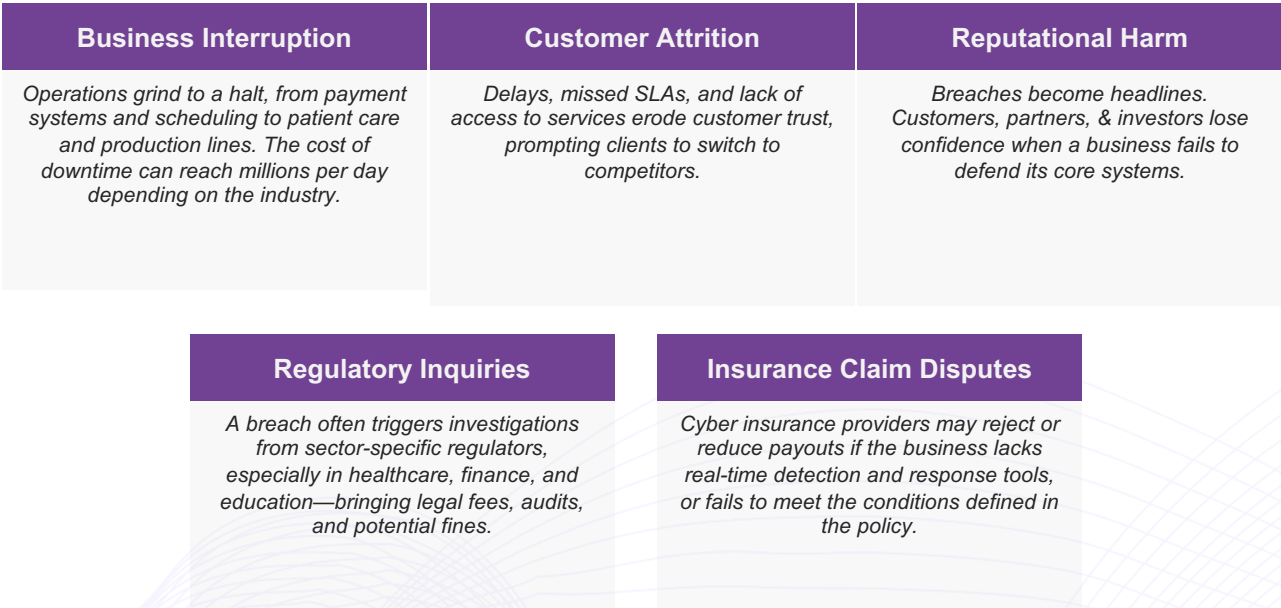


Figure 02: How Downtime Triggers Fallout

And for those that do survive, the aftermath is far from over. Beyond operational disruption, organizations face staggering financial losses that compound recovery efforts.

- Average ransomware recovery cost is **\$4.5M** per incident.
- **60%** of businesses that suffer critical IT downtime close within 6 months.
- Healthcare breach costs average **\$10.93M**—the highest among all sectors (IBM, 2024)

Cyber insurers are tightening eligibility and reducing payouts. Organizations without fast containment capabilities face higher premiums—or worse, denied claims. Real-time defense mechanisms reduce exposure windows and prove risk control maturity to insurers.

“When a factory stops, it’s not just production that halts—stakeholders absorb the ripple effects: wasted materials, missed deliveries, and damaged customer trust.”

(Interstates Crumrine & Post, ISA blog)

**IBM. (2024). Cost of a Data Breach Report 2024. IBM Security.
Crumrine, D., & Post, D. (n.d.). How much is plant or facility downtime costing you? International Society of Automation (ISA).*

ARMORXAI: COMPLEMENTING EDR WITH REAL-TIME CONTAINMENT

ArmorxAI is designed to work with, not replace, your existing EDR.

ArmorxAI leverages AI-driven behavioral analysis at the kernel level to detect and contain threats in real time—before they can cause harm. By intervening at the earliest stage of execution, it serves as a proactive control layer rather than a reactive stopgap.

Delivering sub-second response and significantly reducing alert noise, ArmorxAI empowers your security team to focus on strategic threats with the time and clarity they need to act decisively.

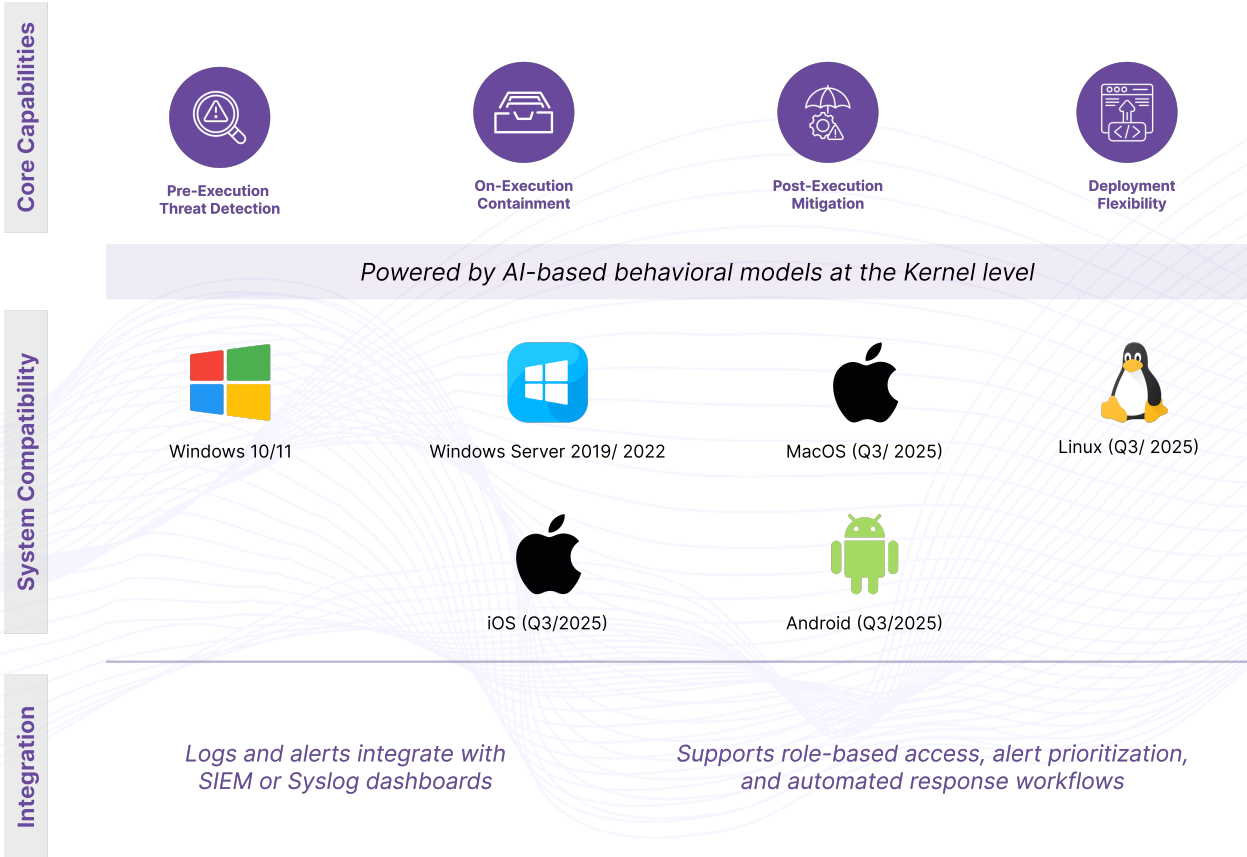


Figure 03: Core Features and System Coverage of ArmorxAI

ArmorxAI acts as a kill-chain interrupter—reducing reliance on human-in-the-loop response cycles. It lowers alert volume and shortens decision time, complementing EDRs without increasing complexity.

USE CASE: PREVENTING RANSOMWARE LOSS IN HEALTHCARE

Ensuring uninterrupted access to critical systems is not just a technical priority, but a core responsibility of care delivery leadership.

Snapshot: Ransomware Disruption at a U.S. Healthcare Provider

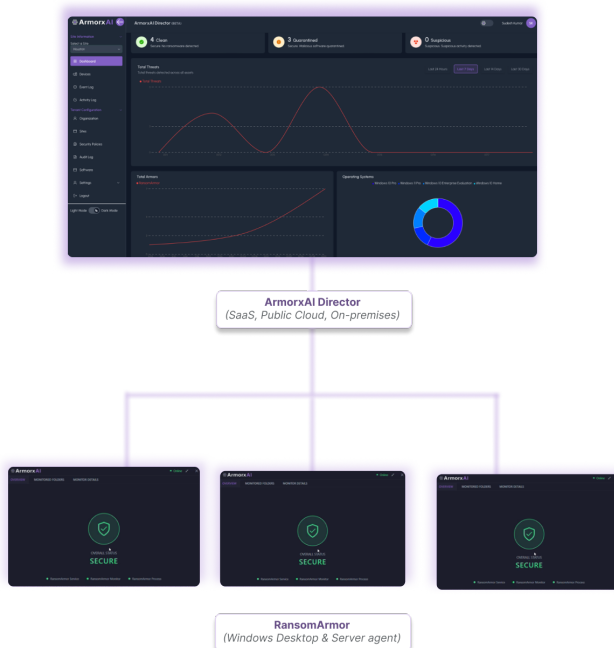
A major U.S. dialysis provider experienced a ransomware attack in April 2025, resulting in encrypted portions of its internal network. The attack was discovered over the weekend, prompting isolation of affected systems and a shift to manual processes to continue patient care. While critical services remained operational, some backend systems were disrupted, and full restoration timelines were not disclosed.

- The provider could not estimate the duration or full scope of downtime at the time of reporting.
- The company's stock dropped approximately **3%** following disclosure of the attack.

"A cyberattack on a hospital is not just a digital event—it's a patient safety event."
— John Riggi, American Hospital Association Senior Advisor for Cybersecurity

How Armorx AI can help

Figure 04: Containment-to-Recovery Pathway
Enabled by Armorx AI



This breach would have been neutralized in real time — **before** it affected business operations — with **Armorx AI**.

- ✓ **Flagged** the anomalous lateral movement **in real-time**.
- ✓ **Isolated** the affected hosts **within seconds**.
- ✓ **Prevented** file encryption from executing **at the kernel level**.

As a result, the organization could have mitigated the impacts with such outcomes:

- Reduced **downtime to <1 day**
- Avoided ransom payment
- **Maintained** patient data **confidentiality**.

*American Hospital Association. (2022, October 4). Cyberattacks on hospitals are patient safety issues, not just data breaches. AHA News.

*CT Insider. (2025, April 15). Ransomware cyberattack disrupts dialysis company with 28 clinics across Connecticut.



Prevent breaches before it strikes

SCHEDULE A DEMO →


ABOUT US

ArmorxAI is a cybersecurity company dedicated to preventing attacks before they strike. Our platform combines advanced AI-based behavioral analysis with real-time containment to protect businesses from modern ransomware and data exfiltration threats.

Designed to complement existing EDR and SOC tools, **ArmorxAI** serves as a critical added layer in a defense-in-depth strategy. By intercepting threats at the kernel level before they execute, ArmorxAI minimizes downtime, limits impact, and helps organizations maintain business continuity.

✉ info@armorx.ai

 [/armorxai/](https://www.linkedin.com/company/armorxai/)

 armorx.ai