ArmorxAI

White Paper

MANTENERSE A LA VANGUARDIA FRENTE AL RANSOMWARE

Minimizar el tiempo de inactividad y la pérdida de datos mediante la contención inteligente de amenazas.

Tabla de contenido

Resumen ejecutivo

Los incidentes comienzan en los **endpoints** y **servidores**.

Sin embargo, las ciberamenazas actuales son más rápidas, evasivas y disruptivas para el negocio: el ransomware, la exfiltración de datos y el compromiso de identidad a menudo se despliegan en cuestión de minutos.
A pesar de invertir en plataformas tradicionales de **Detección y Respuesta en el Endpoint (EDR)**, las organizaciones aún enfrentan límites reales en cuanto a velocidad, visibilidad y eficiencia operativa.

La creciente escala de los ataques —más de **1,600** por organización a la semana a nivel mundial— ha convertido a las herramientas EDR y a los SOC en ***sistemas saturados, que persiguen alertas constantemente y luchan por mantenerse al día.***

La mayoría de los EDR dependen de señales ***post-ejecución*** o de ***indicadores predefinidos***, lo que deja oportunidades para que los atacantes cifren datos o realicen movimientos laterales dentro de la red.

Para muchas organizaciones, el resultado es un juego de persecución **lento y costoso**.

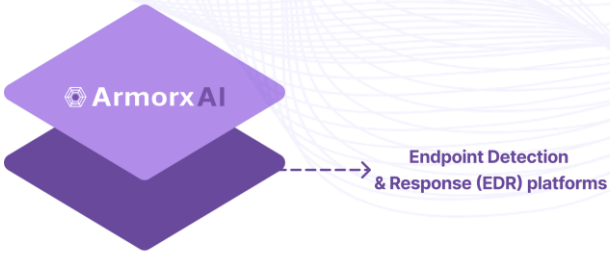

Figura 01:
Defensa de endpoints por capas con ArmorxAI y EDR

ArmorxAI soluciona este desequilibrio;

No compite con su EDR, sino que lo complementa al proporcionar una capa adicional de seguridad con una metodología de defensa en profundidad.

Impulsado por modelos de comportamiento ***basados en IA*** a nivel de kernel, **ArmorxAI** detecta y contiene las amenazas en tiempo real, antes de que se produzcan daños. Actúa como un filtro proactivo, no como un respondedor reactivo: detiene los ataques en milisegundos, reduce el volumen de alertas y le da a su SOC tiempo para reaccionar.

Este documento **explora el cambio en la dinámica de las amenazas modernas, el costo operativo de la latencia en la respuesta** y cómo las empresas pueden ***reducir las reclamaciones de seguros, evitar el tiempo de inactividad y desarrollar resiliencia***, mediante un replanteamiento de lo que es posible en los endpoints y servidores.

Amenazas emergentes en el entorno Empresarial

Las ciberamenazas han evolucionado más allá de las intrusiones basadas en el perímetro.

Ransomware-as-a-service (RaaS)
Ataques automatizados

Doble extorsión
Cifrado y exfiltración de datos

Malware sin archivos (Fileless malware)
Se oculta en la memoria y evade la detección basada en firmas

Industrias que suelen ser blanco del ransomware:

- *Sector salud*
- *Manufactura*
- *Seguros*
- *Servicios financieros*
- *Educación*
- *Gobiernos federales, estatales y locales*

Incluso las empresas que cuentan con sistemas EDR enfrentan brechas de seguridad. Estas herramientas suelen estar ajustadas para indicadores de compromiso (IOC) conocidos y requieren una supervisión significativa por parte de los analistas.

➔ La fatiga por alertas, el retraso en el triaje y los puntos ciegos derivados de la evasión de comportamiento contribuyen al riesgo.

Las pequeñas y medianas empresas (pymes) son ahora objetivos principales.

73%

De los ataques de ransomware en 2024, el 62% tuvo como objetivo a las pymes (IBM, 2024).

21 días

Tiempo promedio de recuperación tras un ransomware: 3.4 semanas (Veeam, 2024)

El ransomware sigue teniendo éxito porque la mayoría de las organizaciones se enfocan en la recuperación una vez que el daño ya está hecho. ***El tiempo de inactividad se extiende desde días hasta semanas, lo que afecta los ingresos, la confianza y la continuidad operativa.***

Los equipos de seguridad a menudo carecen de la velocidad y las herramientas necesarias para contener las amenazas en tiempo real, lo que los obliga a un ***ciclo reactivo*** de limpieza y restauración.

58% *de las víctimas pagó el rescate*

y el porcentaje de datos recuperados con éxito es del **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.*

EL ALTO COSTO DEL TIEMPO DE INACTIVIDAD Y LAS RECLAMACIONES DE CIBERSEGURO

Los incidentes cibernéticos causan más que una simple pérdida de datos. Generan una cascada de desafíos empresariales, donde cada uno de ellos agrava el impacto.

Interrupción de la actividad empresarial	Pérdida de clientes	Daño a la reputación
Las operaciones se paralizan por completo, desde los sistemas de pago y la programación hasta la atención al paciente y las líneas de producción. El costo del tiempo de inactividad puede alcanzar millones por día, dependiendo de la industria.	*Los retrasos, el incumplimiento de los acuerdos de nivel de servicio (SLA) y la falta de acceso a los servicios erosionan la confianza del cliente, lo que los impulsa a cambiarse a la competencia.*	*Las brechas de seguridad se convierten en titulares de prensa. Los clientes, socios e inversionistas pierden la confianza cuando una empresa no logra defender sus sistemas principales.*

Investigaciones regulatorias	Disputas por reclamaciones de seguros
Una brecha de seguridad suele desencadenar investigaciones por parte de los organismos reguladores de cada sector, especialmente en salud, finanzas y educación, lo que conlleva gastos legales, auditorías y posibles multas.	*Los proveedores de ciberseguros pueden rechazar o reducir las indemnizaciones si la empresa carece de herramientas de detección y respuesta en tiempo real, o si no cumple con las condiciones definidas en la póliza.*

Figura 02 Cómo el tiempo de inactividad desencadena el colapso

- Y para aquellas que logran sobrevivir, las secuelas están lejos de terminar. Más allá de la interrupción operativa, las organizaciones enfrentan pérdidas financieras asombrosas que dificultan aún más los esfuerzos de recuperación.
- El costo promedio de recuperación tras un ransomware es de **4.5 millones** de dólares por incidente.

Las aseguradoras de riesgos cibernéticos están endureciendo los requisitos de elegibilidad y reduciendo las indemnizaciones. Las organizaciones que carecen de capacidades de contención rápida enfrentan primas más altas o, lo que es peor, el rechazo de sus reclamaciones. Los mecanismos de defensa en tiempo real reducen las ventanas de exposición y demuestran a las aseguradoras la madurez en el control de riesgos.

"Cuando una fábrica se detiene, no solo se interrumpe la producción; los grupos de interés absorben los efectos dominó: materiales desperdiciados, entregas fallidas y una confianza del cliente dañada". *(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: COMPLEMENTANDO EL EDR CON CONTENCIÓN EN TIEMPO REAL

ArmorxAI está diseñado para trabajar en conjunto con su EDR actual, no para reemplazarlo.

ArmorxAI aprovecha el análisis de comportamiento impulsado por IA a nivel de kernel para detectar y contener amenazas en tiempo real, antes de que puedan causar daños. Al intervenir en la etapa más temprana de la ejecución, funciona como una capa de control proactiva en lugar de ser un parche reactivo.

Al ofrecer una respuesta en menos de un segundo y reducir significativamente el ruido de las alertas, **ArmorxAI** empodera a su equipo de seguridad para centrarse en amenazas estratégicas con el tiempo y la claridad necesarios para actuar con decisión.

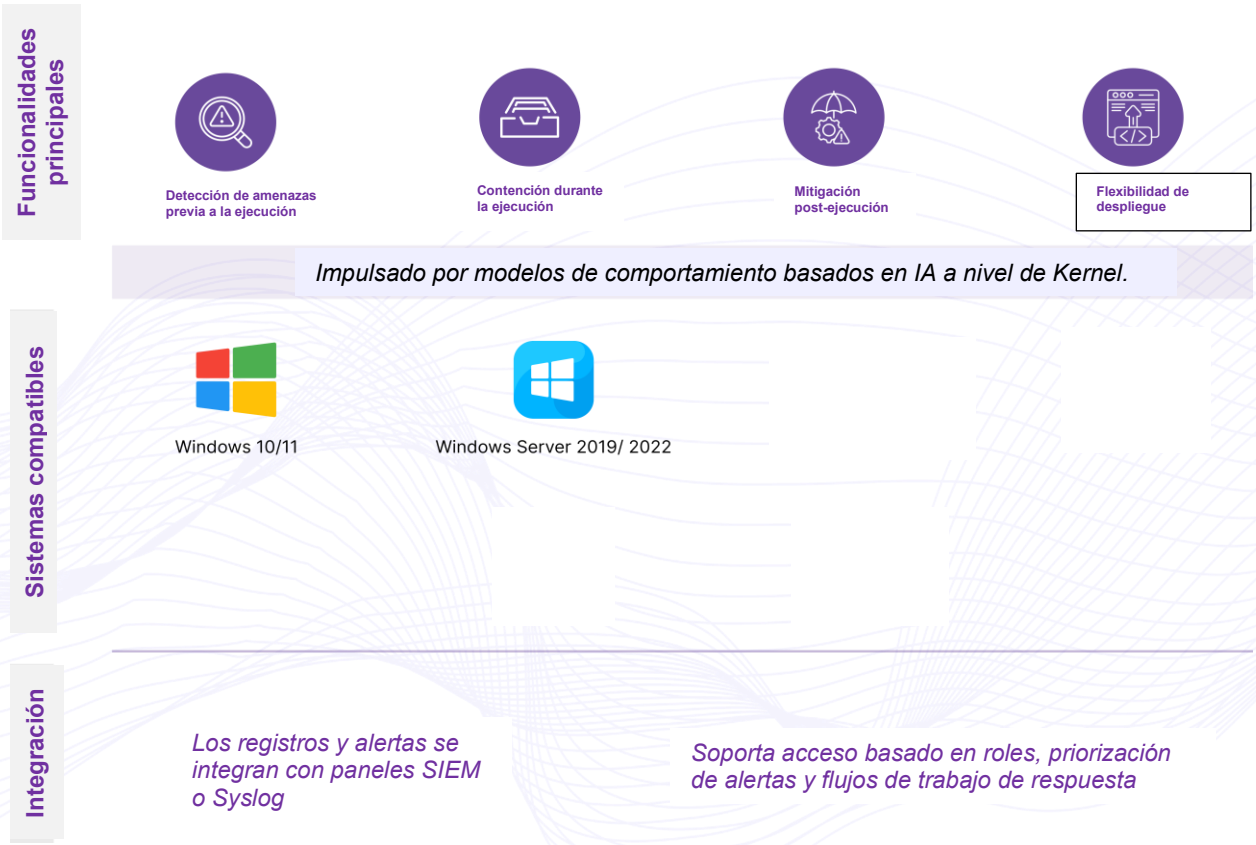

Figura 03: Características principales y cobertura del sistema de ArmorxAI

ArmorxAI actúa como un interruptor de la cadena de ataque (kill-chain), reduciendo la dependencia de los ciclos de respuesta basados en la intervención humana. Disminuye el volumen de alertas y acorta el tiempo de toma de decisiones, complementando a los EDR sin aumentar la complejidad.

CASO DE USO: PREVENCIÓN DE PÉRDIDAS POR RANSOMWARE EN EL SECTOR SALUD

Garantizar el acceso ininterrumpido a los sistemas críticos no es solo una prioridad técnica, sino una responsabilidad fundamental del liderazgo en la prestación de servicios de salud.

Resumen: Interrupción por ransomware en un proveedor de salud de EE. UU.

Un importante proveedor de servicios de diálisis en EE. UU. sufrió un ataque de ransomware en abril de 2025, lo que resultó en el cifrado de partes de su red interna. El ataque fue descubierto durante el fin de semana, lo que provocó el aislamiento de los sistemas afectados y el cambio a procesos manuales para continuar con la atención de los pacientes. Aunque los servicios críticos permanecieron operativos, algunos sistemas internos (backend) se vieron interrumpidos y no se revelaron los plazos para la restauración completa.

- Al momento de emitir el informe, el proveedor no pudo estimar la duración ni el alcance total del tiempo de inactividad.
- Las acciones de la empresa cayeron aproximadamente un 3% tras la divulgación del ataque.

"Un ciberataque a un hospital no es solo un evento digital; es un evento que afecta la seguridad del paciente."
— John Riggi, American Hospital Association Senior Advisor for Cybersecurity

Cómo ArmorxAI puede ayudar

Figura 04: Ruta de Contención a la Recuperación habilitada por ArmorxAI

Esta brecha de seguridad habría sido neutralizada en tiempo real —**antes** de que afectara las operaciones comerciales— con **ArmorxAI**.

- ✓ **Detectó** el movimiento lateral anómalo
- ✓ **En tiempo real.**
- ✓ **Aisló** los hosts afectados en cuestión de **segundos**.
- ✓ **Evitó** que el cifrado de archivos se ejecutara **a nivel de kernel**.

Como resultado, la organización podría haber mitigado los impactos con los siguientes resultados:

- Reducción **del tiempo de inactividad a <1 día**
- Se evitó el pago del rescate
- **Se mantuvo** la **confidencialidad** de los datos de los pacientes.

**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.*

ArmorxAI

Prevenga las brechas de seguridad antes de que ocurra el ataque

Acerca de Nosotros

ArmorxAI es una empresa de ciberseguridad dedicada a prevenir ataques antes de que ocurran. Nuestra plataforma combina análisis de comportamiento avanzado basado en IA con contención en tiempo real para proteger a las empresas contra el ransomware moderno y las amenazas de exfiltración de datos.

Diseñada para complementar las herramientas EDR y SOC existentes, **ArmorxAI** sirve como una capa adicional crítica en una estrategia de defensa en profundidad. Al interceptar las amenazas a nivel de kernel antes de que se ejecuten, **ArmorxAI** minimiza el tiempo de inactividad, limita el impacto y ayuda a las organizaciones a mantener la continuidad del negocio.

ventas@armorx.com.mx

armorx.com.mx