Informe técnico

Actualizar de EDR a XDR: saber cuándo avanzar

kaspersky preparados para el futuro

Actualizar de EDR a XDR: saber cuándo avanzar

Las organizaciones ya no necesitan ser muy conocidas para ser de alto riesgo. Esto refleja un punto de inflexión significativo en la ciberseguridad. Tradicionalmente, solo las grandes organizaciones se consideraban objetivos válidos para los ciberataques más avanzados, lo que justificaba la adopción de soluciones de seguridad robustas adaptadas a las grandes empresas. Sin embargo, en los últimos años se observa que las organizaciones medianas se han convertido en objetivos lucrativos y estratégicos para este tipo de ataques sofisticados.

Este cambio está obligando a muchos Chief Information Officers (CIOs) y especialistas en seguridad informática a replantearse sus estrategias de ciberseguridad. Además, muchas soluciones existentes, especialmente aquellas utilizadas por equipos de seguridad más pequeños o departamentos de TI más amplios, están demostrando ser inadecuadas para gestionar el creciente volumen y la complejidad de las amenazas modernas.

¿Por qué las empresas medianas se están convirtiendo en el principal objetivo de los ciberdelincuentes?

Las empresas con equipos de ciberseguridad más reducidos se convirtieron en los principales objetivos de los ciberataques más avanzados. Hemos descubierto que las pymes sufren una media de 16 ataques al año, mientras que las grandes organizaciones sufren hasta 18, dependiendo del sector.[1] Pero, ¿por qué el interés en las empresas más pequeñas que, a primera vista, no deberían necesitar protección de nivel empresarial?

Pasos hacia organizaciones más grandes

Muchas organizaciones más pequeñas sirven como vínculos críticos con las grandes empresas. Los ciberdelincuentes suelen considerar la red más grande y aprovechar el punto de entrada más fácil. De este modo, pueden interrumpir la cadena de suministro más amplia y causar daños en cadena. Solo en 2025, el 54 % de las grandes organizaciones citan las interdependencias de la cadena de suministro como el factor principal del aumento de la complejidad de la ciberseguridad.[2] Pero mientras que las organizaciones más grandes han registrado un aumento de la ciberresiliencia con respecto a 2024, las organizaciones más pequeñas siguen estando en desventaja, y un 35 % de ellas declara una ciberresiliencia insuficiente.[2]

Falta de personal cualificado

La mayoría de los equipos de ciberseguridad más pequeños desean mejorar sus capacidades de detección de amenazas y respuesta a incidentes, pero carecen de los recursos o el presupuesto para hacerlo. De hecho, estudios recientes muestran que el 41 % de los profesionales de la seguridad de la información afirman que los equipos de ciberseguridad de sus organizaciones carecen de forma "ligera" o "considerable" de personal suficiente.[3] En muchos casos, esto significa que las pymes dependen en gran medida del personal informático general para ocuparse de las tareas de ciberseguridad. Esto no sólo pone a los equipos más pequeños por encima de sus posibilidades, sino que también expone a las empresas a un aumento de las ciberamenazas debido a la falta de formación especializada. Por desgracia, los ciberdelincuentes son conscientes de esta vulnerabilidad y la explotan con facilidad.

Objetivos fáciles para herramientas sofisticadas

Las medianas empresas han demostrado ser objetivos fáciles, ya que muchas carecen de la ciberseguridad necesaria para protegerse adecuadamente de amenazas complejas. Sin embargo, cabe señalar que ser un "blanco fácil" no es únicamente un reflejo del equipo informático, sino también del hecho de que las amenazas sofisticadas son más fáciles de desplegar que nunca. Las pequeñas empresas suelen utilizar soluciones de seguridad informática más sencillas, como la seguridad de red, el EPP y el CWPP, todas ellas cada vez más ineficaces a medida que los ciberdelincuentes aprovechan herramientas sofisticadas para saltarse la ciberseguridad básica con facilidad.

Las pymes sufren una media de 16 ataques al año.[1]

Cómo las herramientas y los factores modernos facilitan la vida a los atacantes

Para comprender mejor el rápido aumento de los ataques complejos, debemos considerar la ciberdelincuencia como algo más que una amenaza técnica, más bien como una próspera empresa multinacional. Los ciberdelincuentes han desarrollado modelos de negocio escalables que les permiten agilizar las operaciones, diversificar sus fuentes de ingresos e innovar con rapidez y precisión. La aparición de multiplicadores de fuerza acelera el aumento de los ataques sofisticados, con herramientas avanzadas que equipan ahora incluso a ciberdelincuentes poco cualificados para lanzar esos ataques.

Los ciberdelincuentes evolucionan constantemente sus tácticas y aprovechan las nuevas tecnologías y las debilidades sistémicas para llevar a cabo ataques de manera más eficiente.

A continuación se enumeran las herramientas y factores clave que permiten a los atacantes explotar a las víctimas con mayor facilidad.

Ingeniería social

Los ataques de ingeniería social, como el phishing, utilizan técnicas de manipulación que explotan tu equipo para obtener información privada, y las tecnologías de IA han facilitado su despliegue más que nunca. Por ejemplo, un chatbot de IA orientado a la ciberdelincuencia puede ayudar a los atacantes a crear correos electrónicos pulidos y solicitudes de DocuSign fraudulentas. Con un esfuerzo mínimo, los atacantes pueden evitar las señales de alarma tradicionales del phishing, personalizar los correos electrónicos fraudulentos y utilizar tácticas de manipulación para crear una sensación de urgencia y autenticidad. Otros ataques de ingeniería social siguen un enfoque de varias etapas. El ataque comienza con el envío masivo de spam por correo electrónico que acaba obligando a los empleados a crear solicitudes legítimas al servicio de asistencia técnica. Los atacantes se hacen pasar por personal de asistencia de TI, contactan con los empleados a través de Microsoft Teams y les engañan para que reciban códigos QR maliciosos diseñados para entregar herramientas de monitorización remota que pueden ser explotadas para acceder a la red.

Spyware como servicio

Los desarrolladores de spyware también alquilan o venden el acceso a sus herramientas, a menudo a través de foros de la web oscura o canales con fines ilegales. Los clientes (normalmente hackers, estados-nación o acosadores) pagan por acceder a registradores de pulsaciones de teclas, herramientas de acceso a micrófonos/cámaras, kits de vigilancia móvil, herramientas de acceso remoto (RAT), herramientas de interceptación de navegadores y correo electrónico o rastreadores GPS.

Estas herramientas pueden utilizarse para recopilar y transmitir información de un dispositivo víctima sin el conocimiento o consentimiento del usuario.

Ransomware as a Service (RaaS)

Los kits RaaS son esencialmente herramientas “plug and play” que permiten a los ciberdelincuentes lanzar sofisticados ciberataques con poco trabajo práctico. Despliegan malware malicioso que puede adaptar tu código sin esfuerzo para evitar ser detectados por los sistemas de seguridad (como antivirus o cortafuegos). Por lo tanto, muchos marcos de ciberseguridad no proporcionan suficiente protección para luchar contra RaaS y dejan expuestos a situaciones de alto riesgo a empresas, gobiernos y particulares.[4]

Similares a los modelos de software como servicio (SaaS), los kits RaaS permiten a los afiliados acceder a herramientas de ransomware, asistencia técnica 24 horas al día, 7 días a la semana, portales de procesamiento de pagos y mucho más por tan solo 40 USD al mes. Y para tener una cierta perspectiva, la infracción media por ransomware cuesta a su víctima 4,91 millones de dólares (incluyendo tiempo de inactividad, pérdida de clientes, multas, etc.).[5]

Software obsoleto

A muchas empresas les cuesta estar al día de los parches y actualizaciones, lo que puede dejar vulnerable su software. Los grupos de ransomware, en particular, aprovechan las vulnerabilidades de día cero sabiendo que pueden superar la velocidad a la que las organizaciones aplican los parches. De hecho, el 85 % de las vulnerabilidades críticas no se han corregido a los 30 días de su descubrimiento, el 47 % siguen ahí a los 60 días y el 20 % siguen persistiendo al cabo de medio año.[6]

La necesidad de una protección avanzada

Procesos interrumpidos:

- Comunicaciones : 41 %
- Asistencia al cliente: 36 %
- Automatización del marketing — 34 %
- Logística — 32 %
- Desarrollo de productos/producción — 31 %
- CRM, ventas — 27 %
- Compras y pagos — 26 %
- Nóminas — 17 %

Las brechas de seguridad cuestan a las pymes 1,5 veces su gasto en ciberseguridad.[1]

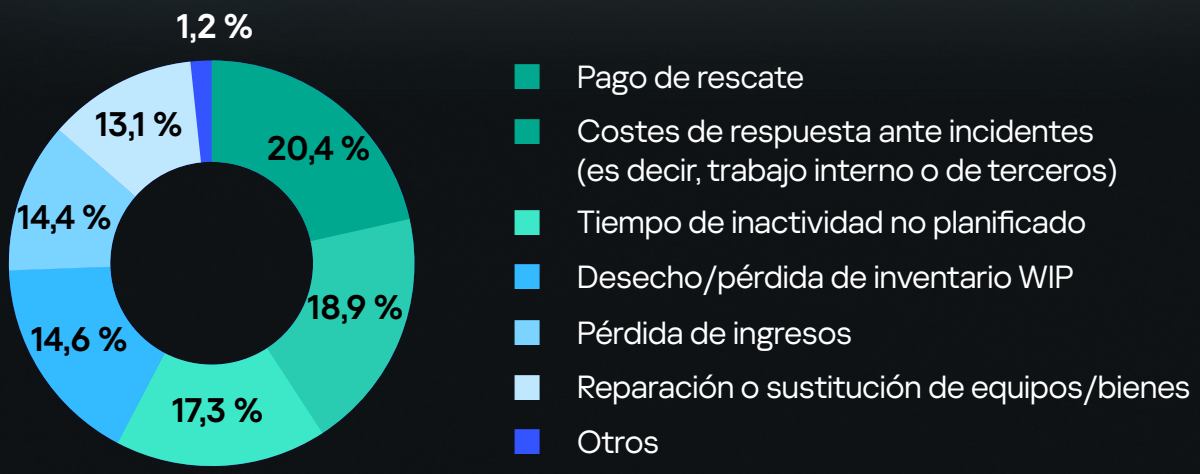
Junto con el aumento de la complejidad de los ciberataques, estudios recientes destacan que los costes derivados de la pérdida de negocio y de la respuesta posterior a la violación aumentaron casi un 11 % con respecto al año anterior.[6] Este aumento se debe en gran medida a que los ataques sofisticados provocan ciclos de vida de las brechas más largos.

Los ciberataques son ahora inevitables, pero la rapidez con que se detectan y se responde a ellos determina si un incidente se convierte en un acontecimiento menor o en una brecha catastrófica. Por ejemplo, en 2024, los tres tipos de brechas por vector inicial que más tardaron en contenerse fueron el phishing, los intrusos malintencionados y las credenciales robadas/comprometidas. Estos fueron también tres de los cuatro tipos de infracción más costosos por vector inicial, lo que pone de relieve la relación entre el tiempo de espera y los daños causados.[5]

Cuanto más tiempo actúen los atacantes sin ser detectados, más daño infligirán. Aquí es donde el tiempo medio de detección (MTTD) se convierte en un indicador clave del rendimiento en la gestión de incidentes, y pone de relieve la capacidad de tu equipo para detectar o descubrir un incidente. En consecuencia, tu tiempo medio de respuesta (MTTR) hace referencia al tiempo medio que se tarda en neutralizar la amenaza. La automatización de las operaciones de seguridad desempeña un papel importante en la mejora de estos parámetros. De hecho, quienes automatizan los procesos de seguridad informan de beneficios como una mejora del 46 % en su MTTR.[8]

La diferencia entre un incidente controlado y un desastre total suele reducirse a la rapidez de la respuesta. El MTTD no tiene sentido sin el MTTR: detectar rápidamente una amenaza no sirve si no se puede detener con la misma rapidez. El tiempo es dinero y cada segundo cuenta. Las organizaciones que responden rápidamente a las vulneraciones pueden ahorrar millones, cumplir fácilmente los requisitos normativos y proteger su reputación.

Coste medio de las infracciones de ciberseguridad en el sector de la alimentación y bebidas[9]



Cuando EDR ya no es suficiente

Durante muchos años, las herramientas de detección y respuesta para endpoints (EDR) han sido la base de cualquier estrategia de ciberseguridad, y con razón. EDR proporciona a los equipos de ciberseguridad valiosos datos y herramientas de visualización para determinar la causa raíz de la amenaza y si son necesarias medidas de respuesta adicionales, y supera con creces a las herramientas antivirus tradicionales tanto en capacidad como en eficacia.

Pero el panorama de las amenazas ha crecido significativamente, al igual que la importancia de la respuesta a incidentes y la investigación de amenazas, lo cual ha empujado a las organizaciones de alto riesgo hacia necesidades más complejas que solo las funcionalidades XDR pueden satisfacer.

Sin embargo, invertir en una solución XDR completa suele resultar inviable para las organizaciones más pequeñas que carecen de hardware, presupuesto o personal cualificado para manejar y analizar la telemetría con eficacia.

Esto deja a las pequeñas y medianas empresas en un delicado punto intermedio en el que las soluciones actuales ya no son suficientes, pero la XDR de nivel empresarial es demasiado avanzada, cara y poco práctica para resolver sus problemas actuales. Al mismo tiempo, la superficie de ataque se amplía y su equipo se ve desbordado por el gran número de alertas que hay que analizar.

Entonces, ¿cómo saber que ha llegado el momento de dar un paso adelante?

El cansancio por las alertas abruma a tu equipo

Si tu organización utiliza diversas herramientas de ciberseguridad que generan numerosas alertas, tu equipo de seguridad informática puede verse desbordado rápidamente. Esto es especialmente cierto si tu equipo carece del contexto suficiente para priorizar e investigar estas alertas con eficacia. El proceso puede ser tedioso, y tu equipo tendrá cada vez más probabilidades de pasar por alto una amenaza entrante si trabaja manualmente. Tu equipo puede incluso agotarse y buscar oportunidades en otra empresa.

> “Cuando un profesional de la ciberseguridad hace bien su trabajo, no pasa nada y su labor diaria es en gran medida rutinaria: comprobar registros y normas, revisar cuentas y garantizar el cumplimiento de las políticas. Estos no son pasos complejos, pero son críticos. Hacer estas tareas de forma manual conduce rápidamente al agotamiento”.
>
> Director de Plataforma Unificada de Kaspersky, Ilya Markelov

Aunque las plataformas EDR hacen un buen trabajo a la hora de detectar anomalías a nivel de endpoints, a menudo carecen del contexto más amplio necesario para comprender el alcance completo de un ataque. Como resultado, los analistas se ven obligados a realizar una labor detectivesca. Por lo tanto, es crucial encontrar una forma de clasificar las alertas de forma eficaz y obtener una visibilidad clara.

La superficie de ataque aumenta, pero tus recursos siguen siendo los mismos

El refuerzo del sistema es un componente crucial para ayudar a las pequeñas y medianas empresas a reducir la superficie de ataque. En esencia, el endurecimiento del sistema consiste en identificar y corregir los puntos débiles de la ciberseguridad para minimizar los posibles vectores de ataque y eliminar servicios o funciones innecesarios que los atacantes podrían explotar fácilmente.

Sin embargo, mantener los sistemas reforzados requiere una supervisión y aplicación de parches constantes para hacer frente a las nuevas vulnerabilidades, por no mencionar la carga que supone mantener el cumplimiento de las normativas de ciberseguridad, que cambian con rapidez. Huelga decir que el endurecimiento eficaz de los sistemas suele ser un reto para un equipo pequeño con recursos limitados.

Tus empleados se esfuerzan por resistir los intentos de phishing e ingeniería social

A pesar de invertir en EDR, es posible que tus empleados sigan siendo víctimas de ataques de phishing y de ingeniería social. Esto no es un fallo de EDR, sino una señal de que el panorama de las amenazas ha evolucionado. EDR es bueno para identificar malware conocido, supervisar el comportamiento del sistema y detectar anomalías, pero no está diseñado para evitar el error humano, que está implicado en el 22 % de las infracciones.[5]

Los ataques de phishing no necesitan explotar una vulnerabilidad en el software, sino en el comportamiento humano. Un correo electrónico bien elaborado o una página de inicio de sesión falsa pueden eludir incluso las plataformas EDR más robustas y conseguir que un empleado entregue sus credenciales o descargue archivos maliciosos.

Si tus empleados tienen dificultades para reconocer este tipo de ataques, es un claro indicador de que tu estrategia de ciberseguridad debe ir más allá de la EDR. Una defensa proactiva significa crear una cultura de la seguridad apoyada por una formación continua y herramientas que faciliten la protección de la identidad. Ir más allá de EDR significa abordar todo el espectro de riesgos, especialmente los que tienen su origen en la ingeniería social.

Los ataques se detectan demasiado tarde

Cuando los atacantes acceden a través de canales legítimos, tu EDR puede detectar la intrusión demasiado tarde, cuando ya se ha concedido el acceso. IBM descubrió que, en 2024, las organizaciones tardaron una media de 194 días en identificar una brecha, y otros 64 días en contenerla.[5] No se trata de un retraso menor. Son numerosos meses de potencial exfiltración, movimiento lateral y persistencia.

Cada día que pasa sin que se detecte un incidente aumenta el riesgo de que se roben datos confidenciales, se pongan en peligro los sistemas o se despliegue un ransomware.

La respuesta manual te ralentiza

Las empresas con planes de respuesta a incidentes sólidos y probados periódicamente obtienen un ahorro medio del 58 % en comparación con las que carecen de ellos.[10] Pero, ¿qué hace que un plan de respuesta a incidentes sea "sólido"? En resumen, todo depende de la velocidad. Los plazos de ataque modernos se acortan rápidamente; por ejemplo, el ransomware puede bloquear sistemas críticos en cuestión de minutos y, en el panorama actual de amenazas en rápida evolución, la respuesta manual a incidentes no puede seguir el ritmo.

A diferencia de los sistemas automatizados, la respuesta manual es más lenta a la hora de responder a incidentes de ciberseguridad e incluso el más mínimo retraso podría dar lugar a un mayor compromiso y riesgo.

No se puede sobrestimar la importancia de la automatización en la respuesta a incidentes. Al aprovechar la automatización, los equipos pueden identificar y contrarrestar las amenazas en tiempo real y reducir significativamente la ventana de exposición. Además, esto permite a tu equipo centrarse en otras tareas críticas que podrían requerir su experiencia, lo que le ahorra tiempo, dinero y recursos.

¿Ampliar o no ampliar?

Las soluciones XDR completas, aunque cruciales para la protección frente a las amenazas avanzadas, aún no han satisfecho las necesidades específicas de los equipos informáticos y de ciberseguridad más pequeños.

> Los mismos desafíos que hacen que las empresas medianas sean vulnerables a ciberataques complejos (presupuesto limitado, falta de recursos) son las mismas razones por las que les cuesta implementar una protección avanzada de manera eficaz.

Estas soluciones especializadas son notoriamente complejas de implantar y manejar, y a menudo requieren una curva de aprendizaje demasiado pronunciada para los equipos informáticos más pequeños. Pero la necesidad de al menos algunas funciones XDR es cada vez más importante, y no solo las empresas las necesitan. Nuestro Informe de Analistas de MDR afirma: "En 2024, el tiempo medio para investigar y notificar ciberincidentes aumentó en un 48 % en comparación con 2023, lo que refleja un aumento significativo de la complejidad de los ataques. Esto está respaldado por el análisis de reglas de detección activadas e IoA; la gran mayoría de los cuales provenía de herramientas de XDR especializadas. Esto marca un cambio con respecto a años anteriores, en los que la detección de los registros del SO tenía una función importante. En estas condiciones, las herramientas especializadas, como XDR, son fundamentales para la detección e investigación eficaces de amenazas modernas".[7]

Cómo puede ayudarle Kaspersky

Protección de nivel empresarial optimizada para equipos pequeños

Kaspersky NEXT XDR Optimum está diseñado para pequeños equipos de TI y ciberseguridad. La solución fortalece la respuesta ante incidentes y contribuye al conocimiento técnico sin sobrecargar al equipo con tareas rutinarias y prolongadas.

Dado que muchos procesos están automatizados, podrás poner tu atención en lo que más importa.

Activa una protección sobresaliente de endpoints

Aprovecha la protección automatizada para evitar la interrupción de la actividad empresarial. Con las herramientas antirransomware y antimalware basadas en ML y probadas en la industria puedes evitar sin esfuerzo las infecciones por amenazas conocidas y desconocidas.

Corrige vulnerabilidades mediante refuerzo del sistema y capacitación

Reduce tu superficie de ataque con el refuerzo del sistema basado en el comportamiento del usuario. Ahorra tiempo con la gestión centralizada de vulnerabilidades, parches y cifrado, y proporciona toda la formación que tu equipo necesita para sacar el máximo partido a tus nuevas capacidades de ciberseguridad.

Capacidades de detección y respuesta extendidas

Podrás recibir información detallada sobre las amenazas y sus movimientos en endpoints y más allá. Las herramientas de automatización y respuestas guiadas permiten responder ante ataques mientras que las herramientas esenciales de investigación pueden hacer un seguimiento de su actividad.

Forma a todo el equipo para que participe en la seguridad

Facilita a tu personal de IT y al personal no técnico las habilidades y el conocimiento necesarios para mantener la seguridad en la empresa. Fortalece a tu equipo de seguridad informática mientras desarrollas una cultura sólida y consciente de seguridad en toda tu fuerza laboral.

Controla la IT en la sombra gracias a una seguridad en la nube fiable

Controla el "shadow IT" para reducir tus vulnerabilidades y proteger tus datos y a tu personal. Detecta qué servicios en la nube se utilizan, bloquea el acceso no autorizado e identifica qué datos confidenciales se almacenan en las aplicaciones de Microsoft 365.

Minimiza la fatiga de las alertas

La función de agregación de alertas de Next XDR Optimum, combinada con el hecho de contar con una protección de endpoints eficaz y probada, reduce el número de alertas que los equipos deben analizar. Esto aumenta la eficacia y alivia la fatiga por alerta, y libera a tu equipo para que pueda centrarse en otras tareas críticas.

La XDR ya no es solo para grandes empresas

Descubre una solución de alto nivel optimizada para equipos más pequeños.

Kaspersky Next XDR Optimum

Más información

Bibliografía:

[1] Kaspersky, B2B IT security risk tracker report, (Kaspersky, 2024)
[2] Tuteja, Akhilesh, 5 risk factors from supply chain interdependencies in a complex cybersecurity landscape, (World Economic Forum, 2025)
[3] Kaspersky, A portrait of a modern Infosec professional, (Kaspersky, 2024)
[4] Willie, Alan, The Evolution of Ransomware-as-a-Service (RaaS): AI's Role in Cybercrime and Countermeasures, (Stanford University, 2025)
[5] IBM, Cost of a Data Breach Report 2024, (IBM, 2024)
[6] Verizon, 2024 Data Breach Investigations Report, (Verizon, 2024)
[7] Kaspersky, Fortress under fire: cyber threat chronicles 2024, (Kaspersky MDR Analyst Report, 2024)
[8] Verizon, 2024 Data Breach Investigations Report, (Verizon, 2024)
[9] Kaspersky and VDC Extended Survey Findings, (Securing OT environments, 2024)
[10] IBM, Cost of a Data Breach Report 2022, (IBM, 2022)

www.kaspersky.es

#kaspersky
#bringonthefuture