kaspersky bring on the future

Así se protege a las empresas de los ciberataques complejos

¿Alguna vez se quedó despierto por las noches preocupado por algún tipo de ciberamenaza avanzada que podría estar escondida dentro de su infraestructura esperando el momento adecuado para robar propiedad intelectual o mantener a su empresa o negocio cautivo para obtener un rescate?

Si es así, tiene un buen motivo. Como su nombre lo sugiere, las amenazas avanzas persistentes (APTs) utilizan técnicas de hackeo sofisticadas para acceder a sus sistemas. Una vez que vulneran sus defensas, pueden permanecer ocultas durante meses o incluso años, obteniendo privilegios de acceso de mayor nivel y recolectando y filtrando sus datos con resultados potencialmente devastadores.

¿Quién está en riesgo?

Como era de esperar, se requiere una cantidad considerable de capacidades, esfuerzo y recursos para montar un ataque de APT o un ataque selectivo, ya que sus principales objetivos suelen ser el sector gubernamental o grandes corporaciones con datos confidenciales o patentados, lo que justifica la inversión.

A pesar de esto, las APTs son un método de ataque que deben estar en el radar de las empresas de todo el mundo; incluso las de tamaño mediano están potencialmente en riesgo.

Los atacantes que usan APTs, por ejemplo, apuntan cada vez más a empresas más pequeñas que conforman las cadenas de suministro de sus objetivos finales. Debido a que dichas empresas por lo general cuentan con menos protección, actúan como trampolín para acceder a las organizaciones más grandes con las que trabajan.

Como resultado, ya sea que tenga una empresa grande o más pequeña que podría ser explotada potencialmente para atacar a una organización más grande, es importante **comprender la naturaleza de las amenazas** con las que podría enfrentarse. Esto incluye las APTs y otros ataques dirigidos, así como las capacidades necesarias para defenderse.

Todos los sectores atacados

Durante los últimos dos años, se observaron ataques selectivos llevados a cabo por humanos en todos los sectores. En 2024, el sector de TI y el sector gubernamental lideraron la categoría con 14.7 % y 13.8 % respectivamente.

Fuente: Kaspersky Managed Detection and Response 2024 Analyst report

US$ 4.880 millones

El costo promedio global de una filtración de datos en 2024, lo que marca un aumento del 10 % con respecto a 2023 y alcanza su máximo histórico. En la región del Medio Oriente, este indicador es considerablemente más alto, y alcanza los 8.75 millones de dólares.

Fuente: Cost of a Data Breach Report 2024 de IBM

258 días

El tiempo para identificar y contener una filtración. Este período de recuperación extendido no solo exacerba las pérdidas financieras, sino que también deja a las organizaciones en una posición vulnerable ante otros ataques.

Fuente: Cost of a Data Breach Report 2024 de IBM

¿Cómo funcionan las APTs?

La meta de una APT es obtener acceso persistente o continuo a los sistemas de TI o TO (tecnología operativa) del objetivo, lo cual los hackers por lo general logran a través de un proceso de cinco etapas.

Figura 1: Etapas de una APT en evolución

Etapa 1

Obtener acceso

Como un ladrón que abre una puerta por la fuerza con una palanca, los ciberdelincuentes a menudo ingresan por primera vez a través del uso de una "palanca digital", como un archivo infectado, correo electrónico de spam o phishing o la vulnerabilidad de una aplicación, para insertar malware en la red objetivo.

Etapa 2

Infiltrarse

Después de esto, implantan malware que les permita crear puertas traseras y túneles que pueden usar para moverse por los sistemas sin ser detectados.

Etapa 3

Profundizar el acceso

Una vez dentro de la red, los hackers utilizan técnicas como el quebrantamiento de contraseñas para acceder a los derechos de administrador, aumentar el control sobre el sistema y obtener mayores niveles de acceso.

Etapa 4

Moverse lateralmente

Más adentro del sistema, y con los mismos derechos que el administrador de la red, pueden moverse a su antojo. Esto les permite acceder a varios servidores y otras partes seguras de la red.

Etapa 5

Mirar, aprender y permanecer

Con un acceso más profundo en el sistema, los ciberdelincuentes pueden obtener un total conocimiento del funcionamiento del entorno y sus vulnerabilidades, lo que les permite recolectar la información que desean a su antojo. También pueden intentar mantener este proceso en ejecución, posiblemente por tiempo indeterminado, o irse una vez que hayan alcanzado sus metas.

¿Cuáles son las posibles consecuencias de convertirse en víctima de un ataque de APT?

Si lee la cobertura mediática de cualquier organización que haya sufrido un ataque selectivo, tendrá en claro que los efectos pueden ser graves y duraderos. Si bien los impactos inmediatos por lo general incluyen daños financieros provocados por la pérdida de datos y la interrupción comercial, los efectos a largo plazo pueden incluir daños en la reputación de la organización, la confianza del cliente y posibles acciones judiciales.

También tenemos el problema de reparar el daño en la infraestructura de TI de la organización, lo que a menudo lleva meses o incluso años. Y, según el sector en el que trabaja, también puede haber consecuencias específicas.

Figura 2: Comprender el impacto de las APTs en la seguridad del negocio

Finanzas

- Interrupción de servicios críticos
- Transacciones no autorizadas
- Ataques de retiro de dinero
- Consecuencias legales del robo de identidad

Entidades gubernamentales

- Posibles efectos del ciberespionaje
- Daños en infraestructura crítica
- Interrupción de servicios de gobierno electrónico
- Exposición de datos personales de ciudadanos

Comercio electrónico

- Consecuencias jurídicas de la apropiación de cuentas a través del robo de identidad
- Transacciones fraudulentas
- Denegación de servicios de TI, pérdidas de ganancias
- Posibles multas según RGPD, PCI DSS, etc.

Transporte

- Interrupción y cierres operativos
- Retrasos en la cadena de suministro y aumento de costos
- Amenaza a la vida
- Daños en infraestructura crítica

Industria alimentaria

- Escasez de existencias y paradas de producción
- Calidad de alimentos en riesgo
- Posible contaminación con químicos, toxinas, etc.
- Necesidad de recaer en operaciones manuales

Salud

- Interrupción de servicios críticos
- Exposición de datos personales de pacientes
- Menor confianza del público
- Amenaza potencial a la vida

TI y telecomunicaciones

- Pérdida de clientes
- Pérdida de ventas
- Tiempo de inactividad no planificado en la red
- Interrupción del servicio de comunicaciones fijas y móviles

Industrial

- Desastres ambientales
- Interrupción operativa
- Aumento de tiempo de inactividad no planificado
- Fallas en cascada o cortes en todo el sistema

Más de 2

incidentes de alta gravedad suceden todos los días.

43 %

de todos los incidentes de alta gravedad detectados por Kaspersky en 2024 son ataques selectivos llevados a cabo por humanos (APTs).

Fuente: Kaspersky Managed Detection and Response 2024 Analyst report

¿Qué significa esto para la ciberdefensa?

Uno de los mayores peligros de las APTs y otros ataques dirigidos es que, incluso cuando han sido descubiertos y la amenaza inmediata parece haber pasado, los atacantes pueden haber dejado múltiples puertas traseras que les permitan regresar cuando lo deseen.

Otro problema es que muchas soluciones tradicionales, como antivirus y firewalls, generalmente no pueden protegerlo frente a este tipo de ataques.

Del breve resumen de los pasos involucrados en el montaje de una APT o un ataque dirigido, debería quedar en evidencia que defenderse de estas amenazas requiere un enfoque de varios niveles en el que se incorporan soluciones capaces de proteger endpoints, redes, nube, correos electrónicos, acceso a Internet y mucho más.

Esto no solo ayudará a prevenir y reducir el riesgo de ataques sofisticados, sino que también ayudará a minimizar las interrupciones y los costos de estos tipos de incidentes si llevaran a ocurrir.

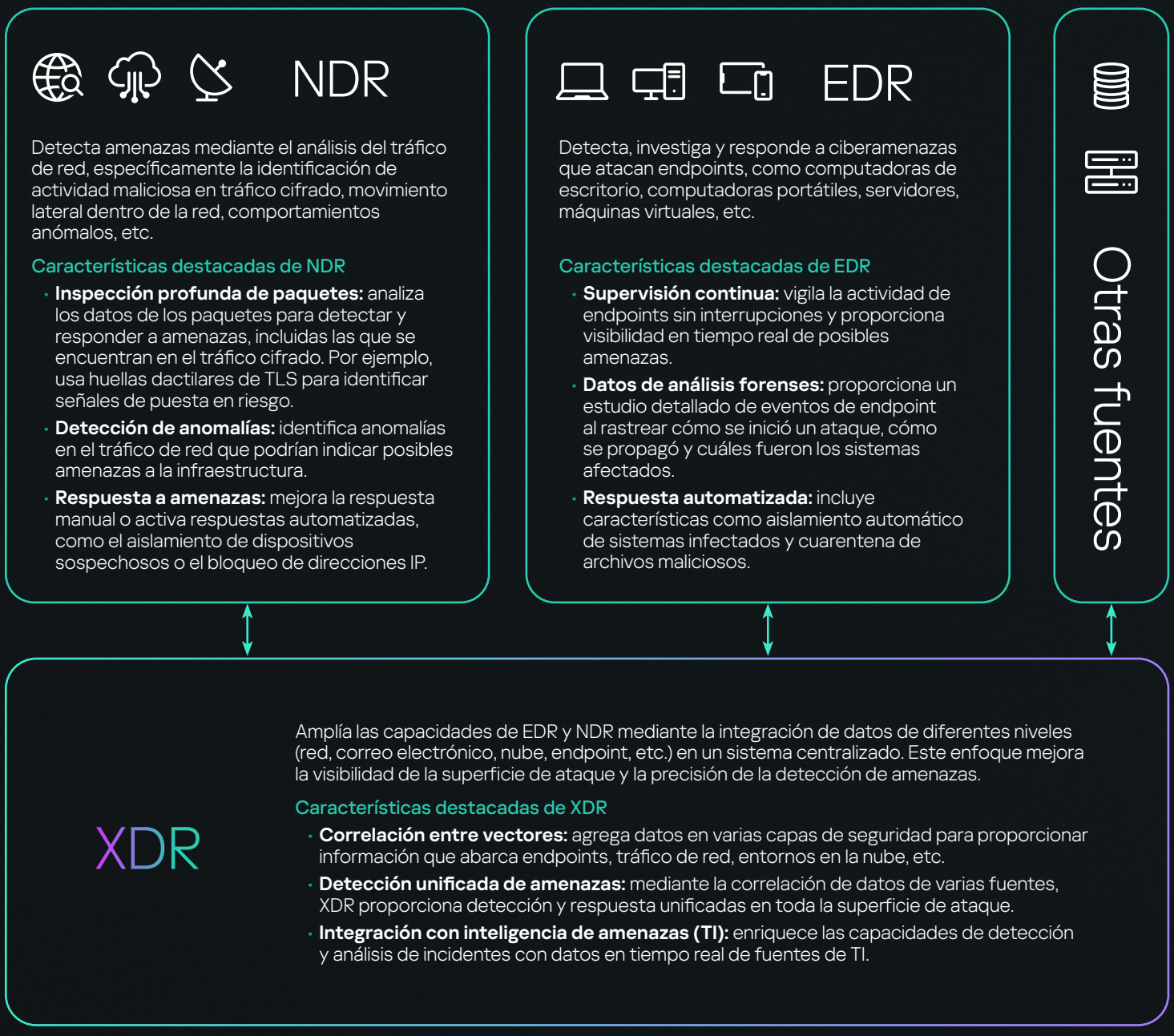
Entonces, ¿qué soluciones deben evaluarse e implementarse?

Así se protege a las empresas de los ciberataques complejos

Si bien una plataforma de protección de endpoints (EPP) por sí sola no lo protegerá de ataques selectivos, proporcionará una fuente vital de datos que se pueden usar en el análisis de ataques nuevos, actuales o históricos. Como resultado, debe utilizarse como parte de un conjunto de soluciones que también incluye lo siguiente:

- Detección y respuesta de endpoints (EDR): proporciona protección y visibilidad de endpoints en el dispositivo, identifica y responde a amenaza en estaciones de trabajo, servidores, etc.
- Detección y respuesta de redes (NDR): supervisa y analiza el tráfico de red, detecta anomalías y responde a amenazas potenciales en la red.
- Detección y respuesta extendidas (XDR): integra EDR, NDR y otras capas de seguridad para mejorar la visibilidad y automatizar la respuesta a las amenazas.

Figura 3: EDR, NDR, XDR: ¿Cómo funciona?



En 2024, el tiempo promedio para investigar y denunciar incidentes de alta gravedad aumentó un 48 %, lo que indica un aumento en la complejidad promedio de los ataques en comparación con 2023. Esto se ve respaldado por el hecho de que la gran mayoría de las reglas de detección activadas y los IOA se realizaron con herramientas de XDR especializadas, en lugar de registros del SO, como en años anteriores.

Fuente: Kaspersky Managed Detection and Response 2024 Analyst report

¿Qué soluciones debería elegir?

Seleccionar la solución correcta depende de las necesidades específicas de su organización, la infraestructura y el panorama de amenazas:

- Elija EDR si las herramientas de protección de endpoints tradicionales ya no alcanzan y necesita una protección más avanzada para enfrentar las ciberamenazas (como malware, ransomware, phishing y más) que atacan los endpoints.
- Elija NDR si las amenazas basadas en la red son lo que más le preocupa y necesita capacidades avanzadas para analizar y responder a las anomalías del tráfico de red.
- Elija XDR si desea una protección integral en los diferentes vectores y la capacidad de correlacionar amenazas en toda su infraestructura de TI.
- Mejor aún, combine EDR, NDR y XDR en un único ecosistema de seguridad para proporcionar una defensa integral frente a una amplia variedad de ciberamenazas evasivas y avanzadas.

Figura 4: EDR, NDR, XDR: ¿a quién va dirigido?

Solución de ciberseguridad	¿Para qué organización es más adecuado?
EDR	• Organizaciones que priorizan la protección de los endpoints y necesitan información en tiempo real sobre la actividad de los endpoints. • Organizaciones con muchos endpoints distribuidos, como instituciones financieras o prestadores de atención médica, que se beneficiarán considerablemente de la capacidad de EDR de detectar y responder a amenazas basadas en endpoints en tiempo real.
NDR	• Organizaciones que dependen mucho del tráfico de red y necesitan capacidades avanzadas para detectar las amenazas basadas en la red. • Empresas que tienen un equipo de seguridad de TI especializado o empresas con alto nivel de regulación, como centros de datos, prestadores de servicios o agencias gubernamentales, pueden beneficiarse de la capacidad de NDR de detectar y responder a amenazas basadas en la red.
XDR	• Organizaciones que requieren una plataforma de seguridad unificada con capacidades integrales de detección y respuesta de amenazas en toda su infraestructura de TI. • Organizaciones grandes con entornos de TI complejos que necesitan un enfoque integral de seguridad. Por ejemplo, una multinacional con centros de datos locales y entornos en la nube se beneficiaría de la capacidad de XDR de proporcionar detección de amenazas unificada en varias plataformas, al mismo tiempo que reduciría la complejidad operativa mediante la centralización de la respuesta a incidentes.

Kaspersky Anti Targeted Attack

¿Cómo Kaspersky puede ayudar?

Kaspersky Anti Targeted Attack (KATA) proporciona una protección integral anti-APT frente a ciberamenazas complejas. Ayuda a las organizaciones a:

- Detectar, analizar y responder con rapidez a los ataques selectivos.
- Proporcionar una seguridad sólida en todos los puntos de entrada de ataques clave, incluidos correos electrónicos, endpoints, sitios web y redes.
- Proteger a los activos más importantes.
- Garantizar el cumplimiento de normativas de la industria.

Todo esto es posible gracias a las tecnologías poderosas de NDR y EDR que están disponibles en los tres niveles de Kaspersky Anti Targeted Attack.

Los tres niveles de KATA ofrecen protección frente a amenazas avanzadas persistentes (APT), que va de NDR esencial y avanzado a XDR nativa.

- KATA: funciona como una solución de NDR esencial y ofrece características básicas para detectar y responder a ciberamenazas.
- KATA NDR Enhanced: basada en las características básicas del nivel KATA, ofrece funciones de NDR avanzadas.
- KATA Ultra: combina las capacidades de NDR y EDR para proporcionar una funcionalidad de XDR nativa. Protege varios puntos de entrada de amenazas, incluidos correos electrónicos, endpoints, sitios web, redes, servidores y máquinas virtuales.

Figura 5: Kaspersky Anti Targeted Attack. Una opción flexible.

Criterios de comparación	KATA	KATA NDR Enhanced	KATA Ultra
Descripción	NDR esencial	NDR avanzado	NDR+EDR (XDR Nativa)
Funcionalidades esenciales de NDR	•	•	•
Desarrollo de un sandbox avanzado	•	•	•
Enriquecimiento gracias a Kaspersky Threat Intelligence y MITRE ATT&CK	•	•	•
Funcionalidad NDR mejorada		•	•
Funcionalidad avanzada de EDR			•
Funciones nativas de XDR			•

Elija entre la funcionalidad de NDR básica o avanzada, u opte por la solución de NDR y EDR combinada para situaciones de XDR nativa, para protegerse frente a las ciberamenazas más sofisticadas, todo en una única plataforma. En el nivel KATA Ultra, obtiene una protección de APT completa y todo en uno, y visibilidad de toda su infraestructura de TI.

¿Por qué debería elegir Kaspersky Anti Targeted Attack?

Visibilidad completa en toda la infraestructura TI

Proporciona una pila completa de tecnologías únicas para eliminar puntos ciegos y controlar todos los puntos de entrada de amenazas potenciales (incluidos endpoints, sitios web, correos electrónicos y redes), todo dentro de una única plataforma unificada.

Protección enriquecida por inteligencia de amenazas global

Enriquece el análisis de amenazas y la respuesta mediante el acceso directo a la base de datos de reputación mundial de Kaspersky Private Security Network, Kaspersky Threat Intelligence y el mapeo al marco MITRE ATT&CK.

Tecnologías probadas y verificadas de forma independiente

Utiliza tecnologías innovadoras para la detección avanzada de amenazas con tecnología de aprendizaje automático, investigaciones exhaustivas y respuesta rápida a incidentes. Agencias analíticas líderes reconocen estas tecnologías y clientes importantes de todo el mundo confían en ellas.

Kaspersky Anti Targeted Attack

Conozca más

Presentación del video de Kaspersky Anti Targeted Attack

Ver ahora

Las predicciones de amenazas avanzadas

Leer ahora

www.kaspersky.es