

Megatendencias de ciberseguridad y sus consecuencias para la protección digital

Redefinir EPP,
EDR y XDR para hoy,
mañana y el futuro

kaspersky



Resumen ejecutivo

Todos los años, los principales analistas, comentaristas, asociaciones comerciales y más resaltan las "megatendencias" que prevén que moldearán su industria a corto plazo.

La ciberseguridad no es diferente. Esta información es vital para ayudar a los gerentes ejecutivos a anticiparse a las principales tendencias y planificar el futuro de sus organizaciones, pero cuando se trata de los directores de la información (CIO), los directores de seguridad de la información (CISO) y los equipos de TI y seguridad de TI, también es importante el modo en que sus consecuencias pueden adaptarse y ponerse en práctica.

Para ayudarte en este proceso, este libro electrónico resume algunas de las tendencias de seguridad más desafiantes que tienen un impacto en la industria de TI en la actualidad. Y, en particular, las consecuencias de estas tendencias para el uso que las organizaciones hacen de soluciones que van de plataformas de protección de endpoints (EPP) a detección y respuesta de endpoints (EDR) y detección y respuesta extendidas (XDR).



Índice

- Resumen ejecutivo
página 2
- Usted dice "megatendencia".
Yo digo "superficie de ataque expandida"
página 3
- ¿Qué sucede con las tendencias
más específicas a la TI?
página 4
- Cómo influyen las megatendencias más
recientes en el panorama de amenazas
página 6
- ¿Cómo pasamos de EPP a EDR y a XDR?
página 7
- ¿Qué tipo de seguridad necesita cada
empresa?
página 8
- Cómo evaluar sus requisitos de seguridad
en evolución: EPP, EDR y MDR
página 9
- Cómo evaluar los requisitos de seguridad
en evolución: XDR
página 15
- Capacidades y beneficios específicos
que debería esperar de una plataforma
de XDR
página 17
- Cómo justificar la inversión en XDR
página 21
- Abordar el panorama general de amenazas
página 23
- Cómo Kaspersky puede ayudar
página 25

Usted dice "megatendencia". Yo digo "superficie de ataque expandida"

Incluso para las personas que trabajan en la industria de TI, a veces puede ser difícil apreciar por completo la importancia vital de la ciberseguridad dentro de un contexto de mercado más amplio.

La [Security Industry Association](#) (SIA), por ejemplo, es la asociación comercial líder para proveedores de seguridad globales, con más de 1400 miembros. Cuando presentó la edición 2023 de su visión para la industria, la SIA afirmó que "no es para nada sorprendente ver a la ciberseguridad de la seguridad física nuevamente en la cima de nuestra lista de Megatendencias de seguridad de 2023".

"La IA y la ciberseguridad siguen compitiendo por ser las tendencias que más impacto tienen en la industria de la seguridad, pero los datos son contundentes: la ciberseguridad es lo primero que se le viene a la mente a los líderes de la industria de la seguridad". Y "la IA y la ciberseguridad están muchísimo más arriba que las tendencias subsiguientes".



Para ponerlo en contexto, los profesionales de la industria de la seguridad consideran que la ciberseguridad y la IA son mucho más importantes que las megatendencias que algunos piensan que dominan la industria, como el desarrollo de personal, el cambio de las condiciones económicas y el uso ético/seguro de los datos y la tecnología.



¿Qué sucede con las tendencias más específicas a la TI?

Si revisa informes similares de analistas líderes como Gartner, IDC y Frost & Sullivan, encontrará referencias a muchas tendencias: del dinamismo creciente de entornos de red que hacen que las vulnerabilidades sean más difíciles de defender, al volumen y la sofisticación cada vez mayores de los ciberataques que explotan estas vulnerabilidades.



En las Megatendencias de ciberseguridad 2022, por ejemplo, IDC destaca "7 tendencias en la realidad de la ciberseguridad", incluidas las siguientes:

- Transformación digital, trabajo híbrido y desaparición del perímetro
- Escasez de profesionales de seguridad de la información
- Sofisticación de ciberdelincuentes, que aumenta con rapidez
- Proliferación de conjuntos de herramientas de seguridad y plataformización
- Crecimiento continuo de normativas de cumplimiento
- Compradores nuevos y compradores antiguos con prioridades nuevas
- Confianza

Mientras tanto, las Principales tendencias en la ciberseguridad de 2023 de Gartner muestran mayor reconocimiento de la importancia de la participación de los empleados en el programa de seguridad para abordar riesgos de ciberseguridad y sostener una función de ciberseguridad efectiva. La naturaleza cada vez más distribuida de trabajo amplía la adopción de la nube. A su vez, esto aumenta la dependencia de la visibilidad integral de los ecosistemas digitales en expansión y las cadenas de suministro resilientes. Además, los CIO están cambiando sus modelos operativos de TI para fomentar la agilidad comercial mejorada. El entorno normativo sigue evolucionando, lo que obliga a las empresas a tener una función más activa en la administración de los riesgos de ciberseguridad. Si bien los pagos de ransomware están disminuyendo, los ataques de ransomware a gran escala y los ataques en los sistemas de identidad continúan.

Estas tendencias globales obligan a los líderes de seguridad y gestión de riesgos (SRM) a concentrar sus esfuerzos en lo siguiente:

1

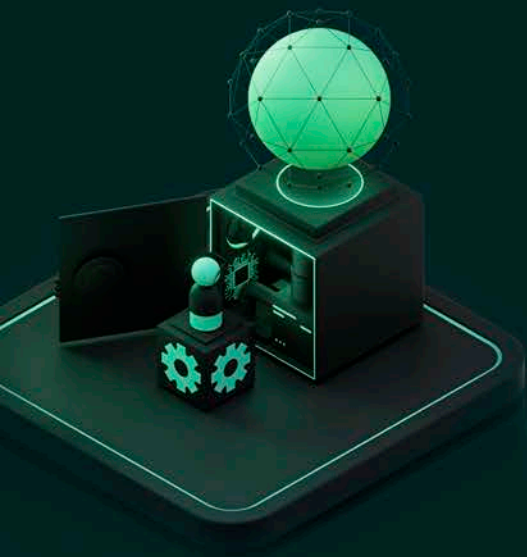
Aumentar el enfoque en la función esencial de las personas para el éxito y la perdurabilidad del programa de seguridad.

2

Implementar capacidades técnicas de seguridad que brindan mucha más visibilidad y capacidad de respuesta en todo el ecosistema digital de la organización.

3

Reestructurar la manera en que funciona la seguridad para facilitar la agilidad sin comprometer la seguridad.



Para abordar estas cuestiones, Gartner recomienda que los líderes de administración de seguridad y riesgos (SRM) hagan lo siguiente:

- Adoptar la mentalidad de un atacante para priorizar los esfuerzos de mitigación de ciberamenazas, al obtener una vista integral de la superficie de ataque y consolidar las carteras de los proveedores, según sea adecuado.
- Optimizar la alineación de las capacidades de ciberseguridad con las nuevas formas distribuidas de trabajo, al adoptar nuevos modelos operativos y enfoques arquitectónicos de seguridad que fomenten la agilidad e incorporen la seguridad en el diseño.
- Priorizar y optimizar las inversiones destinadas a mejorar el comportamiento de los empleados para potenciar y mantener la eficacia de la seguridad empresarial.

No hay duda de que todas estas recomendaciones son buenas. Entonces, ¿cómo puede incorporarlas a su organización?

Para responder, necesitamos comenzar por analizar en mayor detalle el panorama de amenazas en evolución y lo que significa en el contexto de su infraestructura de seguridad de TI, herramientas y controles existentes.

"Las vulnerabilidades de día cero no suelen ser la principal causa de una vulneración. En otras palabras, las organizaciones podrían prevenir las vulneraciones si corrigieran su exposición a una amenaza antes de que un atacante la aproveche. Sin embargo, corregir cada vulnerabilidad conocida siempre fue inviable desde el punto de vista operativo".

Gartner: Principales tendencias en la ciberseguridad de 2023

Cómo influyen las megatendencias más recientes en el panorama de amenazas

En comparación con algunos años atrás, el panorama de amenazas está evolucionando más rápido que antes. Por ejemplo, ahora es extraño que pase una semana sin recibir un informe sobre un ataque de ransomware, una estafa o una filtración de datos de alto perfil. Y no solo crece la cantidad de ciberataques, sino que estos también son cada vez más sofisticados, selectivos y difíciles de detectar.

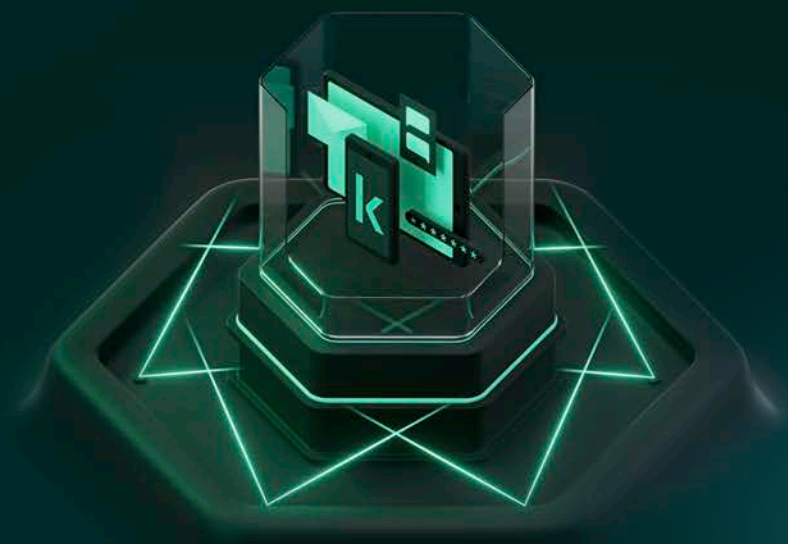
Muchas de las personas involucradas en el lanzamiento de ciberataques son delincuentes profesionales, y es esa experiencia lo que les garantiza el éxito. Asimismo, la falsa idea popular de que los hackers son guerreros solitarios detrás de un teclado ya no es válida.

Si tomamos el ransomware como ejemplo, los grupos involucrados se comportan cada vez más como corporaciones descentralizadas, con redes complejas de afiliados responsables de pasos individuales en el proceso: desde el reconocimiento, el acceso, la creación de malware, la distribución y la exfiltración de datos, hasta la negociación del rescate, la publicación de datos robados en línea y el lavado de pagos de rescate.

Hoy en día, la mayoría de los ataques de ransomware duran horas en lugar de días. Los grupos también ofrecen ransomware como servicio y realizan ataques que se asemejan más a las amenazas persistentes avanzadas (ATP) en cuanto a su alcance. Los ciberactivistas (hacktivists) y los Estados nación pueden usar ransomware y otras técnicas (como wipers) con fines destructivos o geopolíticos, en lugar de motivos completamente comerciales.

Además, las tácticas, las técnicas y los procedimientos (TTP) que los cibercriminales usan son cada vez más sofisticados. Por ejemplo: el uso de funcionalidades que se diseminan y propagan automáticamente; el uso de aplicaciones dirigidas al público, cuentas en riesgo y correos electrónicos maliciosos, y el uso de herramientas como PowerShell, que son muy utilizadas en operaciones de TI normales, lo que hace que estos ataques sean mucho más difíciles de detectar.

Como resultado, establecer el nivel óptimo de protección para su organización, ya sea con EPP, EDR o XDR, nunca ha sido tan importante.



¿Cómo pasamos de EPP a EDR y a XDR?



El 51 % de las empresas tiene dificultades para detectar e investigar amenazas avanzadas con las herramientas actuales.

Informe de ESG Research: la modernización del SOC y el rol de XDR, junio de 2022

Tradicionalmente, además de la defensa de sus perímetros con firewalls y protección de correo electrónico, las organizaciones concentraban sus esfuerzos en los endpoints (PC, computadoras portátiles, servidores tanto físicos como virtuales y estaciones de trabajo) como defensa principal contra las ciberamenazas, hasta el punto que las plataformas de protección de endpoints (EPP) se convirtieron en un paso fundamental al momento de combatir ataques complejos.

A esto, en los últimos tiempos, las organizaciones sumaron el despliegue de herramientas más avanzadas para defenderse de los ataques. Estas se pueden utilizar para identificar y responder a comportamientos anómalos en los endpoints, a través de la detección y respuesta en endpoints (EDR), o en la red, a través de la detección y respuesta en la red (NDR).

Pero, como vimos, los ciberdelincuentes perfeccionan sus tácticas todo el tiempo y desarrollan maneras más sofisticadas de atacar a las empresas. En la actualidad, cada vez más atacantes optan por un enfoque multivectorial para llevar a cabo sus ataques y, por lo general, involucran varios puntos de entrada a la infraestructura, y una variedad de tácticas y técnicas diferentes.

Los actores maliciosos utilizan técnicas avanzadas, como ingeniería social (incluidos el phishing y la vulneración de correos electrónicos empresariales), cuentas en riesgo, aplicaciones dirigidas al público y exploits de día cero para vulnerar las defensas de las empresas, lo que hace que protegerlas de estas amenazas en evolución sea un verdadero desafío.

Por ejemplo, las amenazas persistentes avanzadas (APT) eluden la detección tradicional de endpoints, y pueden mantenerse activas durante semanas o meses: mientras se mueven de manera lateral a través de la red, obtienen permisos, exfiltran datos y recopilan información de las diferentes capas de la infraestructura de TI como preparación para un ataque o una filtración de datos a gran escala.

El gran volumen de estos ataques, y su complejidad, hace que les sea difícil a las organizaciones mantenerse un paso por delante. Al mismo tiempo, una superficie de ataque en constante expansión (incluidos dispositivos móviles, entornos en la nube y trabajo remoto, servidores, etc.) agrava aún más la situación.

Además de todo esto, las organizaciones deben enfrentarse a amenazas internas, vulnerabilidades de la cadena de suministro, requisitos normativos y de cumplimiento, y al mismo tiempo abordar la escasez actual de profesionales de ciberseguridad calificados. El daño potencial a los sistemas corporativos, las operaciones y las reputaciones proveniente de filtraciones de datos, ransomware, ataques de denegación de servicio distribuida (DDoS), APT, ciberespionaje, etc. puede ser enorme.

Por lo tanto, establecer una protección efectiva contra estas amenazas requiere un enfoque integral y proactivo, que combine tecnologías avanzadas, directivas sólidas, supervisión constante, capacitación continua y más, que es exactamente la visión de 360° del panorama de amenazas que XDR se propone proporcionar.

Al descomponer los silos entre las soluciones de punto específicas a cada capa, la XDR les da a los centros de operaciones de seguridad (SOC) y los equipos de seguridad de TI la visibilidad de extremo a extremo y la integración que necesitan para identificar amenazas con mayor agilidad, responder a ellas más rápido, corregirlas más efectivamente y minimizar el daño que puedan causar.

¿Qué tipo de seguridad necesita cada empresa?

La solución ideal es una que complemente la protección de endpoints con una seguridad de clase EDR que aligere significativamente la carga de trabajo de EDR, ya que, mientras más amenazas se prevengan, menor será el volumen de trabajo de investigación para los equipos de seguridad.

Durante muchos años, las pequeñas y medianas empresas (pymes) y organizaciones de nivel inferior lograron depender de las EPP para defenderse de una amplia gama de amenazas básicas. Sin embargo, como analizamos brevemente, los atacantes de la actualidad se enfocan en organizaciones de todos los tamaños, industrias y niveles de preparación, y las pymes y empresas más pequeñas corren cada vez más riesgo de recibir amenazas evasivas más avanzadas, que antes solo se dirigían a organizaciones mucho más grandes.

Como respuesta, los equipos de seguridad de TI complementan las EPP con EDR o servicios de detección y respuesta gestionados (MDR), lo que les permite detectar e investigar incidentes de seguridad, contener la amenaza en el endpoint y recibir una respuesta automatizada o una guía para solucionar el problema.

La solución ideal es una que complemente la protección de endpoints con una seguridad de clase EDR que aligere significativamente la carga de trabajo de EDR, ya que, mientras más amenazas se prevengan, menor será el volumen de trabajo de investigación para los equipos de seguridad. Esto, a su vez, permite que los equipos de TI puedan optimizar los recursos clave y centrarse en el trabajo de la TI, en lugar de perseguir falsos positivos y enormes volúmenes de alertas.

Si subimos de nivel desde EDR y MDR, la palabra "extendidas" en detección y respuesta extendidas refleja el hecho de que, en la XDR, una solución de EDR se complementa y se integra estrechamente con otras herramientas de seguridad diferentes, que pueden no estar diseñadas específicamente para trabajar en conjunto. En lugar de utilizar varias herramientas de seguridad como soluciones puntuales aisladas, la XDR permite que las organizaciones creen un ecosistema de seguridad integral, flexible y escalable, que maximice los beneficios de las herramientas existentes, se pueda personalizar según las necesidades propias, reduzca los riesgos y brinde mayor seguridad.

De modo que, para responder la pregunta "¿Quién necesita qué tipo de seguridad?", se deben tener en cuenta las siguientes consideraciones clave:

- Todas las organizaciones necesitan una base sólida de seguridad de endpoints moderna.
- Los niveles adicionales de seguridad que se requieren además de este dependerán en gran parte de una combinación de los tipos de ciberataques a los que se encuentra expuesta la organización y las capacidades de seguridad de TI del equipo de TI que deberá implementar y usar las herramientas requeridas para prevenirlos.

Ahora, analizaremos cinco pasos clave que le ayudarán a evaluar y poner en práctica los requisitos de seguridad en relación con estas consideraciones.



Cómo evaluar sus requisitos de seguridad en evolución: EPP, EDR y MDR

Paso 1:

Revise la protección de endpoints existente

Con tantas soluciones avanzadas de ciberseguridad disponibles en el mercado, es fácil olvidar la función fundamental que cumple la protección de endpoints. ¿Por qué son tan importantes los endpoints? No solo son los puntos de entrada más comunes en la infraestructura de una empresa — y el objetivo principal de los ciberdelincuentes—, también son las fuentes clave de los datos necesarios para una investigación eficaz de incidentes complejos.

Como resultado, cada organización debe elegir una solución de EPP que proporcione una protección automatizada contra el gran número de posibles incidentes causados por las amenazas básicas, incluidas las amenazas sin archivos y el ransomware.

Debido a que este tipo de configuración requiere personal o conocimientos de seguridad especializados relativamente limitados, satisface las necesidades de seguridad de endpoints de pymes o empresas más pequeñas sin un equipo de seguridad especializado, o de organizaciones con muy bajos niveles de experiencia en ciberseguridad.

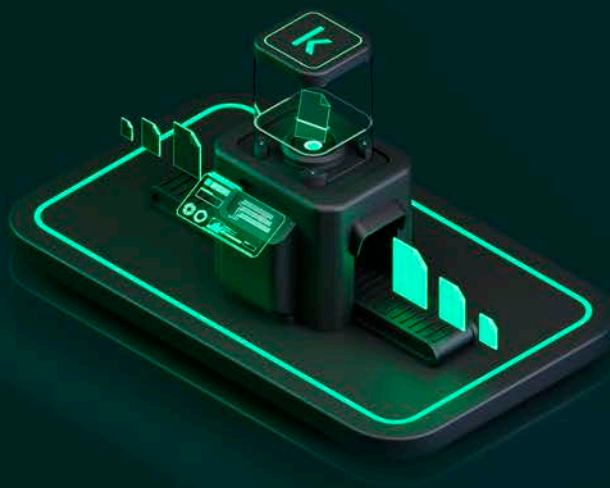
También es una etapa fundamental para empresas medianas y grandes donde, al abordar automáticamente una gran cantidad de amenazas menores, la solución despeja el camino para que los equipos de seguridad se centren en una defensa más avanzada cuando sea necesario.



Elementos clave a tener en cuenta

Al momento de examinar la EPP para evaluar si está proporcionando las capacidades que necesita o espera, tenga en cuenta lo siguiente:

- ¿Qué tan eficaz es?
- ¿Cuántos falsos positivos recibe?
- ¿Ofrece capacidades eficaces de reducción de la superficie de ataque como antivirus para archivos, web y correo, protección de red, interfaz de análisis antimalware (AMSI), prevención de exploits, corrección, detección de comportamientos y prevención de intrusiones basado en host (HIPS)?
- ¿Ayuda a automatizar las tareas rutinarias?
- ¿Es fácil de operar y permite minimizar los costos y los gastos generales del equipo de TI?
- ¿Ayuda con las tareas críticas como la evaluación de vulnerabilidades, el inventario de software/hardware, los controles de inventario, firewall, Web y dispositivos y Cloud Discovery?



Paso 2:

Identifique cualquier brecha crítica en las defensas de endpoints

Por qué la EPP moderna requiere capacidades de EDR

Como ya mencionamos en este libro electrónico, la evolución del entorno de amenazas significa que, con el tiempo, las amenazas cada vez más sofisticadas y que antes solo afectaban a las organizaciones de mayor tamaño ahora están apuntando a pymes y empresas más pequeñas, que no poseen los recursos internos necesarios para enfrentarlas de manera efectiva.

En particular, la llegada de las amenazas evasivas (que utilizan herramientas legítimas para los ataques, incluyen escenarios listos para eludir EPP, son económicas y están disponibles en la red oscura) aumentaron de manera significativa los riesgos de ciberseguridad para las organizaciones que utilizan soluciones de EPP tradicionales.

Estos problemas se acentúan aún más debido a la falta de transparencia proporcionada por las EPP tradicionales. En efecto, estas soluciones ofrecen solo una representación de luz roja/luz verde, para indicar si un ataque se está llevando a cabo o no. Mientras que lo que un equipo de TI con capacidades básicas de seguridad necesita es visibilidad acerca de lo que está sucediendo en endpoints individuales, para poder analizar la situación en más detalle e incrementar el entendimiento de la amenaza.

Por lo tanto, las soluciones de EPP modernas que incorporan capacidades de EDR simples proporcionan un peldaño importante entre la EPP tradicional y las soluciones de EDR más avanzadas y con funcionalidades completas.

Si bien la EPP lo va a proteger contra una amplia variedad de amenazas básicas, también debe considerar la defensa contra amenazas nuevas, desconocidas y evasivas que estén evadiendo la EPP.

Preparar un ataque es cada vez menos costoso para los cibercriminales, lo que pone a más organizaciones en riesgo. Además de ocurrir con más frecuencia, estos tipos de ataques se han vuelto mucho más eficaces debido a que los criminales combinan, prueban y usan varias técnicas para lograr eludir la seguridad de los endpoints.

La urgente necesidad de hacer frente a estas amenazas también es cada vez más crítica debido a cambios como la disolución de los perímetros corporativos a causa del aumento del trabajo remoto. Juntas, estas tendencias crean la necesidad de una EPP cuyas capacidades se extiendan más allá de aquellas proporcionadas por las soluciones de EPP tradicionales y que incluyan, en particular, capacidades de EDR básicas, como el análisis simple de causas raíz.



Elementos clave a tener en cuenta

Entre los indicios que manifiestan que es el momento de expandir las defensas más allá de las EPP tradicionales se encuentran los siguientes:

- La EPP no logra detener un número cada vez mayor de amenazas nuevas, desconocidas y evasivas.
- Su empresa tiene una visibilidad limitada de lo que sucede en los endpoints. Esto incluye la imposibilidad de llevar a cabo análisis de causas raíz, investigar o responder a amenazas en tiempo real, o bien la obligación hacerlo manualmente, con herramientas estándar del sistema operativo (SO) y caso por caso, lo que es lento, complejo y propenso a errores.
- Su empresa no cuenta con especialistas que posean la capacidad o las habilidades de seguridad de TI que se necesitan para hacer frente a amenazas cada vez más sofisticadas.
- Le preocupan las posibles multas o la amenaza a la reputación de su empresa como resultado de un incidente importante de seguridad.

Para implementar una solución eficaz a fin de defenderse contra estas amenazas, deberá considerar aspectos de su organización como el tamaño, perfil corporativo, preparación en seguridad, recursos y experiencia existentes y, en especial, las habilidades de seguridad del equipo de TI o de seguridad de TI.

Paso 3:

Sea claro acerca de lo que desea lograr

Muchas organizaciones tienen tiempo y recursos limitados (o un departamento de seguridad de TI pequeño sin planes de ampliarse), pero deben comprender lo que sucede en la infraestructura y ser capaces de responder a las amenazas evasivas antes de que se produzca el daño.

Agregar las funciones apropiadas de EDR a EPP modernas puede proporcionar una defensa altamente eficaz contra amenazas evasivas más avanzadas. Esto debe permitir respuestas automatizadas rápidas y precisas "con un solo clic", como la cuarentena de archivos, el aislamiento del host, la detención de un proceso, la eliminación de un objeto, etc. Y, si cuenta con especialistas en seguridad de TI, debería ofrecer información, conocimientos y herramientas necesarias para la investigación efectiva, como análisis de causas raíz, creación de indicadores de compromiso (IoC) personalizados, importación de IoC y análisis de estos en todos los endpoints.

También deseará una solución que haga el mejor uso de todas las funciones que realmente necesita, en lugar de pagar por una gran cantidad de funciones que no desea y, luego, tratar de contratar expertos en seguridad de TI con las habilidades necesarias para trabajar con ellas.



Las 5 ideas erróneas más comunes sobre la EDR

1

La protección de nuestros endpoints es perfecta, no necesitamos EDR

Idea errónea: A los ciberdelincuentes no les interesan las empresas como la nuestra: estamos bajo el radar del tipo de ataques que protege la EDR.

Realidad: Es fácil pensar que los ciberdelincuentes no suelen dirigirse a empresas pequeñas, pero la realidad es que las pymes enfrentan varias de las amenazas que también sufren las grandes empresas. Aunque la amplia mayoría de los ciberataques son amenazas genéricas, una gran parte del resto son ataques nuevos, desconocidos y evasivos que eluden las EPP tradicionales. Estas amenazas son difíciles de detectar debido a la variedad de técnicas de evasión que adoptan; en especial, el uso de herramientas legítimas y nativas del sistema. Como permanecen sin ser detectadas por más tiempo, estas amenazas también tienen el tiempo necesario para explorar y atrincherarse en la infraestructura de la empresa y hacer un daño mayor, ya sea por filtración de datos, ataque de ransomware o spyware o la anulación directa de las operaciones.

2

Necesitamos la EDR para compensar una EPP débil

Idea errónea: Nuestra EPP no es lo suficientemente efectiva, por lo que necesitamos reforzarla con EDR.

Realidad: Tratar de reforzar la seguridad de los endpoints agregando una solución de EDR sin abordar los problemas de su EPP es como construir sobre arena movediza. De hecho, una EPP débil puede disminuir la EDR y provocar que no proporcione los resultados esperados. Además, si la solución de EDR es demasiado avanzada para sus necesidades, también puede ser sumamente costosa y, para el equipo, será difícil de comprender y usar.

3

Para usar la EDR, necesita un equipo de especialistas en seguridad de TI

Ideas erróneas: Las pymes y grandes empresas de bajo nivel no poseen suficientes especialistas en seguridad con las habilidades necesarias para comprender y trabajar con herramientas de detección, investigación y respuesta a amenazas evasivas.

Realidad: Cuando se introdujo la EDR por primera vez, los sistemas eran muy complicados y difíciles de usar. Pero con las soluciones modernas, cada vez que reciba una alerta, la EDR le ayudará a entender de dónde proviene la amenaza, cómo se desarrolló, cuál es la causa raíz, si afectó otro host y, por lo tanto, qué alcance tiene. También debe guiarlo a través de un sencillo proceso de manejo de incidentes, que incluya pasos como la identificación, la contención, la erradicación, la recuperación y el análisis de las lecciones aprendidas con el fin de prepararse para futuros ataques.

4

La EDR y la MDR no se pueden combinar

Idea errónea: Si desea una seguridad de clase EDR, deberá invertir en una EDR que esté a cargo de su equipo interno, o bien una detección y respuesta administrada (MDR) tercerizada a cargo de un proveedor especializado.

Realidad: La seguridad de clase EDR no implica optar por una u otra. Tanto la EDR como la MDR poseen beneficios por separado y, a veces, la mejor opción es combinarlas. Por ejemplo, una pyme o empresa grande de bajo nivel puede usar la MDR para aumentar de inmediato su capacidad de seguridad de TI y protegerse contra amenazas evasivas, sin la necesidad de invertir en más empleados o recursos. Por otra parte, una empresa grande con experiencia en seguridad podría usar la MDR para descargar los procesos de investigación y clasificación de incidentes sin interrupciones y enfocar sus recursos de seguridad de TI internos en la respuesta y la investigación detallada.

5

La EDR aumenta la "fatiga por la cantidad de alertas" y no vale la pena el esfuerzo

Idea errónea: La EDR se destaca por generar gran cantidad de alertas y falsos positivos, mientras que los equipos de TI no tienen el tiempo ni los recursos necesarios para actuar o resolverlos.

Realidad: Las soluciones modernas de EDR no solo automatizan varias tareas, sino que la EDR o la MDR también tienen el poder de pasar de una situación de alto riesgo de ataques evasivos a una situación en la que se tiene una confianza renovada en la seguridad de los endpoints. En lugar de no estar seguro de lo que sucede en su entorno, tendrá visibilidad y control de todos los endpoints. Y, en vez de ser reactivo a actualizar su seguridad debido a la complejidad, tendrá una solución simplificada y consolidada, que lo ayudará a optimizar los recursos.

Pruebe nuestro juego de simulación de ransomware interactivo para descubrir cómo mejorar la protección de su infraestructura de TI:

<https://www.kaspersky.com/response-game/es-la/>

Paso 4:

Piense en los casos de uso



Para identificar la protección que mejor se adapte a sus necesidades, debe establecer requisitos claros. Esto significa considerar los aspectos críticos del desempeño y el uso normal de la solución, como los casos específicos para los que la necesita y los resultados que espera que ofrezca.

Por ejemplo, cuando reciba una alerta de seguridad, EDR o MDR deben permitirle responder preguntas claves como:

- ¿Cuál es el contexto de la alerta?
- ¿Qué acciones ya se han realizado en la alerta?
- ¿Sigue activa la amenaza detectada?
- ¿Se ha atacado a otros hosts?
- ¿Qué camino llevó el ataque?
- ¿Cuál es la causa raíz de la amenaza?

También debe ayudarlo a comprender todo el alcance de la amenaza. Por ejemplo:

- Si es susceptible a una amenaza global, es probable que su equipo de administración quiera asegurarse de que no está siendo víctima de un ataque en un momento dado, así que necesitará contar con la capacidad de encontrar un indicador de compromiso (IoC) en línea, ejecutar un análisis y responder a sus inquietudes correctamente.
- Si una autoridad reguladora le solicita ejecutar un análisis para un IoC específico, debe poder importar los IoC de fuentes confiables y ejecutar análisis periódicos para detectar indicios de ataques.
- Si investigó en profundidad una alerta y generó un IoC para la amenaza descubierta, no tendrá que iniciar análisis de toda la red para comprobar si otros hosts fueron afectados, ya que esto se hará automáticamente.

De igual forma, debería ser capaz de responder rápidamente a amenazas prolíficas y de rápida evolución, mediante lo siguiente:

- Contención de amenazas a través del aislamiento del host, la puesta en cuarentena del archivo o el impedimento de la ejecución de archivos durante la investigación
- Uso de una respuesta automatizada entre endpoints basada en análisis de IoC (que le permite responder a amenazas evasivas tan pronto se detectan) o de respuestas guiadas o remotas si utiliza MDR.

Entre los resultados clave que debe esperar de la solución, se incluyen los siguientes:

- Protección contra amenazas evasivas más frecuentes y disruptivas.
- Ahorro de tiempo y recursos con una herramienta simple y automatizada.
- Evaluación del alcance de un ataque, al analizar todos los endpoints en busca de IoC.
- Comprensión de la causa raíz de cada amenaza y cómo ocurrió realmente.
- Rápida respuesta automatizada para evitar más daños.



Las 5 ideas erróneas más comunes sobre la MDR

1

La MDR es simplemente otro servicio de seguridad administrado

Idea errónea: La MDR es como cualquier otro servicio de seguridad administrado (MSS) que incluye la administración de la infraestructura de TI por parte de un proveedor.

Realidad: Generalmente, el MSS cubre una variedad de servicios generales de ciberseguridad, como la evaluación del cumplimiento de normas, tecnologías como VPN y firewalls, pruebas de penetración, recomendaciones, etc. Por su lado, la MDR se enfoca en la detección avanzada y la respuesta rápida a amenazas nuevas, desconocidas y evasivas que eluden las EPP automatizadas, a través de una combinación de TTP para la búsqueda, la detección y el análisis de amenazas.

2

La MDR es solo para las grandes empresas

Idea errónea: Al lidiar con funciones que parecen complejas, como la búsqueda de amenazas y los indicadores de ataque (IoA), la MDR solo es adecuada para las necesidades de las grandes empresas.

Realidad: La MDR no es una solución única que sirve para todas las personas. Brinda diferentes funciones para diferentes tipos de organizaciones. Una pyme o empresa grande de bajo nivel podría usar la MDR para mejorar de forma instantánea su seguridad de TI y protegerse de las amenazas evasivas, mientras que una empresa más grande podría usarla para descargar investigaciones y clasificaciones de incidentes y enfocar mejor sus recursos de seguridad de TI internos.

3

La MDR basada en IA no requiere especialistas humanos

Idea errónea: La inteligencia artificial (IA) y el aprendizaje automático (AA) avanzaron hasta un punto en el que el uso de especialistas humanos en la MDR pronto dejará de existir.

Realidad: La IA, el AA y los IoA propios permiten procesar automáticamente grandes cantidades de alertas, automatizar la clasificación inicial de incidentes, minimizar el tiempo medio de detección (MTTD) y el tiempo medio de respuesta (MTTR) mediante un gran incremento en el rendimiento de los analistas de MDR, así como garantizar una protección continua incluso contra las amenazas más innovadoras que no son malware. Sin embargo, para las TTP que antes eran desconocidas o llevadas a cabo por humanos y que no derivan en la detección automática, la búsqueda de amenazas administrada aún depende del arduo trabajo manual y proactivo de buscadores de amenazas con experiencia.

4

La MDR es difícil de implementar

Idea errónea: A menudo, la MDR se publicita como una solución que proporciona las capacidades de un SOC que trabaja las 24 horas del día, los 7 días de la semana, de modo que su uso debe ser complejo.

Realidad: Como se indica arriba, la MDR se puede usar para todo, desde prevenir amenazas que eluden las ciberdefensas existentes hasta proporcionar una segunda opinión o liberar a los expertos internos para que se centren en tareas más importantes. Se trata de un servicio preconfigurado que se implementa con facilidad y que mejora drásticamente el MTTD y el MTTR. Además, cuanto más rápidos son el MTTD y el MTTR, menor será la cantidad de interrupciones a causa de incidentes y el costo total.

5

Incluso con la MDR, su equipo tiene mucho trabajo por hacer

Idea errónea: Los servicios de MDR se detienen en seco después de la investigación del incidente, por lo que dejan a los clientes a cargo de aplicar informes técnicos y recomendaciones en sus sistemas. Esto añade aún más presión sobre los recursos de seguridad de TI.

Realidad: Si bien esto sucedía en el pasado, gracias a los servicios de MDR modernos, puede optar por autorizar al proveedor para responder por usted automáticamente, iniciar las acciones de respuesta recomendadas por su cuenta (tales como aislar el host, poner los archivos en cuarentena, eliminar archivos, finalizar procesos, solicitar archivos de un programa o ejecutar un programa en el host, analizar IoC, etc.), o bien aprovechar las situaciones de corrección administradas que se pueden aprobar previamente o de forma manual para cada alerta.



El centro de operaciones de seguridad (SOC) y el equipo global de respuesta ante emergencias (GERT) de Kaspersky analizaron los incidentes de seguridad durante todo un año contemplando cada sector con el fin de desarrollar una perspectiva sin igual del panorama de amenazas.

Acceda a los informes:

<https://go.kaspersky.com/mdr-and-ir-reports-2022.html>

Paso 5:

Identifique la protección que mejor se adapte a sus necesidades

Muchas organizaciones no pueden emplear a alguien que se dedique solo a la seguridad de TI. Es posible que algunos recién estén comenzando a construir un departamento de seguridad de TI. Y es probable que otros ya hayan formado y capacitado equipos de seguridad de TI.

Muchas organizaciones no pueden emplear a alguien que se dedique solo a la seguridad de TI. Es posible que algunos recién estén comenzando a construir un departamento de seguridad de TI. Y es probable que otros ya hayan formado y capacitado equipos de seguridad de TI. Por lo tanto, la calidad de la experiencia disponible de estas organizaciones en relación con las defensas contra amenazas variará ampliamente, al igual que la cantidad de tiempo que pueden dedicar a esta tarea.

A fin de hacer frente a las diferentes circunstancias, las organizaciones sin personal dedicado a la seguridad de TI o aquellas cuyo personal de seguridad de TI está sobrecargado con tareas rutinarias, deberán utilizar de manera estratégica la automatización para contrarrestar las amenazas evasivas más recientes.

Esto significa complementar la EPP con herramientas de EDR que, a la vez que protejan contra estas amenazas, también incorporen niveles adecuados de automatización (completo o parcial).

De manera alternativa, en lugar de invertir en una solución de EDR demasiado compleja, para la que tal vez no tengan el tiempo o las habilidades necesarios, la MDR les permite acceder a capacidades como supervisión de seguridad ininterrumpida por parte de expertos del sector, búsqueda automatizada y gestionada de amenazas y escenarios de respuesta guiados y remotos, ya sea de un proveedor, de un proveedor de servicios administrador (MSP) o de un proveedor de servicios de seguridad administrados (MSSP).

Una tercera opción es combinar la EDR y la MDR. Muchas organizaciones no tienen el conocimiento necesario para la búsqueda de amenazas, por lo que, a menudo, una solución ideal es la externalización, al mismo tiempo que se implementan las funciones de detección y respuesta en la empresa. Esto puede ser muy beneficioso para las empresas que quieran desarrollar su propio equipo de ciberseguridad, pero que carecen de los recursos, el personal o las habilidades para respaldar una detección y respuesta especializadas.



¿Qué sucede si solo tiene recursos internos limitados?

Supongamos que tiene recursos internos limitados en seguridad de TI o un pequeño equipo de uno o dos especialistas en seguridad. Supongamos también que está intentando decidir si debe complementar la EPP con EDR o MDR. ¿Qué tipo de beneficios puede esperar y qué sería adecuado para usted?

Si prefiere un enfoque más práctico (y su equipo de TI tiene habilidades de seguridad de TI suficientemente desarrolladas), la EDR puede ayudar a prevenir interrupciones de la actividad y daños a la empresa, mediante la eliminación de los riesgos que representan las amenazas nuevas, desconocidas y evasivas; además, proporciona al personal de seguridad la visibilidad necesaria para la investigación de amenazas, el análisis de causas raíz y la respuesta.

Esto puede impulsar la eficacia de los costos, dado que posibilita que el equipo de seguridad trabaje de manera más eficiente sin tener que hacer malabares con varias herramientas y consolas, y maximiza la capacidad mediante la automatización de una amplia variedad de procesos. También le brinda tranquilidad, ya que le facilita la supervisión y la detección de amenazas, además de la prevención de ataques y la respuesta a estos.

Si busca ampliar su capacidad de seguridad de TI interna mediante la reducción de la carga que representan las tareas clave de respuesta y detección, la MDR puede ofrecer protección avanzada e ininterrumpida contra amenazas que, de otro modo, pueden burlar las barreras de seguridad automatizadas. Esto puede ayudar a potenciar su negocio, al resolver la escasez de especialistas en ciberseguridad y proporcionar todos los beneficios importantes de un SOC de forma ininterrumpida.

La MDR también puede impulsar la eficiencia de los costos, al permitir que los recursos internos se centren en las tareas críticas que realmente exigen la participación del equipo de TI o de seguridad de TI, y maximizar la capacidad al aprovechar los modelos de aprendizaje automático avanzados para aumentar de manera significativa el rendimiento de los analistas y minimizar el MTTR. Además, puede ofrecer supervisión continua de la seguridad por parte de expertos del sector, junto con una búsqueda automatizada y administrada de amenazas. Esto incluye el análisis de amenazas complejas que no son malware y de amenazas peligrosas y que sean difíciles de detectar con herramientas legítimas del SO durante los ataques.

Por otra parte, la combinación de EDR y MDR le permite adaptar sus respectivas funciones de clase EDR a las necesidades particulares de su empresa, por ejemplo, mediante la externalización de la búsqueda de amenazas (para la cual quizás no tenga la experiencia necesaria) mientras implementa las funciones de detección y respuesta en endpoints internamente.

Cómo evaluar los requisitos de seguridad en evolución: XDR

El 40 % de las organizaciones implementará una plataforma de XDR antes de 2027, lo que supone un gran aumento con respecto al 5 % en 2021

Según el Estudio de organizaciones con resiliencia cibernética de 2021 de IBM, el 32 % de las organizaciones informó que utiliza entre 21 y 30 herramientas de seguridad individuales en respuesta a cada amenaza, mientras que el 13 % informó que utiliza 31 o más.

Como consecuencia de la cantidad de herramientas involucradas, se demora mucho en identificar y contener amenazas avanzadas.

El informe sobre el Costo de una filtración de datos de 2022 de IBM descubrió que se necesitaron 277 días para detectar y resolver una filtración de datos promedio, por lo que una filtración que ocurre el 1 de enero se contendría recién el 4 de octubre.

XDR en pocas palabras

Si su organización es mediana o grande y el SOC o equipo de seguridad de TI todavía no le hablaron acerca de la XDR, es solo una cuestión de tiempo hasta que lo hagan.

Como indicó CRN (15/2/23), "cuando se trata de la detección y respuesta de amenazas, ya no alcanza con observar el endpoint o la red". Con respecto a esto, el método que buscan muchas de las empresas de ciberseguridad más grandes del mundo es XDR (detección y respuesta extendidas). XDR, que es una de las categorías con mayor tasa de crecimiento en la ciberseguridad actual, tiene como fin proporcionar seguridad mejorada mediante la correlación de datos de los diferentes entornos y dispositivos de una organización y la posterior priorización de las amenazas más graves para brindar una respuesta.

"Sin importar exactamente cómo se definen, todas las plataformas de XDR se enfocan en darle un impulso a los equipos de seguridad limitados, con el objetivo de mejorar la calidad de la detección de amenazas mientras se reduce la sobrecarga de alertas".

Con XDR, las soluciones de seguridad que no están necesariamente diseñadas para trabajar en conjunto pueden interoperar sin problemas en la prevención, detección, investigación y respuesta a amenazas. Y, al eliminar las brechas de visibilidad entre las herramientas y capas de ciberseguridad, la XDR permite que los equipos sobrecargados de seguridad detecten y enfrenten amenazas con una mayor velocidad y eficiencia, y capturen datos contextuales más completos, para ayudarlos a tomar mejores decisiones de seguridad y prevenir ataques futuros.

¿Qué es lo que hace la XDR exactamente, cuáles son los beneficios y por qué puede ser una de las inversiones en seguridad más importantes que hará su organización?



Comparación entre XDR, MDR y EDR

EDR

Detección y respuesta en endpoints

- Identifica las amenazas nuevas, desconocidas y evasivas que evaden la protección de los endpoints, y automatiza las tareas de seguridad de rutina.

MDR

Detección y respuesta administradas

- Descarga la detección de amenazas, búsqueda de amenazas e investigación de incidentes o complementa las medidas existentes con una protección de amenazas avanzadas ininterrumpida

XDR

Detección y respuesta extendidas

- Detecta de forma proactiva amenazas complejas en varios niveles de la infraestructura y responde y contrarresta automáticamente estas amenazas.

Funcionamiento

- Mejora la visibilidad y la visualización de amenazas
- Proporciona mecanismos de detección avanzados (p. ej., IoC, IoA)
- Simplifica el análisis de causas raíz y respalda la búsqueda de amenazas
- Ofrece una respuesta rápida y automatizada
- Ofrece una protección administrada continua, incluso contra las amenazas sin malware más complejas e innovadoras
- Se integra con múltiples herramientas de seguridad, aplicaciones e infraestructura de ciberseguridad existente
- Supervisa los datos de varias fuentes para detectar y eliminar amenazas complejas

Valor comercial

- Permite que los equipos de seguridad de TI trabajen con mayor eficacia sin tener que hacer malabares con diversas herramientas y consolas
- Automatiza una amplia gama de procesos para evitar la dependencia en procesos de corrección tradicionales, que pueden resultar en tiempos de inactividad
- Facilita la supervisión y detección de amenazas, agrega datos de análisis forenses de forma centralizada, responde a ataques y los previene
- Concentra los recursos internos costosos en las tareas críticas que realmente requieren la participación de un equipo de seguridad de TI
- Utiliza modelos de aprendizaje automático patentados para aumentar considerablemente el rendimiento de los analistas y reducir el MTTD y el MTTR
- Resuelve la escasez de especialistas en ciberseguridad
- Proporciona todos los principales beneficios de un SOC que trabaja las 24 horas del día, los 7 días de la semana
- El enfoque del ecosistema maximiza la eficiencia de las herramientas de ciberseguridad utilizadas, ahorra recursos y reduce el riesgo
- Simplifica el trabajo de los especialistas en seguridad de TI y les proporciona el contexto adicional necesario para investigar los ataques multivectoriales
- Minimiza el tiempo medio de detección y tiempo medio de respuesta (MTTD/MTTR), fundamentales para combatir las amenazas complejas y los ataques dirigidos
- Proporciona una protección integral contra el panorama cambiante de las amenazas

¿Para quién va dirigido?

- Empresas con aversión al riesgo y conservadoras en términos de tecnología, que desean agregar visibilidad a la protección automática
 - Usuarios de TI convencionales que desean desarrollar procesos de respuesta a incidentes
 - Organizaciones que utilizan TI como ventaja competitiva y necesitan que los expertos puedan buscar y neutralizar amenazas complejas
 - Empresas que buscan ampliar la capacidad interna de seguridad informática liberándose de las tareas clave de detección y respuesta
 - Organizaciones que podrían no tener el presupuesto o el personal especializado disponible para crear su propio SOC interno
- Organizaciones con recursos de seguridad significativos que desean una plataforma única que ofrezca lo siguiente:
- Una imagen coherente de lo que ocurre en toda su infraestructura
 - Búsqueda de amenazas e inteligencia de amenazas integradas
 - Priorización de incidentes superior y menos alertas de falsos positivos

Capacidades y beneficios específicos que debería esperar de una plataforma de XDR



La plataforma única integra varias herramientas de seguridad

Con XDR, las soluciones de seguridad que no están necesariamente diseñadas para trabajar en conjunto pueden interoperar sin problemas en la prevención, detección, investigación y respuesta a amenazas.

- Por ejemplo, estas podrían incluir soluciones diseñadas para proteger correo, web, la red, infraestructura en la nube, aplicaciones, identidad, etc., al permitir que tipos adicionales de escenarios de ataque puedan detectarse e investigarse, y fortalecer el proceso para combatir amenazas complejas.
- XDR también puede integrar herramientas de inteligencia de amenazas, como fuentes de datos de amenazas y la plataforma que se utiliza para administrar estos datos, para brindarles a los equipos de SOC el contexto adicional que tiene tanta importancia durante la investigación de incidentes cibernéticos complejos.
- Además, según los requisitos y la industria de una organización, la XDR puede integrar herramientas de seguridad de Internet de las cosas (IoT) y tecnología operativa (OT) para extender una protección de seguridad integral sobre todos los entornos de TI/OT.



Une diferentes tipos de telemetría

Al posibilitar el análisis de telemetría y de comportamiento en tiempo real a través de varias capas de seguridad, incluidos los endpoints, la red y la nube, los analistas de seguridad pueden visualizar las ciberamenazas con mayor precisión, y abordar y eliminar amenazas en función de la severidad con la que impactan la infraestructura de TI de la organización.



Proporciona una visibilidad integral de las amenazas

Al descomponer los silos entre las soluciones de punto específicas a cada capa, la XDR les da a los SOC y los equipos de seguridad de TI la visibilidad de extremo a extremo y la integración que necesitan para identificar amenazas con mayor agilidad, responder a ellas más rápido, corregirlas más efectivamente y minimizar el daño que puedan causar.

Debido a que la XDR puede vincular cada paso de una cadena de ataque completa y presentarlo como una alerta única en la que se detalla todo el contexto del ataque, se reduce la cantidad de alertas, se aumenta su calidad y se proporcionan orquestación y respuesta integrales.



Simplifica y centraliza la recopilación de datos y aumenta la eficiencia

Un único lago de datos proporciona recopilación, administración y almacenamiento integrales de registros, al proporcionar una plataforma centralizada para recopilar, indexar y analizar los registros de diferentes fuentes, incluidos soluciones de seguridad (EPP, FW, NGFW, IAM, SIEM, SOAR, etc.), sistemas operativos, aplicaciones empresariales (sistemas de RR. HH., herramientas de oficina), seguridad física (sistemas de control de acceso automatizado) y otros dispositivos.

Esto permite a los equipos del SOC y de seguridad de TI obtener información valiosa, detectar anomalías e identificar posibles incidentes de seguridad al utilizar datos de registros enriquecidos que cubren eventos pasados y presentes (en tiempo real). La integración con otras plataformas y herramientas de seguridad también mejora la eficiencia operativa, al centralizar la gestión de seguridad y proporcionar una vista unificada de los eventos e incidentes de seguridad.



Acelera la detección, investigación y respuesta a amenazas

Al eliminar las brechas de visibilidad entre las herramientas y capas de ciberseguridad, la XDR permite que los equipos de seguridad sobrecargados detecten y enfrenten amenazas con una mayor velocidad y eficiencia, y capturen datos contextuales más completos, para ayudarlos a tomar mejores decisiones de seguridad y prevenir ataques futuros.

Mediante la automatización de tareas de rutina, como la clasificación, contención y resolución de amenazas, las organizaciones pueden optimizar sus recursos de seguridad y enfocarse en actividades más estratégicas.



Reduce el tiempo medio de detección y respuesta (MTTD y MTTR)

La XDR ayuda a minimizar el tiempo medio de detección (MTTD) y el tiempo medio de respuesta (MTTR), fundamentales para combatir ataques selectivos y amenazas complejas, en los cuales las acciones rápidas realizadas por los expertos en seguridad de TI reducen el tiempo de permanencia y las posibilidades de que los atacantes logren su objetivo de causar daños en las finanzas y la reputación de una organización.



Mejora la búsqueda de amenazas

Al utilizar la inteligencia de amenazas más reciente, la XDR mejora la búsqueda y detección de amenazas, mientras que la automatización de las tareas rutinarias, los procesos de investigación guiados y las detecciones personalizables promueven una resolución rápida para los incidentes. La detección y neutralización rápidas y precisas de las amenazas avanzadas es crucial para enfrentar ataques complejos y APT.



Ayuda a abordar la escasez mundial de expertos en seguridad de TI

Ante una falta global de expertos en TI, la XDR proporciona una protección holística para una infraestructura de TI en cambio y expansión, frente a un entorno de ciberamenazas que evoluciona rápidamente. La XDR simplifica los trabajos de los recursos valiosos que escasean, como especialistas en seguridad de TI, reduce su necesidad de involucrarse en tareas rutinarias y les permite tener tiempo para trabajar en incidentes complejos.



Contribuye al cumplimiento normativo y a la gestión de riesgos

Al proporcionar capacidades integrales de visibilidad, inteligencia de amenazas y generación de informes, las organizaciones pueden demostrar que cumplen con las normativas y los marcos de la industria, como la RGPD, PCI DSS, HIPAA y otros. Esto las ayuda a mitigar los riesgos legales y financieros asociados con el incumplimiento.

La administración de registros también cumple una función fundamental para garantizar el cumplimiento de los estándares y las normativas industriales o regionales, al facilitar el almacenamiento y la retención de datos y registros durante los períodos estipulados y permitirles a las organizaciones recuperar y analizar registros con facilidad cuando es necesario.



Brinda administración fácil de usar a través de una única consola

Las soluciones de XDR intuitivas proporcionan información integral sobre las amenazas actuales y las actividades sospechosas a través de una única consola. Esto facilita la búsqueda proactiva de amenazas y la respuesta rápida a incidentes, y brinda una vista holística que ayuda a los equipos del SOC a identificar actividades sospechosas y potenciales incidentes de seguridad con mayor eficiencia.



Opciones de plataforma abierta y nativa

La XDR abierta admite la integración con soluciones de terceros para recopilar formas específicas de telemetría, a fin de proporcionar detección, búsqueda e investigación de amenazas en diferentes orígenes de datos y ejecutar acciones de respuesta. Esto evita que se dependa de un solo proveedor y permite que las organizaciones aprovechen herramientas de seguridad de terceros ya implementadas y elijan los productos más adecuados de diferentes proveedores.

La XDR nativa es una solución desarrollada por un único proveedor y diseñada para funcionar con los productos de ese proveedor.



Implementación local o en la nube

Si bien la gran mayoría de las plataformas de XDR son abiertas y están basadas en la nube, la implementación local es ideal para las organizaciones que desean contar con una soberanía de datos completa y garantizar el cumplimiento de normativas y requisitos.



Integración con la confianza cero

Cuando se usan en conjunto, la XDR y Confianza Cero proporcionan una defensa avanzada frente a las ciberamenazas. Confianza Cero ayuda a prevenir el acceso no autorizado a recursos y aplicaciones o revocar el acceso ya otorgado si las condiciones cambiaron, mientras que la XDR ayuda a detectar y responder a amenazas potenciales que logran eludir esos controles de acceso iniciales.



Comparación entre XDR, SIEM y SOAR

XDR

Detección y respuesta extendidas

- Detecta de forma proactiva amenazas complejas en varios niveles de la infraestructura y responde y contrarresta automáticamente estas amenazas.

SIEM

Administración de información y eventos de seguridad

- Recopila, unifica, analiza y almacena los datos de registro de toda la infraestructura de TI para casos de uso, como el control y cumplimiento normativo, y la coincidencia y correlación basadas en reglas para la actividad sospechosa

SOAR

Orquestación, automatización y respuesta de seguridad

- Recibe datos de diversas fuentes en toda la infraestructura, incluidos los sistemas de administración y las plataformas de inteligencia de amenazas, y brinda un análisis prioritario
- Permite a los equipos de seguridad configurar respuestas automatizadas de varias etapas y soluciones ante amenazas entrantes

Funcionamiento

- Integra varias herramientas y aplicaciones de seguridad
- Supervisa los datos de los endpoints, las redes, las nubes, los servidores web, los servidores de correo, etc. para detectar y eliminar amenazas complejas
- Busca patrones o eventos que podrían indicar un comportamiento sospechoso y genera una alerta para el SOC o el equipo de seguridad de TI
- Utiliza manuales para automatizar una amplia variedad de flujos de trabajo, como el análisis de vulnerabilidades, el análisis de registros, la gestión de accesos de los usuarios, la clasificación de amenazas y más
- Coordina diversas herramientas y procesos dispares en un flujo de trabajo más amplio, que recopila todos los datos relevantes en una única plataforma para obtener información unificada y útil

Entonces, ¿cuáles son las diferencias?

- El enfoque del ecosistema maximiza la eficiencia de las herramientas de ciberseguridad utilizadas, ahorra recursos y reduce el riesgo
- Simplifica el trabajo de los especialistas en seguridad de TI y les proporciona el contexto adicional necesario para investigar los ataques multivectoriales
- Minimiza el tiempo medio de detección y tiempo medio de respuesta (MTTD/MTTR), fundamentales para combatir las amenazas complejas y los ataques dirigidos
- Proporciona una protección integral contra el panorama cambiante de las amenazas
- El enorme conjunto de datos proporcionado por SIEM puede generar demasiadas alertas que deben filtrarse, procesarse y analizarse manualmente
- No proporciona el contexto necesario para enfrentarse a ataques nuevos, complejos o sofisticados
- Una solución pasiva que no incluye capacidades de bloqueo, cuarentena o respuesta
- Funciona mejor cuando se utiliza en conjunto con soluciones de investigación y respuestas proactivas, como XDR o SOAR
- El mantenimiento de una plataforma SOAR bien configurada que se integre con las herramientas de los partners requiere el esfuerzo continuo de un SOC altamente capacitado y experimentado
- Sin este mantenimiento especializado y minucioso, los analistas de SOAR pueden terminar con demasiadas alertas de baja prioridad, falsos positivos y un conjunto de datos generalmente incoherente, como resultado de todas las herramientas diferentes y aisladas que se integran en la plataforma: justo lo que intentaban evitar

Cómo justificar la inversión en XDR

Junto con los beneficios técnicos, existen buenas razones comerciales para invertir en XDR, como aquellas relacionadas con la mitigación de ataques, detección de amenazas internas, nube y cumplimiento, investigación y respuesta de incidentes y más.



Mitigación de ataques

Si una organización fue víctima de un ataque de ransomware que generó el cifrado de datos críticos y la suspensión de las operaciones, las capacidades de detección de amenazas proactiva de la XDR habrían ayudado a identificar y prevenir este tipo de ataque antes de que pudieran causar estragos, a través de la capacidad de detectar comportamientos sospechosos, aislar endpoints infectados y proporcionar respuesta a incidentes en tiempo real, reduciendo considerablemente el impacto del ataque y restaurando la continuidad del negocio de forma rápida.



Detección de amenazas internas

Las amenazas internas son una de las principales preocupaciones para la mayoría de las organizaciones: ya sean deliberadas o no. Pero, debido a que la XDR proporciona una visibilidad integral de todos los endpoints, redes, aplicaciones y la nube, puede detectar indicios reveladores de amenazas internas, como comportamientos anómalos de usuarios, intentos de exfiltración de datos y accesos no autorizados. Y, mediante la correlación y el análisis de datos de varios orígenes, la XDR puede ayudar a identificar y mitigar amenazas internas, proteger información confidencial y mantener la integridad de los datos.



Nube y cumplimiento

A medida que más organizaciones adoptan tecnologías en la nube, garantizar la seguridad y el cumplimiento es cada vez más importante. Al proporcionar visibilidad y detección de amenazas unificadas en entornos híbridos y de varias nubes, la XDR permite que las organizaciones supervisen cargas de trabajo en la nube, detecten configuraciones erróneas e identifiquen actividades sospechosas para, de ese modo, mantener una infraestructura en la nube segura y que cumpla con las normativas, mientras mitigan los riesgos asociados con ataques basados en la nube.



Respuesta e investigación de incidentes

Las respuestas rápidas y las investigaciones exhaustivas son fundamentales para minimizar los daños y prevenir incidentes futuros. La XDR simplifica los procesos de respuesta a incidentes al automatizar los flujos de trabajo de detección de amenazas, la clasificación de alertas y la investigación, y al proporcionarles a los equipos de seguridad una visión integral de los incidentes, para que puedan responder de forma rápida y efectiva. Los ahorros de tiempo y recursos que derivan de las capacidades de respuesta automatizada de la XDR la convierten en una solución revolucionaria en la administración de incidentes.



Complemento de EPP, EDR, SIEM y mucho más

Prevenir los tipos de amenazas que se mencionan arriba más que justifica la inversión en XDR, mientras que, para los usuarios de EPP, EDR, SIEM y más, la XDR fortalece el rendimiento de todas estas soluciones.

- Para las **EPP**, la XDR mejora las capacidades de protección de endpoints al proporcionar detección de amenazas avanzadas, automatización de respuestas y mayor visibilidad en entornos de red y en la nube, lo que la convierte en el próximo paso lógico en las hojas de ruta de seguridad, y permite que las organizaciones alcancen un mayor nivel de protección contra las amenazas en evolución.
- Para la **EDR**, la XDR (que se suele desarrollar a partir de la EDR) extiende las capacidades de la solución más allá de la detección y la respuesta enfocadas en los endpoints, al proporcionar visibilidad y detección de amenazas holísticas en la infraestructura protegida (incluidos entornos de la nube, aplicaciones, máquinas virtuales y la red) y al proporcionar una respuesta a incidentes más eficiente y mejores capacidades de búsqueda de amenazas.
- Para **SIEM**, la XDR complementa la solución al proporcionar detección de amenazas en tiempo real, capacidades de respuesta avanzadas y mejor visibilidad y correlación de los eventos de seguridad en todos los endpoints, redes y en la nube, lo que facilita una respuesta a incidentes más rápida y tiempos de investigación reducidos.

Para aquellos que tienen probabilidades de invertir en tecnología de XDR en el futuro cercano, la facilidad de uso es, por lejos, el beneficio percibido más importante para su organización, ya sea que tengan pensado integrar la tecnología con sus herramientas de seguridad existentes o establecer una infraestructura de XDR de un único proveedor. Los encuestados también indicaron otras inversiones a corto plazo en soluciones para unificar la detección y la respuesta y para mejorar la visibilidad de productos/servicios de seguridad tenían más probabilidades de implementar detección y respuesta en endpoints (EDR), detección y respuesta en la red (NDR), administración de eventos e información de seguridad (SIEM) e inteligencia de amenazas.

CRA Business Intelligence, XDR Poised to Become a Force Multiplier for Threat Detection, marzo de 2022



Abordar el panorama general de amenazas

En muchas organizaciones, los analistas de seguridad dedican más de la mitad de su tiempo a descartar falsos positivos, en lugar de a la búsqueda y respuesta proactivas a amenazas, lo que aumenta de forma significativa los tiempos de detección

Inteligencia de amenazas

Para muchas organizaciones, y en especial aquellas que son vulnerables a ataques selectivos y APT, la **inteligencia de amenazas** es una herramienta fundamental en la defensa proactiva contra amenazas. Pero, aunque sus usos y beneficios son muchos y variados, sus orígenes también lo son, lo que significa que identificar lo más efectivo para una organización en particular puede ser todo un desafío.

En muchas organizaciones, los analistas de seguridad dedican más de la mitad de su tiempo a clasificar falsos positivos en lugar de buscar y responder de forma proactiva, lo que lleva a un aumento considerable de los tiempos de detección. Basar las operaciones de seguridad en inteligencia irrelevante o inexacta multiplica el volumen de alertas falsas y supone un impacto grave y negativo en las capacidades de respuesta, así como en la seguridad en general. Entonces, ¿cómo puede evitar esto?

Aunque no hay un criterio universal unívoco para evaluar los productos comerciales de inteligencia de amenazas, estos son algunos aspectos para tener en cuenta:

- Con una amplia gama de proveedores entre los que elegir, las organizaciones deben buscar la inteligencia de amenazas que transforme su comprensión del panorama de amenazas específico (por ejemplo, a través del análisis detallado de amenazas históricas y emergentes dirigidas a su industria, región o empresa particular), a fin de mejorar el rendimiento de funciones, como la gestión de vulnerabilidades, búsqueda de amenazas, respuesta ante incidentes y muchas otras.
- Para combinar de manera eficaz la inteligencia de amenazas con las herramientas de seguridad, los controles y los procesos que una organización ya utiliza y conoce, se deben buscar métodos de entrega, mecanismos de integración y formatos que admitan la integración fluida de la inteligencia de amenazas en sus operaciones de seguridad existentes.
- Además, es importante identificar inteligencia de amenazas con alcance global. Los ataques no tienen fronteras: ¿el proveedor obtiene información a nivel global y recopila actividades aparentemente inconexas en campañas integrales, ya que este tipo de información le ayudará a tomar medidas más adecuadas?
- Las organizaciones que buscan contenidos más estratégicos para orientar su planificación de seguridad a largo plazo deben buscar un proveedor de inteligencia de amenazas con antecedentes comprobados de detección e investigación continua de amenazas complejas en su región o industria.
- La capacidad del proveedor de adaptar sus capacidades investigativas a los aspectos específicos de su organización también es un factor crítico.

La inteligencia de amenazas (TI) es un recurso en evolución constante. Para ser efectivos, los programas internos de TI que lo utilizan no pueden quedarse atrás. Evalúe su rendimiento actual con nuestra herramienta de TI interactiva y obtenga recomendaciones personalizadas para mejorar en función de las respuestas: https://go.kaspersky.com/ti_tool_2023.html

Además, utilizar Kaspersky Threat Intelligence Portal ayuda a una organización a unificar, administrar y poner en práctica la inteligencia de amenazas, lo que resulta fundamental cuando las herramientas de seguridad utilizan inteligencia de amenazas de varios orígenes. Específicamente, Kaspersky Threat Intelligence Portal debería ayudar a la organización a hacer lo siguiente:

- Responder a amenazas de manera más eficaz, al verificar cualquier indicador de amenazas que se considere sospechoso, se trate de un archivo, un hash de archivo, una dirección IP o una dirección web.
- Analizar archivos para detectar amenazas avanzadas de generalizadas, evasivas y de tipo APT.
- Enviar direcciones IP, hashes de archivos, dominios o direcciones web que se consideren sospechosas, para validar y priorizar rápidamente alertas e incidentes mediante niveles de riesgo e información contextual complementaria, para determinar cuáles son amenazas reales.
- Recibir informes de manera regular sobre el comportamiento de archivos o direcciones web específicos.
- Automatizar flujos de trabajo mediante la vinculación de aplicaciones relevantes con Kaspersky Threat Intelligence Portal.

Una formación sobre concienciación

Más del 80 % de los incidentes de ciberseguridad se deben a errores humanos.

Más del 80 % de todos los incidentes de ciberseguridad se deben a errores humanos, entre otras cosas porque, como las soluciones de ciberseguridad se desarrollan y se adaptan con rapidez a amenazas complejas, les dificultan la tarea a los cibercriminales, que, como respuesta, apuntan al elemento más vulnerable de la ciberseguridad: el factor humano. Algunos ejemplos de impactos de lo mencionado son los siguientes:

- El 52 % de los ejecutivos de alto nivel afirma que los empleados son la mayor amenaza para la seguridad operativa.
- El 43 % de las pequeñas empresas sufrió un incidente de seguridad a causa de infracciones de las directivas de seguridad de TI por parte de empleados.
- El 60 % de los empleados tiene datos confidenciales en su dispositivo corporativo (datos económicos, base de datos de correo electrónico, etc.).
- El 30 % de los empleados admite que comparte sus credenciales de inicio de sesión de la PC con los colegas.

Una cultura de comportamiento seguro en el ámbito digital, junto con la concientización y las habilidades de ciberseguridad fundamentales en toda la organización, son la clave para reducir la superficie de ataque y el número de incidentes a los que el equipo de TI debe hacer frente.



Cómo Kaspersky puede ayudar



**Kaspersky Next
EDR Foundations**

[La protección avanzada de endpoints basada en aprendizaje automático, los controles de seguridad flexibles y las herramientas de análisis de causas raíz de EDR de Kaspersky Next EDR Foundations](#) le brindan todas las herramientas que necesita para construir una base sólida para su ciberseguridad. Una consola simple, con despliegue local o en la nube, y diversas funciones que promueven una mejor calidad de vida laboral, reducen la complejidad y aumentan la eficiencia.



**Kaspersky Next
EDR Optimum**

[Kaspersky Next EDR Optimum](#) proporciona una protección de endpoints sólida, controles mejorados, formación, administración de parches y más, todo mejorado con la funcionalidad esencial de EDR. La visibilidad de las amenazas, su investigación y respuesta son simples, rápidas y guiadas para ayudar a los equipos de TI y de seguridad de TI a desviar los ataques rápidamente y con recursos mínimos.



**Kaspersky Next
XDR Expert**

[Kaspersky Next XDR Expert](#) se integra sin problemas a la infraestructura de seguridad existente de una organización, y proporciona visibilidad en tiempo real y conocimientos exhaustivos acerca de las amenazas en evolución, para ofrecer detección de amenazas avanzada y respuestas automatizadas, así como también las capacidades de XDR esenciales detalladas en este libro electrónico.



**Kaspersky
Managed Detection
and Response**

[Kaspersky MDR](#) ofrece una protección avanzada e ininterrumpida frente al creciente volumen de amenazas que eluden las barreras de seguridad automatizadas, para ayudar a las organizaciones que tienen dificultades para encontrar personal especializado o que cuentan con recursos internos limitados. Sus capacidades superiores de detección y respuesta están respaldadas por uno de los equipos de búsqueda de amenazas más exitosos y experimentados del sector. A diferencia de otros productos similares, Kaspersky MDR utiliza modelos de aprendizaje automático patentados, inteligencia de amenazas exclusiva y un eficaz historial probado de investigación de ataques selectivos. Fortalece la resiliencia corporativa frente a las ciberamenazas de manera automática, al mismo tiempo que optimiza los recursos existentes y futuras inversiones en seguridad de TI.



**Kaspersky
Threat Intelligence**

[La cartera de inteligencia de amenazas de Kaspersky](#) cubre una amplia gama de escenarios de seguridad (prevención, detección, investigación, respuesta, informes estratégicos, etc.), que se pueden adaptar a las necesidades de organizaciones individuales. Nuestro Equipo de Investigación y Análisis Global (GReAT) es un grupo selecto de expertos que, al infiltrarse en comunidades cerradas y foros oscuros de todo el mundo, descubrieron y analizaron más de 50 de los ataques selectivos más sofisticados del mundo. Y, gracias a nuestros conocimientos, experiencia e inteligencia avanzada sobre todos los aspectos de la ciberseguridad, nos convertimos en un partner de confianza de las fuerzas del orden público y las agencias gubernamentales más importantes, entre las que se incluyen la Interpol e importantes equipos CERT.

Ejemplos de nuestras soluciones y servicios de inteligencia de amenazas innovadores incluyen más de 20 tipos de orígenes de datos sobre amenazas; una amplia gama de informes de inteligencia de amenazas; un entorno de pruebas desarrollado internamente para detectar amenazas sofisticadas y evasivas; un portal abierto de inteligencia de amenazas, y servicios como análisis del panorama de amenazas específico de clientes y [Kaspersky Digital Footprint Intelligence](#), que analiza datos de rastros digitales para identificar potenciales amenazas y vulnerabilidades.



**Kaspersky
Security
Awareness**

Kaspersky Security Awareness ofrece una variedad de soluciones de formación atractivas y efectivas, que impulsan la concientización sobre la ciberseguridad de los empleados en todos los niveles y los ayuda a cumplir con su función en la ciberseguridad general. Dado que los cambios perdurables en el comportamiento llevan tiempo, nuestro enfoque implica el desarrollo de un ciclo de aprendizaje continuo con múltiples componentes, que incluye simulaciones interactivas de protección que cubren una variedad de escenarios de la industria; herramientas lúdicas de evaluación; una plataforma automatizada de concientización sobre la seguridad que proporciona campañas de phishing simuladas; formación para ejecutivos de alto nivel, y más.



**Kaspersky
Professional
Services**

La cartera de Kaspersky Professional Services de servicios de evaluación, implementación, mantenimiento y optimización ayuda a las organizaciones a satisfacer sus necesidades únicas, minimizar los riesgos de seguridad, maximizar el retorno de la inversión, minimizar la presión sobre los recursos, responder de forma rápida a las nuevas amenazas de seguridad y obtener el máximo beneficio de las soluciones de Kaspersky.



Confianza



**Proven.
Transparent.
Independent.**

En 2017, Kaspersky lanzó la **Iniciativa de transparencia global**. A diferencia de otros proveedores similares, si tiene alguna inquietud sobre nuestros productos, puede revisar el código fuente, las actualizaciones de software y las reglas de detección de amenazas, así como nuestros procesos de ciclo de vida de desarrollo seguro y las estrategias de mitigación de riesgos de software y de cadena de suministro. Para respaldar esta iniciativa, abrimos más de 10 Centros de transparencia en todo el mundo, que recibieron visitas de reguladores, proveedores de infraestructura crítica, clientes, partners, medios de comunicación y más. En caso de que alguno de nuestros clientes lo requiera, contamos con auditorías de SOC 2 y certificación ISO/IEC 27001.



**Kaspersky
Next**

Para obtener más información sobre Kaspersky Next visita:
https://go.kaspersky.com/next_latam

Noticias sobre ciberamenazas: securelist.lat
Noticias sobre seguridad de TI: business.kaspersky.com
Seguridad de TI para pymes: kaspersky.com/business
Seguridad de IT para grandes empresas:
latam.kaspersky.com/enterprise-it-security

latam.kaspersky.com

© 2023 AO Kaspersky Lab.
Las marcas registradas y las marcas de servicio
pertenecen a sus respectivos propietarios.

Obtenga más información acerca de Kaspersky Next en:
<https://go.kaspersky.com/next>

Elija el nivel que más se adapte a sus necesidades al
realizar una encuesta breve con nuestra herramienta
interactiva:
https://go.kaspersky.com/Kaspersky_Next_Tool

