Kaspersky Next XDR Expert

Revelando Kaspersky Next XDR Expert

¿Qué es Kaspersky Next XDR Expert?

Como el más avanzado de los tres niveles de producto de Kaspersky Next, Kaspersky Next XDR Expert se integra sin problemas con la infraestructura de seguridad existente de la organización, y proporciona visibilidad en tiempo real y conocimiento exhaustivo sobre las ciberamenazas en evolución, ofreciendo una detección de amenazas avanzada, respuestas automatizadas y una amplia gama de capacidades de XDR esenciales.

¿Por qué Kaspersky Next XDR Expert y por qué ahora?

Los ciberdelincuentes mejoran sus prácticas todo el tiempo y desarrollan maneras cada vez más sofisticadas de atacar a las organizaciones. 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.

Por ejemplo, las amenazas persistentes avanzadas (APT) eluden la detección tradicional de endpoints y pueden mantenerse activas durante semanas o meses: mientras se mueven lateralmente a través de la red, ganan 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.

Lograr una seguridad efectiva frente a estas amenazas requiere un enfoque integral y proactivo que combine tecnologías avanzadas, directivas robustas, supervisión constante, capacitación continua y más. Y esta es, en efecto, la visión 360 ° del entorno de amenazas que XDR se propone ofrecer.

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

¿Cómo XDR soluciona estos problemas?

La palabra “extendida” en detección y respuesta extendida refleja el hecho de que, en XDR, una solución de detección y respuesta de endpoints (EDR) está complementada por una variedad de otras herramientas de seguridad (e integrada estrechamente con estas).

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 correos, web, la red, infraestructura en la nube, aplicaciones, identidad, etc., permitiendo que tipos adicionales de escenarios de ataque puedan detectarse e investigarse, y fortaleciendo el proceso de combatir ciberamenazas complejas.

Al proporcionar una única interfaz para acceder a las herramientas y capas de ciberseguridad, XDR ofrece una visibilidad completa entre ellas. Esto permite a los equipos de seguridad sobrecargados detectar y combatir amenazas con mayor rapidez y eficiencia, capturando datos contextuales más completos para ayudarles a tomar mejores decisiones de seguridad y prevenir ataques futuros.

Para combatir ciberamenazas cada vez más sofisticadas, las organizaciones necesitan más que un conjunto unificado de herramientas de seguridad del mismo proveedor

Descubra qué producto de Kaspersky Next es mejor para usted con la ayuda de nuestra herramienta interactiva: https://go.kaspersky.com/Kaspersky_Next_Tool

¿Cuáles son los beneficios empresariales?

Para combatir ciberamenazas cada vez más sofisticadas, las organizaciones necesitan más que un conjunto unificado de herramientas de seguridad del mismo proveedor.

- Ante una falta global de expertos en seguridad de la información, XDR proporciona una protección holística para una infraestructura de TI en cambio y expansión frente a un entorno de ciberamenazas que evoluciona rápidamente.
- Al automatizar las tareas de rutina, XDR reduce el esfuerzo manual y los tiempos de respuesta, simplifica el trabajo de los recursos valiosos y escasos, como los especialistas en TI, y los libera para que se ocupen de lidiar con incidentes complejos.
- Al posibilitar el análisis de telemetría y de comportamiento en tiempo real a través de varias capas de seguridad, 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.
- XDR ayuda a minimizar el tiempo medio de detección (MTTD) y el tiempo medio de respuesta (MTTR) (fundamentales al combatir amenazas complejas y ataques selectivos).

Además, incluso si su organización tiene recursos expertos limitados, XDR puede protegerla frente a ataques complejos a través de una serie de capacidades como las siguientes:

- Una mayor automatización de procesos.
- El uso de una consola individual y unificada.
- Playbooks y automatización que permiten una interacción estrecha entre las herramientas de seguridad de TI como parte de XDR y escenarios conjuntos.
- Un único entorno de lago de datos.
- Enriquecimiento integrado con datos de https://go.kaspersky.com/Kaspersky_Next_Tool inteligencia de amenazas relevante.
- Menos falsos positivos y un impacto minimizado por parte de amenazas reales.

¿Cómo puede ayudar Kaspersky Next XDR Expert?

Lo que hace

La plataforma completa de XDR abierta se integra sin problemas con la infraestructura, las herramientas y las aplicaciones existentes.

Ofrece visibilidad en tiempo real y un análisis profundo de las ciberamenazas en evolución con el fin de proporcionar una detección avanzada de amenazas junto con respuestas automatizadas de forma oportuna

Funcionamiento

Detecta amenazas complejas a través de la correlación cruzada de varios orígenes de datos

Incluye una funcionalidad de EDR potente con capacidades avanzadas de detección y respuesta

Permite la búsqueda proactiva de amenazas para descubrir ataques complejos ocultos

Valor comercial

El enfoque del ecosistema, junto con un diseño abierto, 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 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?

Organizaciones con recursos de seguridad significativos que desean una plataforma única que ofrezca lo siguiente:

- Una imagen coherente de lo que ocurre en toda la infraestructura protegida
- Búsqueda de amenazas e inteligencia de amenazas integradas
- Mejor clasificación de incidentes y reducción de falsos positivos.

¿Qué obtiene?

Protección de endpoints

Antivirus web, de archivos y de correo, protección de red, detección de comportamiento, corrección, prevención de exploits, HIPS, AMSI, protección contra cifradores, prevención de ataques BadUSB

Gestión de la seguridad

Controles web, de aplicaciones, de dispositivos y de firewall, control de anomalías adaptable, Cloud Discovery y Cloud Blocking, monitor de integridad de archivos, inspección de registros, monitor de integridad del sistema

Protección y administración de dispositivos móviles

Protección, controles y administración, MDM (administración de dispositivos móviles) iOS

Escenarios TI

Evaluación de vulnerabilidades, administración de parches, eliminación de datos, inventario de software/hardware, instalación de sistemas operativos y aplicaciones de terceros, conexión remota

Cifrado

Cifrado y administración del cifrado

Capacidades de EDR

Análisis de causas raíz, análisis de IoC, respuesta automatizada y en un solo clic, guía de respuesta

Capacidades de EDR avanzadas

Recopilación de datos de telemetría, capacidades de búsqueda de amenazas, detección de Indicadores de ataque (IoA), asignación a MITRE ATT&CK

Capacidades de XDR

Unificación de alertas, entornos de pruebas, integración de AD, inteligencia de amenazas/ enriquecimiento de Kaspersky Security Network, administración de casos, playbooks automatizados y manuales, gráfico de investigación, conectores de terceros, administración de registros y lago de datos, respuesta completamente automatizada, detección de amenazas y correlación cruzada

¿Qué sucede si ya estoy usando Kaspersky?

Su solución Kaspersky	Migración recomendada	Capacidades adicionales que obtendrá
Kaspersky Endpoint Detection and Response Standard/Advanced/Expert*	Kaspersky Next XDR Expert	• Escenarios de correlación entre activos • Unificación de alertas • Flujo de trabajo de incidentes • Gráfico de investigación

* Tenga en cuenta que es posible adquirir o utilizar Kaspersky EDR Expert como una solución independiente, o actualizarla y usarla como parte de Kaspersky Next XDR Expert

Más información acerca de Kaspersky Next XDR Expert

Kaspersky Next XDR Expert

Kaspersky Next EDR Foundations — Más información

Kaspersky Next EDR Optimum — Más información

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

Noticias sobre ciberamenazas: securelist.lat
Noticias sobre seguridad TI: business.kaspersky.com
Seguridad TI para pymes: kaspersky.com/business
Seguridad TI para grandes empresas: kaspersky.com/enterprise

latam.kaspersky.com