Su empresa en crecimiento necesita una solución de seguridad ampliada, efectiva, asequible y fácil de usar.

Kaspersky Next XDR Optimum

kaspersky preparados para el futuro

Para pequeñas y medianas empresas

Exprima sus recursos al máximo y mejore la efectividad de su estrategia de respuesta ante incidentes

Kaspersky Next XDR Optimum está pensada para pequeñas y medianas empresas que cuentan con una infraestructura de TI firme y disponen de un presupuesto razonable destinado a la ciberseguridad. Ya sea que la seguridad se administre desde un equipo de TI general o un grupo pequeño específico, la solución proporciona herramientas fáciles de administrar para ofrecer una protección sólida e integral sin sobrecargar los recursos existentes.

Las ciberamenazas que afectan a las pequeñas y medianas empresas son cada vez más sofisticadas e intensas. Los atacantes se ocultan detrás de las herramientas legítimas del sistema y de técnicas avanzadas para evitar cualquier detección. Mientras tanto, los empleados, sin conocimiento de los riesgos de ciberseguridad, quedan vulnerables ante ataques de suplantación de identidad (phishing) e ingeniería social, lo que afecta a las finanzas y perjudica la reputación de la empresa.

Asimismo, la limitación en los recursos (como contar con presupuestos ajustados y la falta de personal calificado) dificulta la defensa de la empresa ante estas amenazas. Por eso, es fundamental contar con herramientas avanzadas que sean fáciles de usar y que ofrezcan el nivel de protección adecuado para su empresa.

Aumente su seguridad con Kaspersky Next XDR Optimum

Diseñada para equipos de seguridad pequeños, esta solución fortalece la respuesta ante incidentes y contribuye al conocimiento técnico sin sobrecargar al equipo con tareas rutinarias y prolongadas. Dado que muchos procesos están automatizados, su equipo podrá enfocarse en lo que más importa.

Kaspersky Next XDR Optimum se integra fácilmente en la infraestructura existente. No es necesario agregar ningún componente adicional al sistema.

Detección, análisis y respuesta

- Detección del comportamiento
- Unificación de alertas
- Cloud Sandbox
- Descubrimiento de pruebas de amenazas (IoC) e IoC personalizados
- Análisis de causa raíz
- Rango de acciones de respuesta

Características de la protección de endpoints

- Antimalware mejorado
- Mayorendurec-imiento
- Diagnósticode vulnerabilidades
- Controles para endpoints
- Protecciónde datos
- Administraciónde parches

Desde la protección excepcional de los endpoints y la seguridad en la nube hasta la automatización de las tareas de TI y las características esenciales de XDR:

Active la protección **extraordinaria de endpoints**

Evite interrupciones en las operaciones con una protección automatizada mediante herramientas antimalware y antirramsomware probadas por la industria y con tecnología de ML que evitan las infecciones producto de amenazas conocidas y desconocidas.

Corrija las vulnerabilidades con cursos de formación y el refuerzo del sistema

Reduzca la superficie de ataque y refuerce el sistema según el comportamiento de los usuarios, así ahorrará tiempo con una administración centralizada de vulnerabilidades, parches y cifrado. Además, proporcionamos toda la capacitación que su equipo necesita para aprovechar al máximo las nuevas capacidades de seguridad.

Amplíe sus capacidades de **detección y respuesta**

Obtenga información sobre las amenazas y sus movimientos dentro y fuera de los endpoints. Utilice la automatización y las respuestas guiadas para contrarrestar los ataques, y las herramientas de investigación esenciales para hacer un seguimiento de su actividad.

Capacite a todo el equipo para que participe en la seguridad

Equipe al personal de TI y a los empleados no técnicos con las habilidades y conocimientos necesarios para mantener segura a la empresa. Fortalezca al equipo de seguridad de TI mientras desarrolla una cultura sólida y consciente de la seguridad para toda la fuerza laboral de la organización.

Aproveche nuestro sistema en la nube para **procesar archivos**

Investigue los archivos maliciosos con facilidad y obtenga más contexto e información detallada gracias a la integración con Cloud Sandbox. Cargue muestras potencialmente maliciosas para verificar su reputación en un instante desde la interfaz del producto y use los datos resultantes para futuros análisis de IOC.

Controle la TI en la sombra con una solución de seguridad en la nube confiable

Supervise la TI en la sombra para minimizar riesgos y garantizar la protección de sus datos y activos digitales. Detecte qué servicios en la nube se utilizan, bloquee el acceso no autorizado e identifique qué datos confidenciales se almacenan en las aplicaciones de Microsoft 365.

Aproveche las **diversas opciones de entrega**

Reduzca el costo total de propiedad con herramientas de despliegue y automatización basadas en la nube, o instale la solución de forma local para un control total[1].

[1] La consola de administración local se basa en Linux. Kaspersky Next XDR Optimum admite todos los sistemas operativos en los agentes para endpoints y en Cloud Console. En el cuarto trimestre de 2025, estará disponible una opción de despliegue basada en la nube

Kaspersky Next XDR Optimum forma parte de la línea de productos de Kaspersky Next

Kaspersky Next es una línea de productos por niveles para todas las empresas, sin importar cuál sea su tamaño. Kaspersky Next Optimum está pensada para pequeñas y medianas empresas que cuentan con equipos de ciberseguridad básicos que desean escalar su protección sin mayores complicaciones. El primer nivel ofrece una sólida protección de endpoints, mientras que el segundo nivel cuenta con características de detección y respuesta en endpoints. Además, permite mejorar a funcionalidades esenciales de XDR o MXDR sin problemas para disfrutar de un nivel de ciberseguridad más sofisticado.

¿Por qué debería elegir Kaspersky Next Optimum?

Se creó a partir de la mejor solución para endpoints de la industria

Durante más de una década, los productos de Kaspersky ocuparon sistemáticamente los primeros puestos en pruebas y análisis independientes. Nuestra protección automatizada y probada de endpoints reduce la cantidad de alertas que los equipos de seguridad necesitan para analizar las amenazas, lo que mejora la eficiencia.

Cuenta con el respaldo de información detallada, habilidades y conocimiento experto

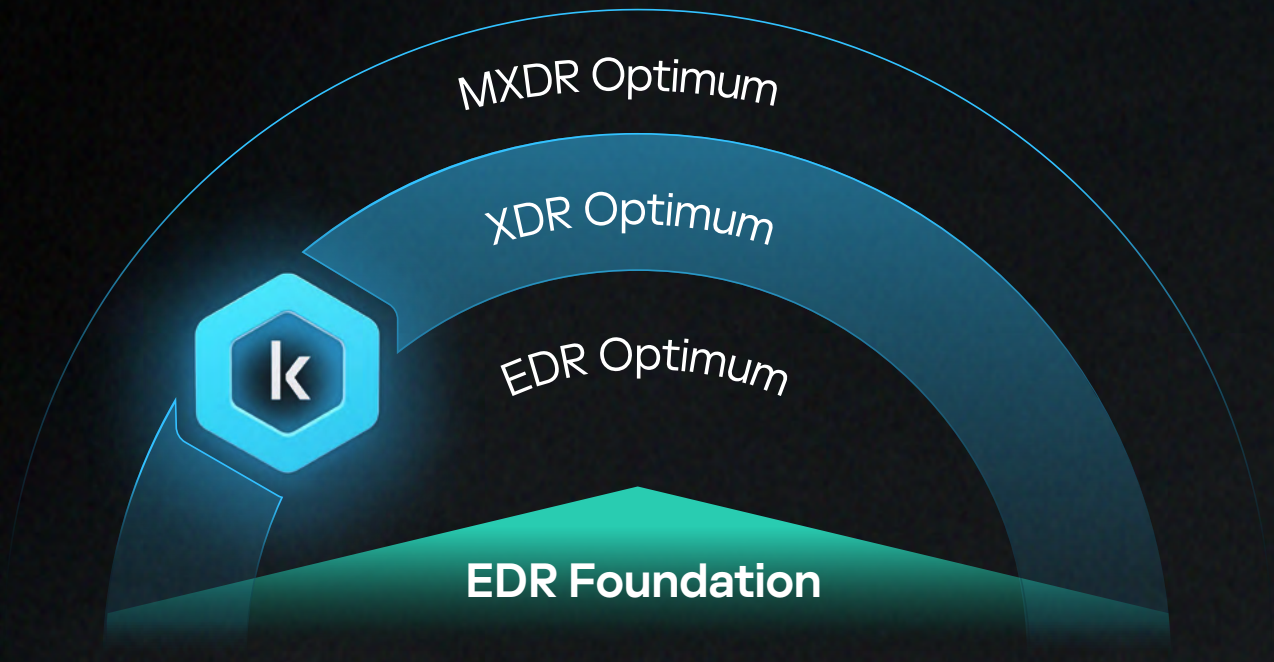
Kaspersky Next se desarrolló gracias a las décadas de experiencia acumulada y a los profundos conocimientos técnicos de nuestros equipos de seguridad internacionales. Nuestros especialistas trabajan en colaboración para hacer frente a ciberamenazas complejas, lo cual perfecciona continuamente las tecnologías que impulsan nuestros productos. Este enfoque basado en expertos garantiza que nuestras soluciones sean confiables e innovadoras y que se ajusten a las necesidades de seguridad del mundo real.

Defensa multicapa con tecnología de IA

Kaspersky utiliza algoritmos predictivos, agrupamiento, redes neuronales, modelos estadísticos y algoritmos expertos para aumentar la velocidad de detección y mejorar la precisión.

Ciberseguridad que crece con usted

Kaspersky Next protege a empresas de todos los tamaños. A medida que crecen sus necesidades, puede pasar fácilmente de la protección esencial de endpoints a las soluciones avanzadas de nivel experto disponibles en niveles superiores.



latam.kaspersky.com

© 2025 AO Kaspersky Lab.
Las marcas comerciales registradas y las marcas de servicio pertenecen a sus respectivos propietarios.

Más información

#kaspersky
#bringonthefuture