Kaspersky Next

Seguridad preparada para el futuro

¿Por qué las operaciones de seguridad son más difíciles en la actualidad?

El 41 % de las organizaciones lo atribuye al entorno de amenazas, que cambia con rapidez

El 40 % lo atribuye a la superficie de ataque en expansión[1]

Kaspersky Next une la protección robusta de endpoints, la rapidez de EDR y las capacidades avanzadas de XDR en tres niveles simples de producto. Elija las herramientas que necesita en este momento y cambie con facilidad cuando esté listo para el siguiente nivel.

¿A qué se enfrenta?

Ataques que evolucionan

El ransomware, el malware y las filtraciones de datos evolucionan de forma constante. Utilizan técnicas complejas para evitar ser detectados y penetrar en la infraestructura a través de vulnerabilidades y ataques al correo corporativo y a la cadena de suministro.

Superficie de ataque en expansión

El trabajo remoto, la transición a la nube y el trabajo sobre la marcha son asombrosos. Sin embargo, generan una gran cantidad de formas nuevas para que los hackers puedan obtener acceso, y aumentan la cantidad de aspectos que se deben supervisar.

Recursos limitados

Lanzar un ataque es más barato que nunca. Sin embargo, para protegerse se requieren recursos significativos, y es probable que sus necesidades superen su presupuesto. Esto provoca que el TCO sea más importante que nunca.

Regulaciones que se refuerzan

Los requisitos de divulgación de filtraciones de datos, RGPD, CCPA y PCI DSS representan una gran presión para los departamentos de seguridad en términos de seguridad e informes.

Complejidad creciente

Las infraestructuras de IT y ciberseguridad no suelen volverse más simples y contenidas. Estas crecen con rapidez y cada nueva herramienta agrega nuevos servidores, consolas e integraciones que se deben conocer y mantener.

¿Cómo viene, por ahora?

Debido al volumen de proyectos, tareas urgentes, innovaciones, llamadas y reuniones interminables, los especialistas en ciberseguridad tienen demasiado trabajo.
Las nuevas actualizaciones y herramientas deberían darle más tiempo, no quitárselo.

[1] SOC Modernization and the Role of XDR, Enterprise Strategy Group, 2022

kaspersky

El 51 % de las herramientas actuales tienen problemas para detectar e investigar amenazas avanzadas[1]

La ayuda está a su disposición

Kaspersky Next es la nueva línea de productos de Kaspersky que fortalece la seguridad con EDR y XDR, respaldado por una protección sólida de endpoints. Ayuda a asegurar la superficie de ataque y erradica los ataques antes de que generen daños.

Innovación en seguridad

Kaspersky Next, desarrollado a partir de la base de nuestra seguridad de endpoints galardonada, cubre todas sus necesidades básicas y lo ayuda a avanzar a EDR y XDR sin problemas, con rapidez y con recursos mínimos.

Desarrollado a partir del aprendizaje automático

Nuestros productos utilizan una variedad de tecnologías de detección, siendo el aprendizaje automático la principal. Esta tecnología detecta y neutraliza de manera efectiva incluso las amenazas más nuevas y complejas.

La solución perfecta para sus necesidades

No existe una solución universal cuando se trata de ciberseguridad. Por este motivo, Kaspersky Next ofrece tres niveles de protección, que van desde la seguridad básica de endpoints hasta el fortalecimiento de la experiencia y el equipamiento de expertos con herramientas avanzadas..

Ventajas clave

- Defienda su empresa frente a varios tipos de amenazas y evite pérdidas e interrupciones
- Elija el nivel que se adapte a mejor a sus necesidades únicas
- Migre con facilidad de un nivel al siguiente, a medida que sus necesidades de seguridad crezcan y evolucionen
- Obtenga beneficios de la funcionalidad de EDR en todos los niveles, según sus necesidades y recursos
- Controle la infraestructura completa con una XDR abierta e integral
- Obtenga una protección inigualable de endpoints basada en el aprendizaje automático de cada nivel nivel
- Administre su seguridad desde la nube o las instalaciones
- Ahorre tiempo para dedicar a otros proyectos importantes, gracias a las funciones de automatización de las tareas de rutina de ciberseguridad

Estructura de protección

Kaspersky Next ofrece tres niveles, en función de sus necesidades más esenciales de ciberseguridad. A medida que sus necesidades crezcan, será fácil cambiar de uno a otro y actualizar la función de seguridad rápidamente.

Kaspersky Next

Kaspersky Next EDR Foundations

Uso recomendado
El equipo de TI se encarga de la seguridad

Valor
Asegure la protección de todos sus endpoints

Características clave:
- Protección de endpoints
- Análisis de causa raíz
- Administración de la seguridad y la TI

Kaspersky Next EDR Optimum

Uso recomendado
Equipo pequeño de ciberseguridad

Valor
Impulse la seguridad con una investigación y respuesta optimizadas

Características clave:
- Protección avanzada de endpoints
- Protección de nube
- Orientación y automatización de EDR

Kaspersky Next XDR Expert

Uso recomendado
Equipo grande de ciberseguridad o SOC

Valor
Herramienta profesional principal para los expertos en seguridad

Características clave:
- EDR con todas las funciones
- Acumulación de alertas y flujos de trabajo de IRP
- Aprendizaje automático y detección avanzada

[1] SOC Modernization and the Role of XDR, Enterprise Strategy Group, 2022

El 69 % de los ataques duraron solo 2 días, en promedio[1]

Casos de uso

Kaspersky Next resuelve los problemas críticos de ciberseguridad.

Kaspersky Next EDR Foundations

Kaspersky Next EDR Optimum

Kaspersky Next XDR Expert

Proteja sus endpoints

Protéjase de forma automática contra el malware, el ransomware y otras amenazas masivas con nuestro motor de protección de endpoints galardonado.

Responda rápidamente

Reaccione a las nuevas amenazas evasivas con un solo clic o cree fácilmente una tarea de automatización para ataques recurrentes. El tiempo de respuesta es una de las métricas clave de una seguridad efectiva.

Enfrente amenazas complejas

Cuando su empresa es el objetivo de un ataque complejo o avanzado, es necesario equipar a los expertos con la información y las herramientas más avanzadas disponibles. La acumulación, el análisis de datos y la detección avanzada son claves.

Obtenga visibilidad

Investigue amenazas con el análisis de causa raíz y determine su alcance con rapidez. No siga especulando; conozca las amenazas.

Desarrolle su experiencia

No todas las personas necesitan tener una EDR compleja y avanzada desde el primer momento, pero con algo se debe empezar. La visibilidad, el análisis y la respuesta en un único paquete lo ayudan en su recorrido de EDR/XDR.

Seguridad entre activos

La correlación entre activos de datos de varias fuentes, la integración con productos de terceros y la automatización de tareas de rutina les permite a los expertos buscar amenazas y responder a ellas de manera precisa, rápida y sistemática.

Reduzca la superficie de ataque

Implemente el control de dispositivos, aplicaciones y acceso web, además de asegurar los dispositivos móviles, para reducir la cantidad de formas en que los atacantes pueden ingresar a sus sistemas.

Seguridad en la nube

Descubra, restrinja y bloquee el acceso a recursos no autorizados en la nube, en los servicios de mensajería instantánea y demás. Obtenga visibilidad y control de MS SharePoint Online, OneDrive y Teams.

Playbooks

La automatización y la organización con varios manuales preestablecidos reduce el tiempo promedio de respuesta y detiene incluso las amenazas avanzadas antes de que se desarrollen.

[1] Incident Response Analyst Report, Kaspersky, 2022

¿Qué se incluye?

Observe las funciones clave específicas en cada nivel.

	Kaspersky Next EDR Foundations	Kaspersky Next EDR Optimum	Kaspersky Next XDR Expert
Protección de endpoints Antivirus para archivos, la Web y correos, protección de red, AMSI, prevención de exploits, corrección, detección de comportamiento, HIPS	✓	✓	✓
Gestión de la seguridad Firewall; controles de aplicaciones, dispositivos y la Web; administración y protección de dispositivos móviles	✓	✓	✓
Escenarios de IT Evaluación de vulnerabilidades, administración de parches, eliminación de datos, inventario de SW/HW, instalación de sistemas operativos y aplicaciones de terceros, conexión remota	✓[1]	✓	✓
Cifrado Cifrado y administración del cifrado		✓	✓
Seguridad en la nube Descubrimiento y bloqueo en la nube, seguridad para MS Office 365, descubrimiento de datos	✓[2]	✓	✓
Educación Capacitación en ciberseguridad para administradores de IT		✓	✓
Capacidades de EDR esencial Análisis de causa raíz, análisis de IoC, respuesta de endpoints	✓[3]	✓	✓
Capacidades de EDR avanzadas Telemetría de recopilación, búsqueda de amenazas, detección de Indicadores de ataque (IoA), asignación a MITRE ATT&CK			✓
Capacidades de XDR Acumulación de alertas, entorno de pruebas, integración AD, enriquecimiento de IT, conectores de terceros, herramientas mejoradas de investigación, administración de registros y lago de datos, respuesta completamente automatizada, manuales, detección de amenazas y correlación cruzada			✓
Consola de administración Disponible en la nube o en las instalaciones en dos vistas:	**Vista pro** Cantidad máxima de usuarios, optimizada y fácil de administrar: 2500	**Cloud**	**Cloud**	**No aplica**
	Vista de expertos Cantidad mínima de usuarios, granular y personalizable para la nube: 300	**En la nube y en las instalaciones**	**En la nube y en las instalaciones**	**En las instalaciones**

Consulte la Lista de funciones de productos correspondiente para conocer la disponibilidad de funciones específicas en el tipo de consola de su elección.

[1] Funciones disponibles: evaluación de vulnerabilidades, inventario de SW/HW

[2] Funciones disponibles: Cloud Discovery

[3] Funciones disponibles: análisis de causas raíz

El 43 % de las organizaciones mencionan el costo de asegurar entornos tecnológicos cada vez más complejos como parte de los desafíos clave de la seguridad de IT[1]

Lleve la seguridad al siguiente nivel

La experiencia externa o los servicios adicionales pueden ayudarlo a llevar la seguridad al siguiente nivel.

Los siguientes son algunos de los servicios que recomendamos para mejorar aún más la experiencia con Kaspersky Next.

Considere la seguridad administrada

Kaspersky Managed Detection and Response

- Protección administrada sin interrupciones frente a las amenazas evasivas
- Flexibilidad para adaptarse a todas las necesidades de cualquier organización o sector
- Inversión en seguridad de IT rentable y justificada

Deje de perder tiempo

Kaspersky Professional Services

- Evite las configuraciones erróneas y minimice el impacto en la implementación
- Olvídese de las evaluaciones, la implementación, el mantenimiento y la optimización, según sea adecuado
- Obtenga ayuda con las actualizaciones y la migración de productos de Kaspersky
- Paquetes de servicio básicos o proyectos personalizados

Reciba asistencia de expertos

Kaspersky Premium Support

- Maximice su ROI y evite la sobrecarga de capacidades
- Línea telefónica directa con soporte especializado
- Expertos técnicos especializados de Kaspersky
- Horario extendido para problemas críticos

¿Cuál es el siguiente paso?

Lo que ofrece cada nivel de Kaspersky Next:

Kaspersky Next EDR Foundations

Es la forma más directa de generar una base sólida para la ciberseguridad.

- Protección avanzada de endpoints basada en aprendizaje automático
- Remediación automática
- Múltiples funciones de automatización
- Controles de seguridad flexibles
- Herramientas de análisis de causas raíz de EDR

Más información

Kaspersky Next EDR Optimum

Mejore las defensas y la experiencia frente a las amenazas evasivas.

- La funcionalidad de Essential EDR ofrece visibilidad, análisis y respuesta
- Una protección sólida de endpoints
- Controles mejorados, administración de parches y seguridad en la nube
- Formación en ciberseguridad para personal de IT

Más información

Kaspersky Next XDR Expert

Proteja su empresa contra las amenazas más complejas y avanzadas.

- Se integra a la perfección con su infraestructura de seguridad existente
- Visibilidad en tiempo real y análisis exhaustivo de las amenazas
- Detección de amenazas avanzadas
- Correlación entre activos
- Respuesta automatizada

Más información

[1] IT Security Economics 2022, Kaspersky, 2022

¿Quiénes somos?

Kaspersky es una empresa global de ciberseguridad con más de 250 000 clientes corporativos en todo el mundo. Desarrollamos herramientas y ofrecemos servicios para mantener a nuestros clientes protegidos desde hace más de 25 años, con las tecnologías más probadas y galardonadas. Estamos comprometidos con la transparencia y la independencia.

IDC

Evaluación global de proveedores IDC MarketScape sobre seguridad moderna en endpoints para empresas y pymes 2021

Actor principal

AV-Test

Protección avanzada de endpoints: Evaluación de seguridad contra el ransomware

Protección del 100 %

Radicati Group

Cuadrante de mercado sobre amenazas persistentes avanzadas (APT)

Top player

Info-Tech

Champion for Endpoint Protection in 2023

G2

Best estimated ROI for Enterprise in the fall of 2023