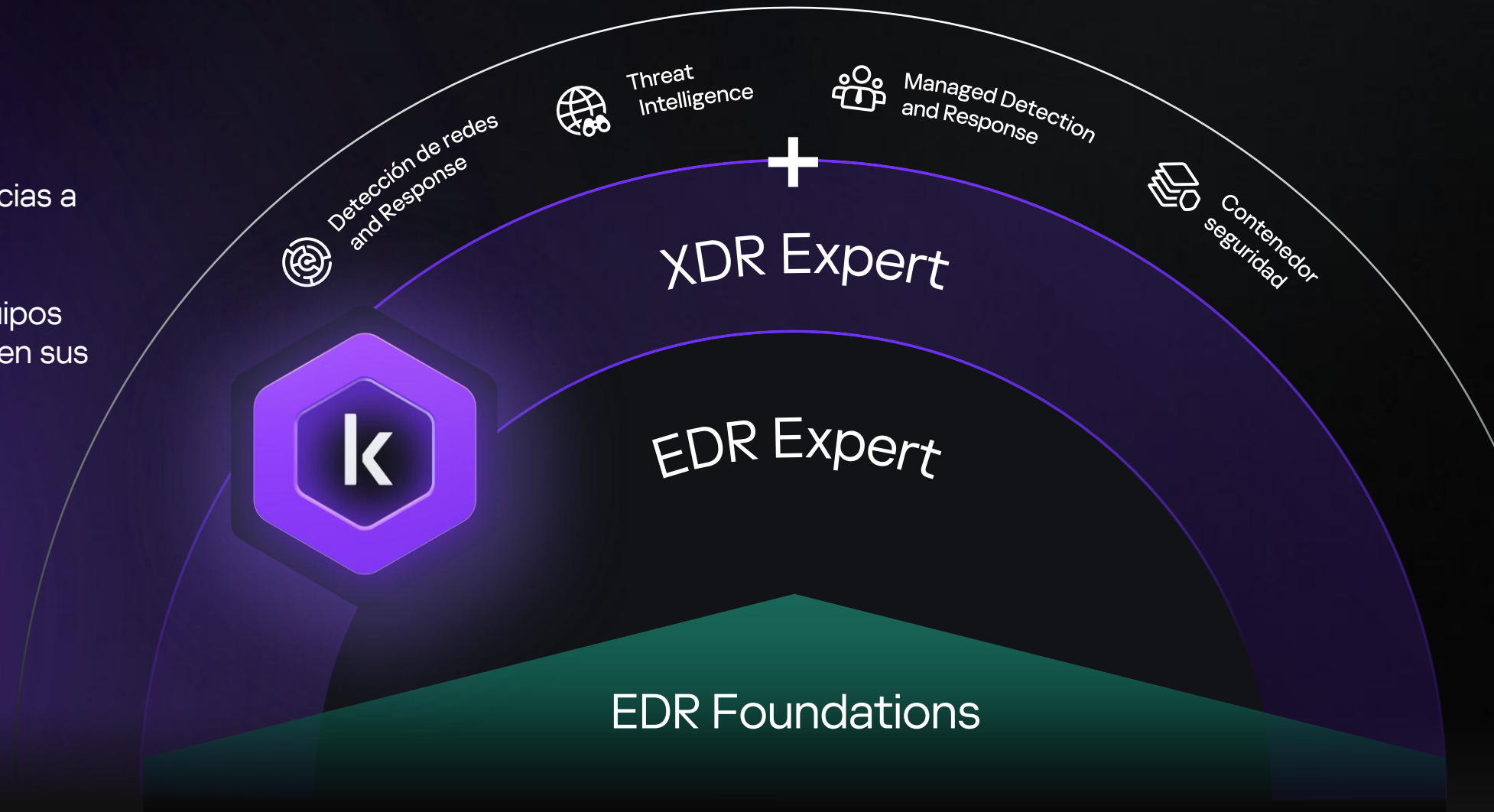
Soluciones expertas

Kaspersky Next Expert

Para empresas de todos los tamaños

Identifique rápidamente, responda con precisión e investigue las amenazas avanzadas con rapidez gracias a las herramientas de última generación basadas en IA, diseñadas para que los equipos de ciberseguridad maximicen sus operaciones



Comparación de características

Kaspersky Next EDR Foundations

Protección interna **básica**

Kaspersky Next EDR Expert

Protección interna **avanzada**

Kaspersky Next XDR Expert

Protección interna **ampliada**

- Protección automatizada frente a amenazas masivas
- Cloud discovery
- Diagnóstico de vulnerabilidades; inventario de hardware y software; controles web, de aplicaciones y de dispositivos; MDM; resolución remota de problemas; instalación de SO y aplicaciones de terceros

- Bloqueo de nubes, detección de datos y seguridad para Microsoft Office 365
- Detección y respuesta en los endpoints ante amenazas complejas y persistentes
- Administración de parches, borrado remoto, administración del cifrado y administración de movilidad segura (MTM+EMM integrados), capacitación en ciberseguridad para administradores de TI
- Espacio aislado avanzado integrado, gestión de servicios, análisis forense (solo Windows)

- Seguridad para el correo electrónico, seguridad para nubes híbridas, 100 solicitudes de Kaspersky Threat Lookup
- Detección y respuesta ampliadas completas; motor de correlación cruzada para la recopilación, normalización, supervisión y correlación de datos
- Automated Security Awareness Platform

Tecnologías disponibles bajo demanda para mayor protección

- Detección y respuesta en redes
- Inteligencia de amenazas
- Managed Detection and Response
- Seguridad de los contenedores

Kaspersky Next EDR Foundations

Página del producto

Para pequeñas y medianas empresas

EPP potentes basadas en ML, controles de seguridad flexibles y herramientas de análisis de causa raíz EDR que le proporcionan la forma más simple de construir una base sólida para su ciberseguridad.

Una consola simple, opciones de despliegue flexibles (en la nube o en una instalación local) y funciones diseñadas para mejorar los flujos de trabajo cotidianos contribuyen a reducir la complejidad y aumentar la eficacia.

¿Cómo podemos ayudar?

Detectamos y erradicamos los ataques avanzados y proporcionamos una ruta visual de las amenazas con un análisis de causa raíz

Le enviamos alertas de actividades sospechosas o brechas de seguridad con Cloud Discovery y diagnóstico de vulnerabilidades

Proteja sus datos con las herramientas antirransomware y antimalware probadas del sector

Asegúrese de que sus aplicaciones estén siempre actualizadas con el análisis automático de vulnerabilidades

¿Por qué Kaspersky?

>1500

Primeros y terceros puestos gracias a nuestras tecnologías de prevención y detección

Más de 21.000

Clientes activos de diferentes sectores en todo el mundo

¿Por qué nos diferenciamos de la competencia?

Administración in situ sin depender de redes externas

Control e inventario de aplicaciones para reducir la superficie de ataque

Tecnologías de cifrado y prevención de ataques BadUSB

Política para trabajo fuera de la oficina para gestionar la protección fuera de la red corporativa

¿Cómo funciona?

Kaspersky Next EDR Foundations

1 Prevención de la exposición

- Filtrado de red
- Filtrado de contenido vía nube
- Firewall

2 Antes de la ejecución

- Fortalecimiento de endpoints
- Servicios de reputación
- Detección estática basada en IA/ML

3 Control de tiempo de ejecución

- Análisis de comportamiento

Prevención de exploits | Protección contra ransomware | Detección dinámica

- Control de privilegios de ejecución

4 Respuesta e investigación automatizadas

- Reversión automatizada
- Desinfección avanzada
- Análisis forense
- Análisis de causas raíz

+

Detección precisa

Inteligencia en tiempo real desde la nube (KSN)

Actualización basada en IA/ML

Kaspersky Next EDR Expert

Página del producto

Tecnologías

Una potente solución de Endpoint Detection and Response que trabaja en conjunto con una plataforma de protección de endpoints para bloquear ataques masivos y detectar ciberamenazas más complejas, lo cual ayuda a investigar incidentes de forma proactiva y equipa a los especialistas de TI con herramientas de respuesta integrales.

¿Cómo podemos ayudar?

Reduzca la complejidad y mejore la calidad y velocidad del análisis de amenazas con una única consola de gestión para la prevención, detección, investigación y respuesta.

Escale con confianza sin que el negocio pierda el ritmo para mantenerlo protegido frente a las ciberamenazas en evolución que pueden interrumpir las operaciones, mermar los ingresos y dañar la confianza en la marca.

Permita una detección y respuesta más rápidas e inteligentes con análisis IoA/IoC avanzado, inteligencia de amenazas integrada, potente búsqueda de amenazas y administración de incidentes agilizada.

Aligere la carga de los equipos pequeños de analistas con herramientas mejoradas con IA, mapeo MITRE, alto contenido integrado y automatización avanzada.

¿Por qué Kaspersky?

Más de 1.900

reglas de detección creadas por el equipo líder del SOC de Kaspersky

Más de 2,5 millones

de endpoints protegidos en el mundo

>490

técnicas de la matriz MITRE ATT&CK cubiertas

¿En qué nos diferenciamos de la competencia?

Potenciado por la mejor protección de endpoints de su clase

Respaldado por detectores de amenazas y SOC de élite

Integraciones amplias y arquitectura abierta

Entorno aislado avanzado e integrado

Más de 600 clientes de todo el mundo confían en nosotros

Arquitectura

Kaspersky Next
EDR Expert



Página del producto

Tecnologías

Kaspersky Next XDR Expert

Esta solución representa el nivel más avanzado de la línea Kaspersky Next. Proporciona a su equipo de seguridad o SOC un control completo sobre la infraestructura protegida, con visibilidad total, correlación en tiempo real y automatización. Todo ello mediante una amplia variedad de herramientas de respuesta y fuentes de datos — endpoints, redes y nubes.

¿Cómo podemos ayudar?

Ofrecemos herramientas de prevención eficaces y probadas para reducir la cantidad de alertas que los equipos de ciberseguridad tienen que analizar para aumentar su eficiencia.

Ayudamos a establecer procesos de respuesta para mejorar el MTTR y minimizar los errores en escenarios frecuentes mediante el aprovechamiento de playbooks y la coordinación de flujos de trabajo colaborativos.

Proporcionamos una visión integral de la infraestructura protegida. Recopilación y almacenamiento de todos los datos necesarios para la detección de APT, junto con la visualización de todas las fases de la investigación de amenazas.

¿Por qué Kaspersky?

>300

integraciones predefinidas e interoperabilidad nativa profunda entre las tecnologías de Kaspersky

>2,700

reglas de detección preconfiguradas mantenidas por el SOC de Kaspersky, asignadas a MITRE ATT&CK y respaldadas con directrices de respuesta

¿En qué nos diferenciamos de la competencia?

- Productos potenciados por la mejor protección de endpoints de su clase
- Experiencia integrada en SOC
- Integraciones amplias y arquitectura abierta
- Detección de amenazas basada en IA

Líder reconocido

ISG Provider Lens™ - Ciberseguridad - Servicios y soluciones 2025 Brasil

SPARK Matrix™: Detección y respuesta ampliadas (XDR), tercer trimestre de 2025

¿Cómo funciona?

Fuentes de datos

- Soluciones de Kaspersky
- Terceros

xFlows

Eventos

Integraciones

- **Kaspersky Anti Targeted Attack** (NDR Enhanced)
- **Kaspersky Threat Intelligence**
- **Kaspersky Managed Detection and Response**

... y, a pedido, más integraciones con soluciones de Kaspersky o de terceros

Datos

Respuesta

Open Single Management Platform

- Endpoint Detection and Response
- Gráfico de investigación
- Gestión de registros y lago de datos
- Detección de amenazas y correlación cruzada
- Playbooks
- Paneles e informes
- Gestión de activos centralizadas
- Gestión de casos
- Conjunto de herramientas de implementación
- Conectores para soluciones de terceros

Datos

Respuesta

Concienciación sobre seguridad, entorno de pruebas, seguridad del correo electrónico y de la nube híbrida

- **Kaspersky Automated Security Awareness Platform**
- **Kaspersky Hybrid Cloud Security**
- **Kaspersky Security for Mail Server**
- **Kaspersky Sandbox**

XDR

Beneficios de un ecosistema unificado

Integraciones sencillas

Disfrute de una funcionalidad XDR completa mientras conserva la opción de integrar soluciones de seguridad de terceros. Además, nuestras tecnologías bajo demanda facilitan la integración sin esfuerzo de otras soluciones de Kaspersky, lo que mejora su postura de seguridad.

Eficiencia de costos

Ahorre al cubrir las principales prestaciones de XDR con un único proveedor y tenga la opción de integrar las soluciones de terceros en la API. Armar una solución XDR desde cero involucrando a varios proveedores es más costoso.

Consolidación

Ahorre tiempo y recursos aprovechando una consola centralizada que le proporciona al equipo de su SOC una visibilidad completa de la infraestructura protegida. Nuestra plataforma XDR todo en uno también mejora la experiencia del usuario y elimina la necesidad de gestionar varias herramientas y sistemas aislados.

Propuesta experta para grandes empresas

La disponibilidad de las funciones puede variar según el método de implementación y la licencia elegida

Kaspersky Next EDR Foundations

Protección automatizada frente a amenazas masivas
- Antimalware SEP multicapa
- Detección del comportamiento
- Prevención de exploits
- Motor de remediación
- Protección frente a amenazas en la red, en la web, de archivos y de correos electrónicos en el nivel de los endpoints
- Firewall
- Prevención de intrusiones en el host (HIPS)
- Protección AMSI
- Prevención de ataques BadUSB
- Análisis de causas raíz con una tarjeta de alerta
- Inteligencia de amenazas global a través de Kaspersky Security Network
- Defensa contra amenazas móviles

Reforzamiento del sistema
- Evaluación de vulnerabilidades
- Inventarios de hardware y software
- Controles web, de aplicaciones y de dispositivos
- Administración de dispositivos móviles (MDM)
- Resolución de problemas remota
- Instalación de SO y aplicaciones de terceros

Seguridad para nubes
- Cloud discovery

+

Kaspersky Next EDR Expert

Protección avanzada de endpoints, detección y respuesta a amenazas complejas y persistentes
- Recopilación de telemetría de endpoints
- Búsqueda proactiva de amenazas y análisis retrospectivos
- Detección avanzada con indicadores de ataque (IoA)
- Reglas YARA
- Mapeo a MITRE ATT&CK
- Administración de parches
- Borrado remoto
- Administración del cifrado
- Administración de movilidad segura (MTM+EMM integrados)

Entorno de pruebas avanzado e integrado
- Evaluación multinivel y análisis del comportamiento de objetos emulados
- Gestión de plantillas de máquinas virtuales
- Interfaz de red especial integrada para supervisar interacciones entre objetos malintencionados y recursos de Internet
- Simulación de las acciones de usuarios convencionales
- Contrarresta eficazmente las técnicas modernas de evasión de espacios aislados utilizadas por el malware

Administración de servicios (solo Windows)
- Inicio, detención, eliminación, pausa o reanudación de servicios
- Modificación del tipo de servicio de inicio

Análisis forense
- Listas de procesos, archivos y objetos con ejecución automática
- Volcado de memoria de procesos
- Volcado de memoria
- Imagen de disco
- Archivos de servicio de NTFS
- Clave del Registro

Funciones adicionales
- Cloud Blocking
- Data Discovery
- Seguridad para Microsoft Office 365: Exchange, OneDrive, SharePoint, Teams
- Detección de secuestro de DLL mediante IA
- Detección de robo de cuentas con IA
- Resumen de incidentes impulsado por IA
- Asistente de GenAI del analista del SOC

Enriquecimiento con inteligencia de amenazas
- 100 solicitudes de Kaspersky Threat Lookup

+

Kaspersky Next XDR Expert

Seguridad para el correo electrónico
- Detección de malware, spam y phishing basada en ML
- Distintas opciones de implementación (SEG, nube, independiente)
- Filtrado de contenido
- Autenticación de remitentes de correo electrónico mediante SPF, DKIM y DMARC
- Funcionalidades de integración
- Exportación de datos a SIEM ampliada
- Análisis de archivos adjuntos mediante la integración nativa con el espacio aislado de red de KATA

Seguridad para nubes híbridas
- Control de integridad del sistema
- Inspección de registros
- Compatibilidad con nubes privadas (VMware, Red Hat Enterprise Linux, KVM)
- Compatibilidad con nubes públicas: Google Cloud, Microsoft Azure, AWS

Automated Security Awareness Platform
- Formación flexible en concientización sobre seguridad para el personal
- Cursos personalizables, disponibles en 25 idiomas
- Paneles e informes de concientización de seguridad
- Campañas de phishing simuladas
- Formación en formatos de audio y video
- Respuestas de Automated Security Awareness Platform desde la tarjeta de alerta

Detección y respuesta extendidas ante amenazas complejas y persistentes
- Gráfico de investigación con modo de línea de tiempo
- Respuesta a incidentes y gestión flexible de casos con SLA
- Manuales: orquestación y automatización de respuestas
- Kit de herramientas de despliegue y API abierta
- Editor visual de playbooks

Motor de correlación cruzada para la recopilación, normalización, supervisión y análisis de datos
- >300 conectores para soluciones de terceros
- Paneles e informes
- Gestión de registros con lago de datos
- Detección avanzada de amenazas y correlación cruzada
- Agregación de alertas y gestión de activos
- Ingesta de datos y respuesta para Active Directory
- Puntuación del riesgo de los activos mediante IA
- Gráfico de dependencias de recursos

Tecnologías disponibles bajo demanda para mayor protección



Con Kaspersky Next XDR Expert, puede adaptar la seguridad a las necesidades de su empresa agregando tecnologías, reforzando su postura y mejorando la experiencia del usuario. Todo ello sin gastar en exceso ni depender de múltiples proveedores para cubrir diferentes dominios, mejorar la respuesta ante incidentes y enriquecer los datos con inteligencia de amenazas.