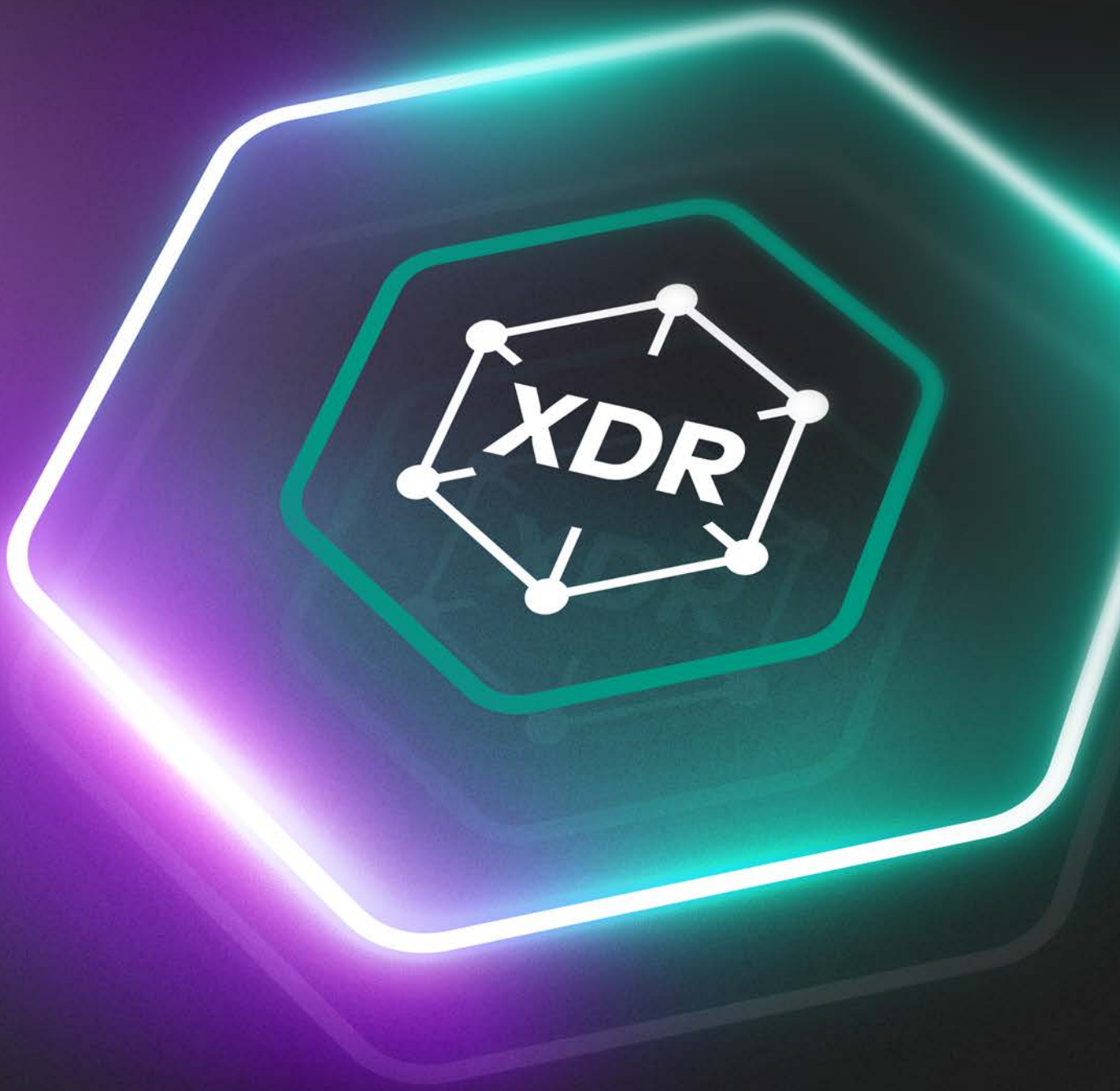


Visibilidad inigualable.
Protección integral.

Kaspersky Extended Detection and Response

kaspersky BRING ON THE FUTURE

La complejidad de la ciberseguridad de las empresas

El panorama de las ciberamenazas hace que sea extremadamente desafiante para las organizaciones estar al día con su ciberseguridad mientras se enfocan en las operaciones principales de la empresa. Si agregamos una superficie de ataque en constante expansión, requisitos regulatorios y un déficit mundial de competencias a este panorama, es fácil ver por qué las empresas modernas están bajo tanta presión y por qué tienen éxito tantos ciberataques.

51%

de las empresas tienen dificultades para detectar e investigar amenazas avanzadas con las herramientas actuales

68%

de las empresas experimentó un ataque dirigido en sus redes y sufrió la pérdida de datos como resultado directo

$6 billones

por año: el costo anual global de la ciberdelincuencia

400000

elementos de malware nuevos se detectan todos los días

Fuentes: Kaspersky, PurpleSec, CybersecurityVentures

Kaspersky Extended Detection and Response

Visibilidad completa. Protección inigualable.

Kaspersky XDR es una solución de ciberseguridad sólida que ofrece protección frente a ciberamenazas sofisticadas. Proporciona visibilidad, correlación y automatización completas al utilizar una amplia gama de fuentes de datos, incluidos datos de endpoints, redes y la nube.

Ha evolucionado desde la plataforma Kaspersky Anti-Targeted Attack como una solución XDR nativa en 2016 hasta convertirse en una plataforma XDR abierta en 2023. Desde entonces, esta solución proporciona una visión integral de la seguridad y se gestiona fácilmente a través de la Plataforma de Administración Única Abierta. Además, ofrece una seguridad completa en las instalaciones, garantizando que los datos confidenciales de los clientes permanezcan en su propia infraestructura y cumpliendo con los requisitos de soberanía de datos.

XDR abierta

Las soluciones de XDR abierta están diseñadas para funcionar con una amplia variedad de productos de seguridad, lo que les permite a las organizaciones integrar productos de seguridad de diferentes proveedores y ofrecer mayor flexibilidad y capacidades independientes de proveedores.

XDR nativa

Las soluciones de XDR nativa suelen funcionar sin problemas con el propio ecosistema de herramientas de seguridad del proveedor, lo que permite brindar una experiencia más unificada e integral. Estas soluciones están diseñadas para trabajar en conjunto y ofrecen integración profunda, automatización y flujos de trabajo simplificados dentro del conjunto de productos de seguridad del proveedor.

Tecnologías clave

Ofrecemos XDR abierta como una herramienta única y universal que permite crear un sistema unificado de productos de ciberseguridad. En el centro de Kaspersky XDR se encuentran nuestras soluciones líderes: Kaspersky Unified Monitoring and Analysis Platform, Kaspersky Endpoint Security for Business y Kaspersky Endpoint Detection and Response. KATA es una opción adicional para la gestión avanzada de redes.

Supervisión y análisis

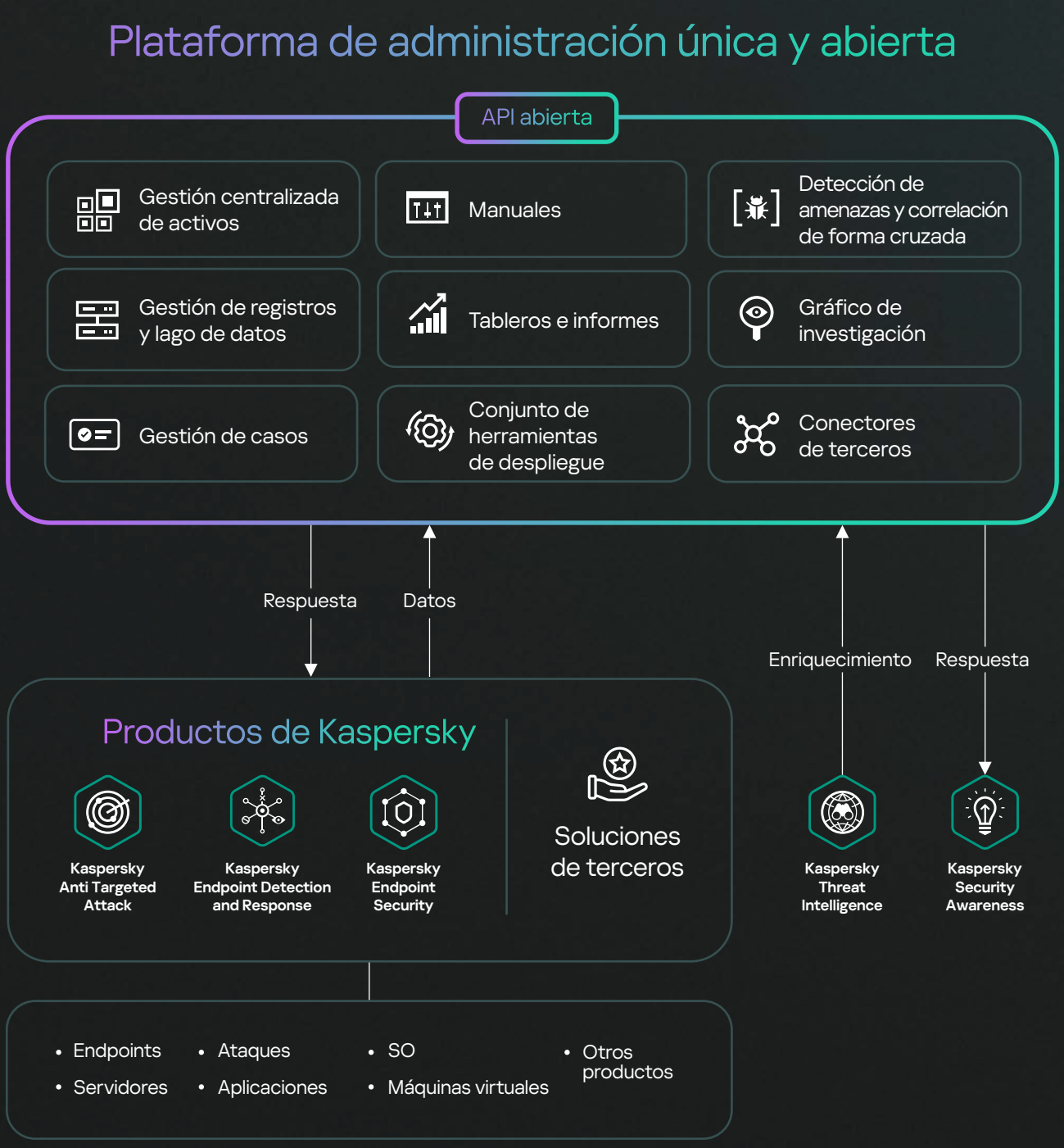
Proporciona recopilación y análisis centralizados de registros, correlación de eventos de seguridad en tiempo real y notificación oportuna de incidentes. Además, incluye un conjunto preparado de reglas y acceso a la amplia cartera de servicios de Kaspersky Threat Intelligence, priorizando amenazas, ataques e indicadores de compromiso.

Protección de endpoints

Proporciona una sólida seguridad para dispositivos finales, protegiéndolos contra ransomware, malware y ataques sin archivos. Nuestra protección, ya sea local o en la nube, utiliza aprendizaje automático y análisis de comportamiento para asegurar todos los tipos de dispositivos que ejecutan cualquier sistema operativo.

Detección y respuesta en endpoints

Proporciona una visibilidad integral y defensas superiores en todos los endpoints de una organización. La mejora en la búsqueda y detección de amenazas se logra gracias a la exhaustiva inteligencia de amenazas exclusiva de Kaspersky. Además, la automatización de tareas rutinarias, los procesos de investigación guiada y las detecciones personalizables fomentan una rápida resolución de incidentes.



Características poderosas

Fusión de datos de terceros en tiempo real

La capacidad de integrar datos de fuentes externas va más allá de los endpoints y está potenciada gracias a la correlación cruzada en tiempo real.

Respuesta y corrección automatizadas

Aísle o coloque en cuarentena endpoints en riesgo, bloquee actividades maliciosas y solucione vulnerabilidades para reducir el esfuerzo manual y el tiempo de respuesta.

La mejor EPP/EDR

Kaspersky es reconocido como el líder global y referente de las soluciones de EPP/EDR en todo el mundo. Kaspersky EDR sobresale a escala global, respaldada por premios y la participación activa en comités internacionales como Interpol y MAPP.

Escalabilidad sin precedentes

Kaspersky XDR, que tiene la capacidad de soportar cargas de cientos de miles de endpoints en una sola instancia, supervisa las amenazas en tiempo real y de forma diligente, mientras garantiza una alta disponibilidad.

Soberanía de datos

Kaspersky XDR destaca como uno de los pocos proveedores que proporciona una solución XDR completa y local, asegurando que los datos confidenciales de los clientes permanezcan dentro de su propia infraestructura, al mismo tiempo que se cumplen los requisitos de soberanía de datos.

Integración fluida y firme entre los productos de Kaspersky

La interacción entre nuestros productos va más allá de lo que ofrecen las soluciones externas, lo que nos permite proporcionar un sistema de soporte unificado y un diseño completamente integrado.

Funcionalidad de tenencia múltiple que proporciona escenarios de MSSP

Proporcione XDR como servicio con inquilinos de pleno derecho. Los usuarios de un inquilino no pueden ver los datos de otros inquilinos, mientras que el administrador principal (el MSSP) puede desarrollar procesos de detección y respuesta para todos los clientes.

Personalización de escenarios de seguridad avanzada y análisis de datos en toda la infraestructura

Los usuarios pueden configurar escenarios de seguridad complejos con la capacidad agregada para analizar datos en toda la infraestructura.

Capacidades de integración

La amplia gama de integraciones que funcionan con Kaspersky XDR brinda una vista contextualizada y unificada de amenazas potenciales, lo que le proporciona a su equipo de seguridad todas las herramientas e información que necesitan para proteger la organización de los ataques de ciberdelincuentes.

Las capacidades de integración del producto incluyen la recepción de datos (registros) de otros sistemas y dispositivos, así como la configuración de respuestas automatizadas en otros productos. Kaspersky XDR viene con una amplia variedad de integraciones listas para usarse con Kaspersky y otros productos de terceros. Además, es posible agregar integraciones adicionales que pueden ser desarrolladas por Kaspersky Professional Services, por partners o por los propios clientes (incluso se pueden usar las capacidades de API de productos conectables). La integración es posible con sistemas de diferentes dominios y proveedores, y se admiten diversos protocolos y formatos de datos.

Por dominio de seguridad

Endpoint Security

- Soluciones de EPP y EDR

Seguridad de red, Internet y correo electrónico

- Protección de correos electrónicos
- Detección y respuesta de red (NDR)
- Firewalls (FW) y firewalls de última generación (NGFW)
- Gestión unificada de amenazas (UTM)
- Sistemas de detección de intrusiones (IDS)

Seguridad en la nube

- Agentes de seguridad de acceso a la nube (CASB)
- Plataformas de protección de la carga de trabajo en la nube (CWPP)

Threat Intelligence

- Inteligencia frente a ciberamenazas (CTI)

Seguridad de identidad

- Gestión de acceso y de identidad (IAM)
- Gestión de accesos con privilegio (PAM)

Concientización en seguridad de OT/IoT

Por tipo de transporte

- TCP
- UDP
- Netflow
- sflow
- nats-jetstream
- kafka
- HTTP
- SQL
  - SQLite
  - MSSQL
  - MySQL
  - PostgreSQL
  - Cockroach
  - Oracle
  - Firebird
- Archivo
- 1c-log y 1c-xml
- Diodo
- FTP
- NFS
- WMI
- WEC
- SNMP
- SNMP-TRAP
- API de VMware

Por tipo de datos

- XML
- Syslog
- Csv
- JSON
- SQL
- IPFIX
- CEF
- Netflow 5
- Netflow 9
- KV

Por proveedor

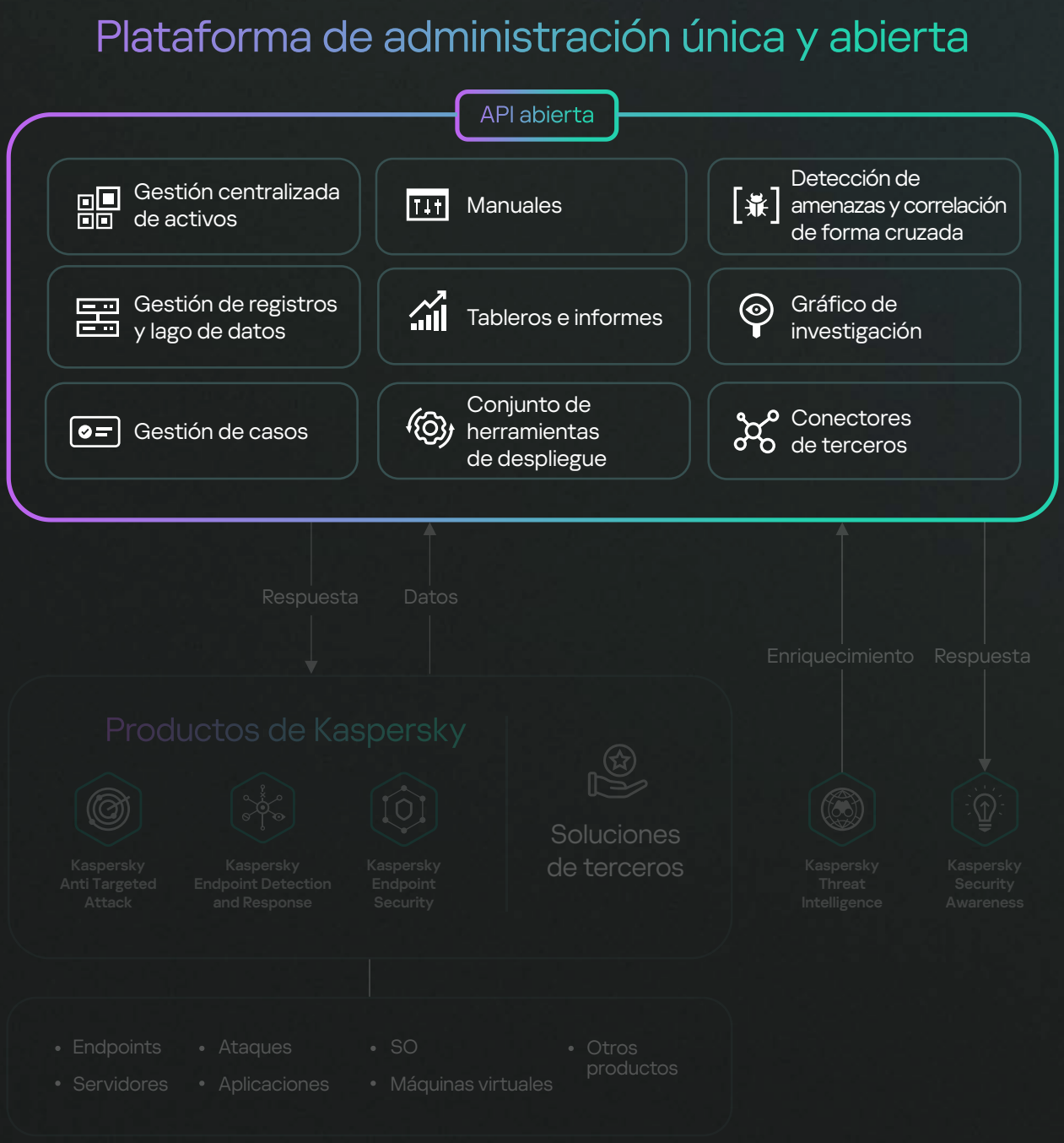
- Kaspersky
- Absolute
- AhnLab
- Aruba
- Avigilo
- Ayehu
- Barracuda
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- CheckPoint
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- DeepInstinct
- Delinea
- EclecticIQ
- Edge Technologies
- Eltex
- ESET
- F5 BigIP
- FireEye
- Forcepoint
- Fortinet
- Gigamon
- Huawei
- IBM
- Ideco
- Illumio
- Imperva
- Orion Soft
- Intralinks
- Juniper
- Kemptechnologies
- Kerio
- Lieberman
- MariaDB
- Microsoft
- MikroTik
- Minerva
- NetIQ
- NetScout
- Netskope
- Netwrix
- Nexthink
- NIKSUN
- Oracle
- PagerDuty
- Palo Alto
- Penta Security
- Proofpoint
- Radware
- Recorded
- ReversingLabs
- SailPoint
- SentinelOne
- Sonicwall
- Sophos
- ThreatConnect
- ThreatQuotient
- Trend Micro
- Trustwave
- VMWare
- Vormetric
- WatchGuard - Firebox
- Winchill Fracas
- Zettaset
- Zscaler, etc.

Lo que ofrecemos

Kaspersky XDR está disponible en dos opciones.

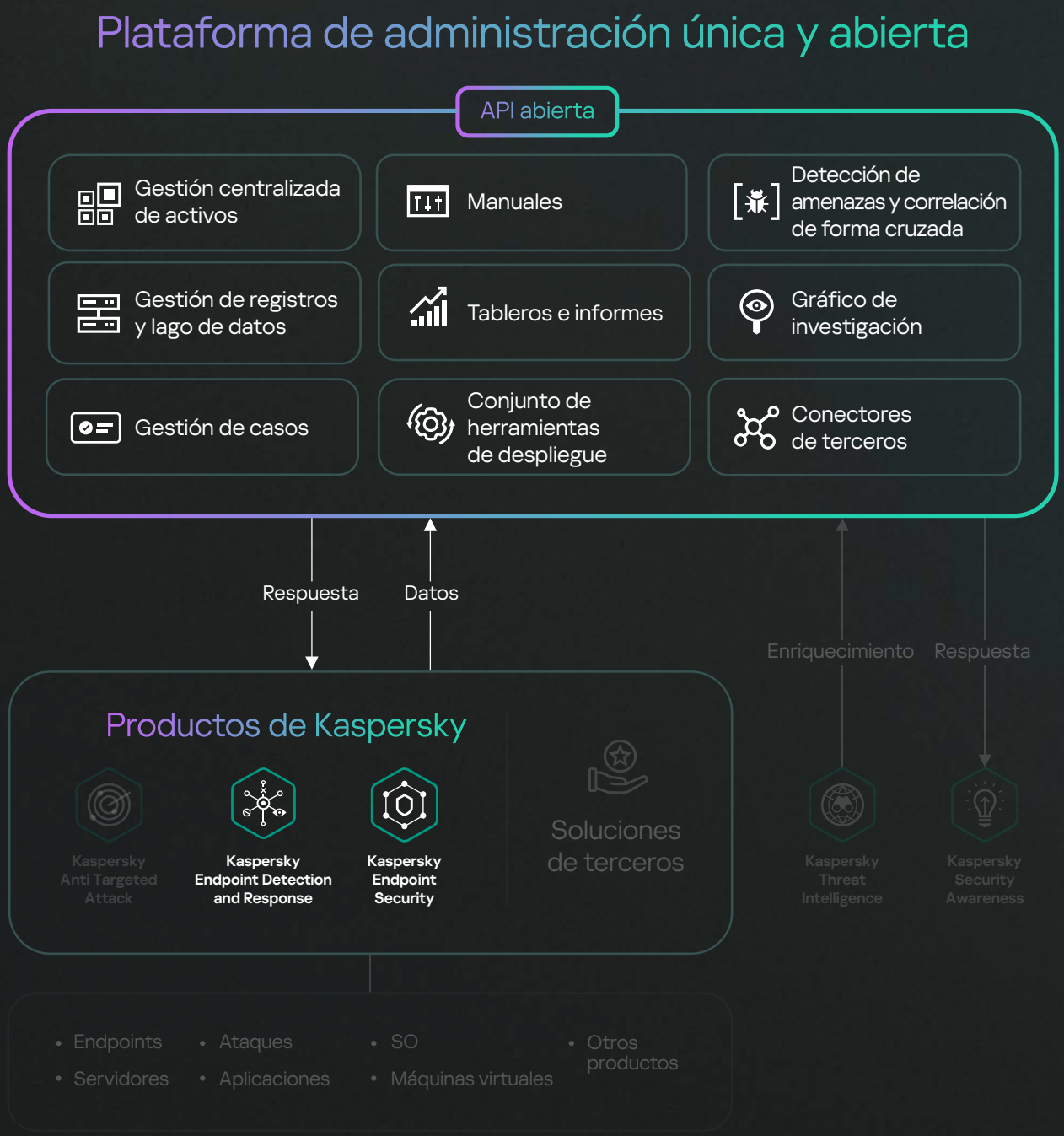
KasperskyXDR Core

Kaspersky XDR Core es para los clientes que ya tienen soluciones de endpoints y EDR implementadas y no quieren reemplazarlas, por lo que prefieren extender la funcionalidad con un motor de correlaciones, respuestas automatizadas y conectores externos.



Kaspersky XDR Expert

Kaspersky XDR Expert combina la mejor protección de endpoints de su clase con las capacidades de detección avanzada de Kaspersky EDR Expert, un motor de correlaciones y respuestas automatizadas. Pueden agregarse conectores externos para unir los datos.



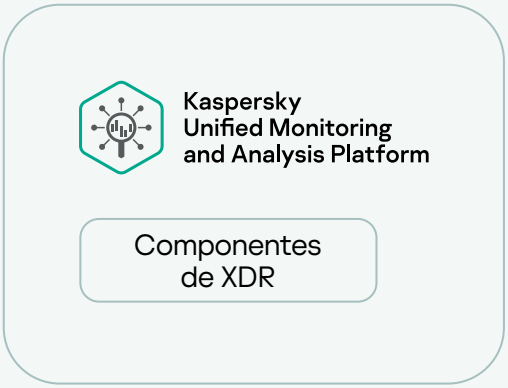
Valor agregado con sensores complementarios

Kaspersky XDR permite una integración fluida de sensores complementarios diseñados para proteger activos específicos. Estos sensores se integran eficazmente en XDR, agregando un valor adicional y transformándola en una plataforma cohesiva. Esto proporciona a los analistas un espacio de trabajo centralizado que abarca todas las soluciones integradas.

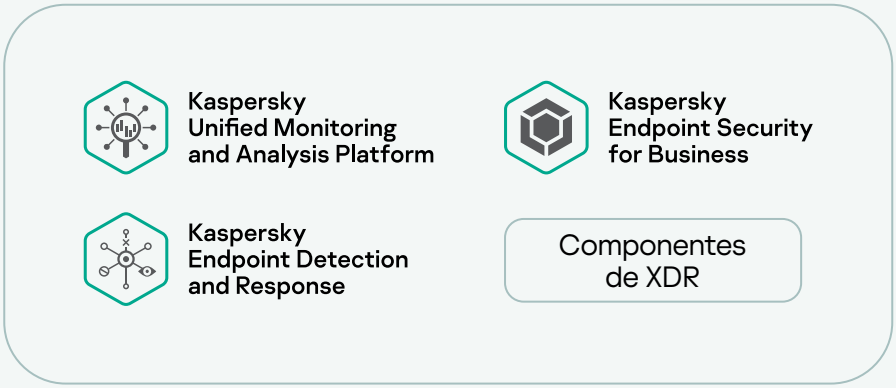
No solo mejora sus defensas a través de EDR, sino que también ofrece capacidades de integración flexibles para que los clientes puedan agregar productos al ecosistema en cualquier momento.

		Kaspersky XDR Core	Kaspersky XDR Expert
Componentes de una plataforma de administración única y abierta	Motor de correlación cruzada (con tecnología de KUMA) • Conectores de terceros • Gestión de registros y lago de datos • Detección de amenazas y correlación de forma cruzada • Gestión de activos • Tableros e informes	●	●
	Componentes de XDR • Gestión de casos • Orquestación y automatización de respuestas (manuales) • Investigación • Conjunto de herramientas de despliegue • API abierta	●	●
Funcionalidad de Kaspersky EDR y KESB	Detección automatizada, semiautomatizada y manual		●
	Supervisión de endpoints protegidos		●
	Contención de la amenaza		●
	Opciones de recuperación		●

Kaspersky XDR Core



Kaspersky XDR Expert



¿Por qué elegir Kaspersky XDR?

La más probada y premiada, así es la protección Kaspersky.

Kaspersky es una empresa de ciberseguridad global establecida con una sólida trayectoria en seguridad. Hace más de 25 años que protegemos a organizaciones .de todo el mundo y recibimos incontables galardones por nuestros productos y servicios. Entre 2013 y 2022, los productos de Kaspersky:

827

participaron en 827 pruebas y revisiones independientes

587

alcanzaron 587 primeros puestos

685

quedaron entre los tres primeros puestos

En 2023, Kaspersky recibió la mención de Empresa líder en el mercado de soluciones de XDR, por parte de la empresa global de asesoría e investigación de tecnología ISG. Este reconocimiento define "empresas líderes" como aquellas que tienen una oferta integral de productos y servicios y que representan una fortaleza innovadora y estabilidad competitiva.

Más información

Kaspersky Extended Detection and Response

Solicitar una demostración

latam.kaspersky.com

#kaspersky
#bringonthefuture