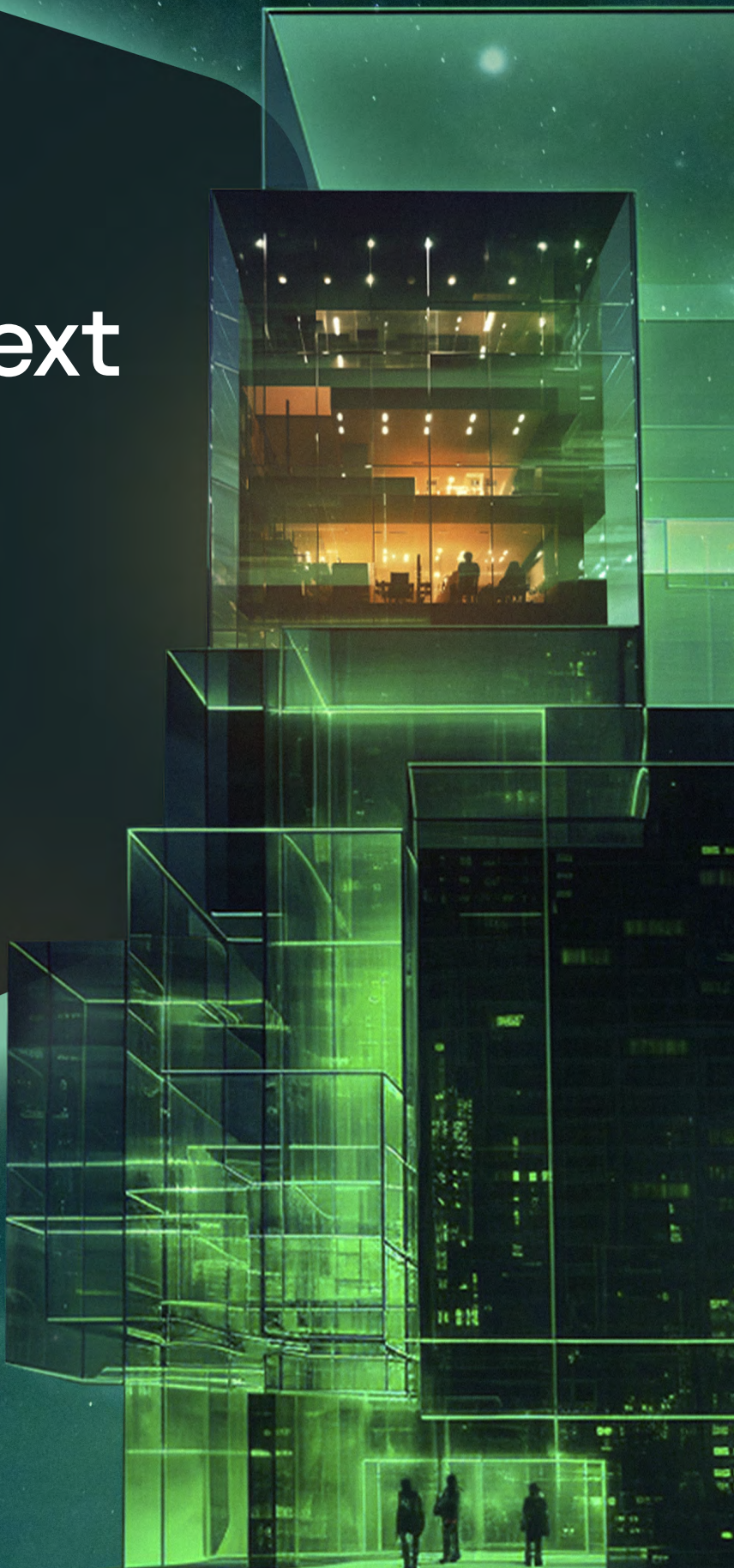
Kaspersky Next XDR Expert

Visibilidad inigualable.
Protección integral.



kaspersky

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, los requisitos regulatorios y el déficit mundial de competencias IT a este panorama, es fácil entender 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 a 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.

Como parte de la línea de productos de Kaspersky Next, presentamos Kaspersky Next XDR Expert, una solución que representa el enfoque de XDR de Kaspersky y proporciona una visión integral de la seguridad de una empresa.

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.

Evolucionó de la plataforma Kaspersky Anti-Targeted Attack como XDR nativa en 2016 a XDR abierta en 2023, y proporciona una visión integral de la seguridad. Kaspersky XDR, que se puede administrar fácilmente desde la Plataforma de administración única abierta, ofrece una seguridad integral en las instalaciones y permite garantizar que los datos confidenciales de los clientes permanezcan dentro de su propia infraestructura, mientras cumple 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 única plataforma abierta: una herramienta universal para crear un ecosistema unificado de productos de ciberseguridad. En el centro de Kaspersky XDR se encuentran nuestras soluciones líderes: Kaspersky Unified Monitoring and Analysis Platform, Kaspersky Next EDR Foundations y Kaspersky Endpoint Detection and Response Expert. KATA es una opción adicional para la gestión avanzada de redes.

Supervisión y análisis

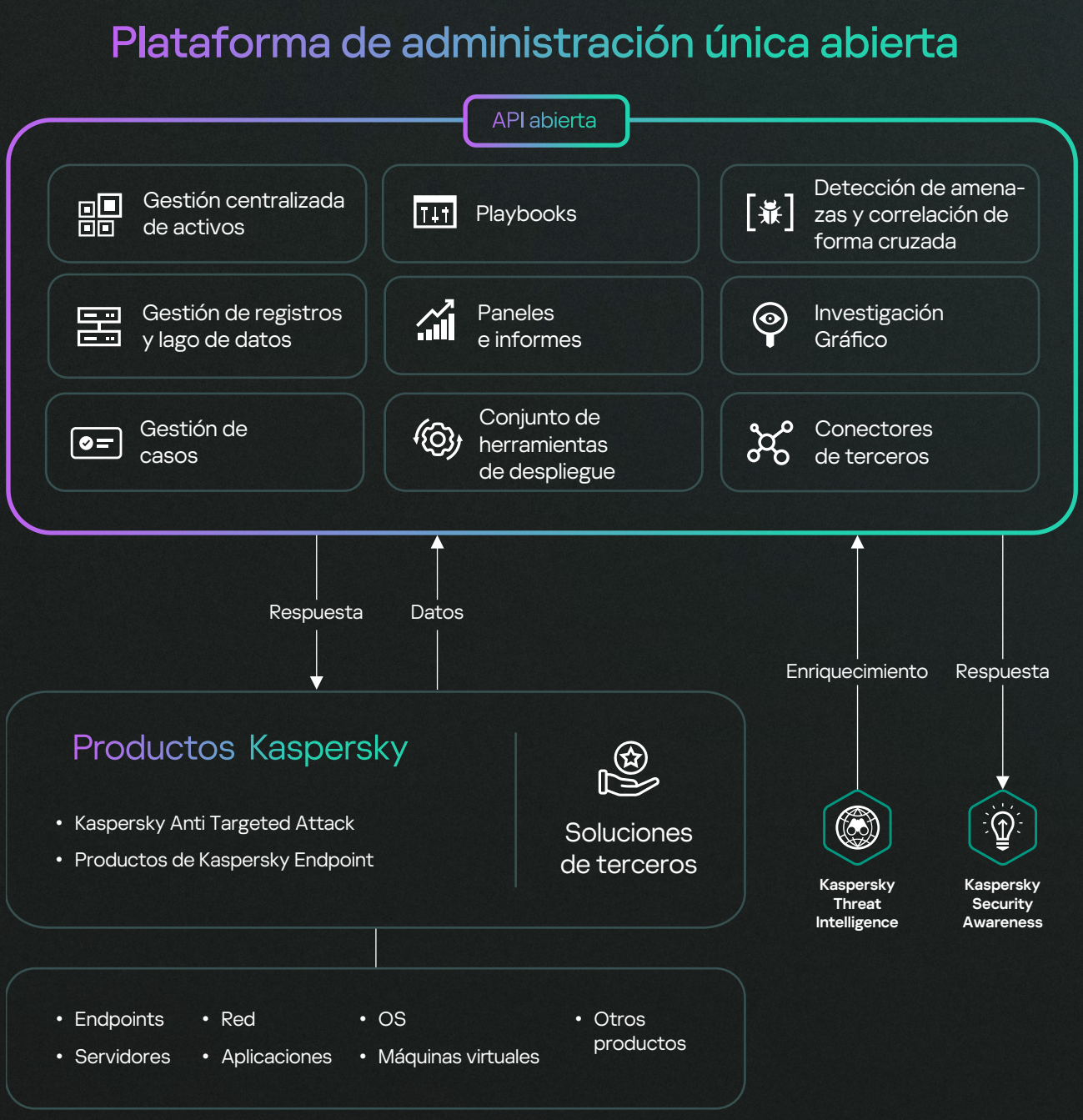
Proporciona recopilación y análisis centralizados de registros, correlación de eventos de seguridad en tiempo real y notificación oportuna de incidentes. Incluye un conjunto preparado de reglas y acceso a la amplia cartera de servicios de Kaspersky Threat Intelligence y prioriza amenazas, ataques e indicadores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

Protección de endpoints

Proporciona una protección sólida de endpoints, asegurándolos contra ransomware, malware y ataques sin archivos. Nuestra protección de endpoints, ya sea en las instalaciones o en la nube, utiliza aprendizaje automático y análisis de comportamiento para proteger todos los tipos de endpoints 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 búsqueda y detección de amenazas mejoradas, gracias a la inteligencia de amenazas única y exhaustiva de Kaspersky, además de la automatización de tareas rutinarias, los procesos de investigación guiada y las detecciones personalizables, promueven una resolución rápida de incidentes.



Características poderosas, beneficios importantes

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 es uno de los pocos proveedores que ofrecen una solución de XDR integral en las instalaciones que garantiza que los datos confidenciales de los clientes permanezcan dentro de su propia infraestructura, mientras se cumplen los requisitos de soberanía de datos.

Integración fluida y firme entre los productos de Kaspersky

La interacción entre los productos alcanza un nivel que va más allá del alcance de las soluciones externas, lo que permite contar con un sistema de soporte unificado y un diseño integrado a la perfección.

Funcionalidad de tenencia múltiple que proporciona escenarios de MSSP

Brinde XDR como un servicio con inquilinos independientes. Los usuarios de un grupo no pueden ver los datos de otros, 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 abarcan 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 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)

Inteligencia de amenazas

- Inteligencia frente a ciberamenazas (CTI)

Seguridad de identidad

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

Concientización en seguridad 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

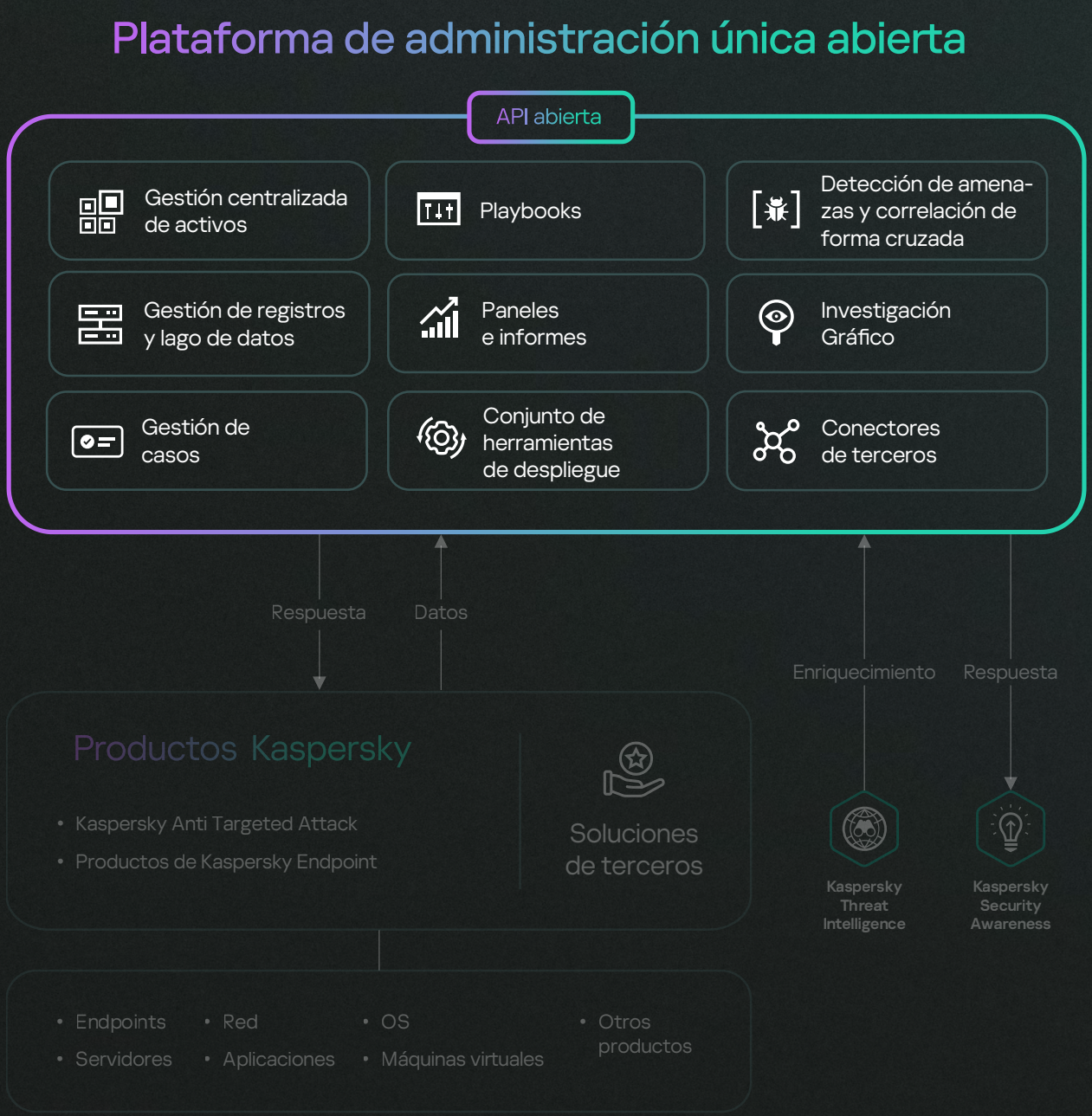
- Kaspersky
- Absolute
- AhnLab
- Aruba
- Avigilo
- Ayehu
- Barracuda
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- CheckPoint
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- DeepInstinct
- Delinea
- EclecticIQ
- Edge Technologies
- Eltex
- ESET
- 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.

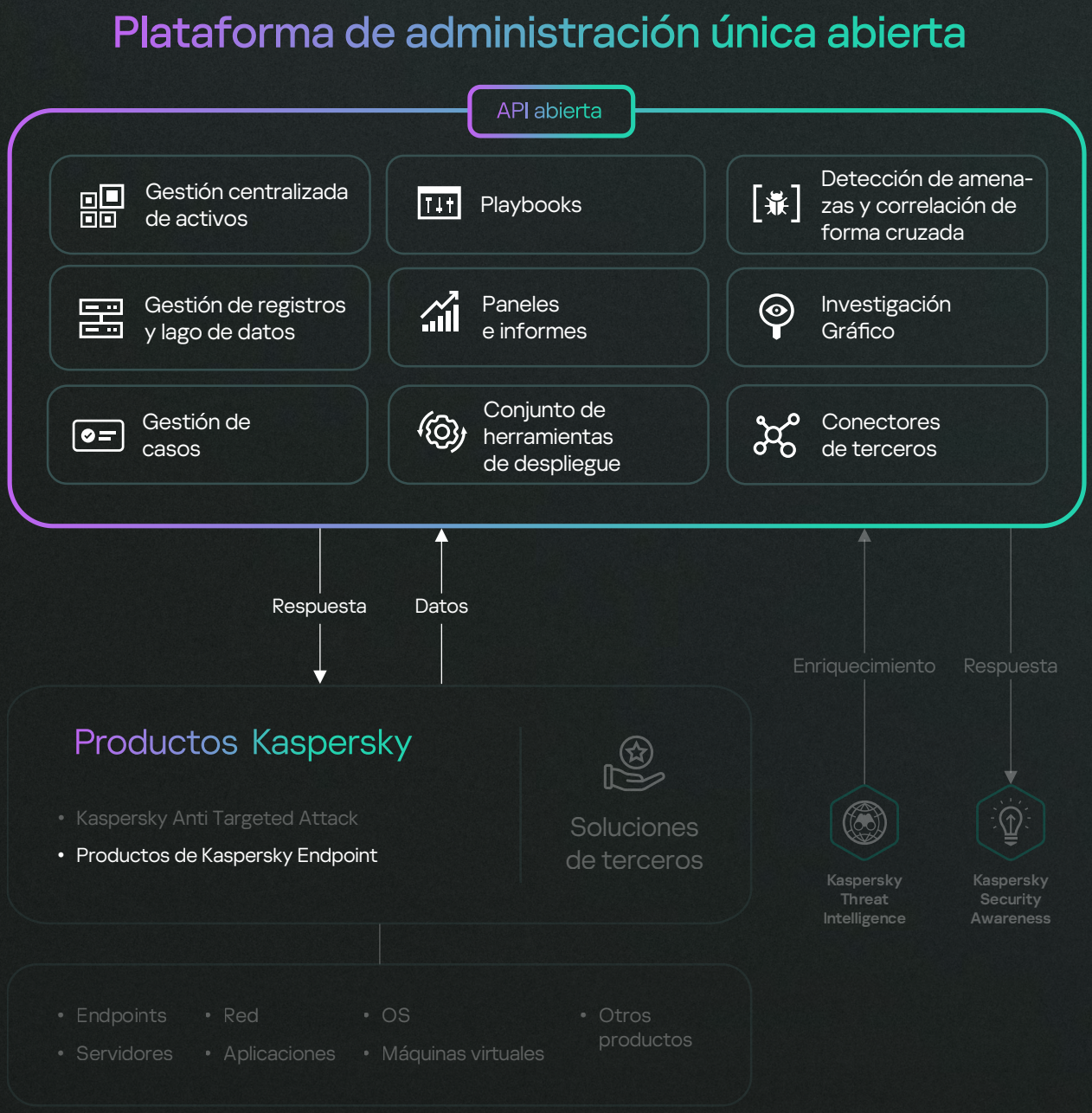
Kaspersky XDR Core

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



Kaspersky Next XDR Expert

Kaspersky Next 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 admite la integración fluida de sensores complementarios diseñados para proteger activos específicos, que se integran eficientemente en XDR para brindar una capa agregada de valor y transforman a XDR en una plataforma cohesiva que les proporciona a los analistas un espacio de trabajo centralizado que abarca todas las soluciones integradas.

Kaspersky XDR 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 Next XDR Expert
Plataforma de administración única abierta y sus componentes	Motor de correlación cruzada • 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 XDR • Gestión de casos • Orquestación y automatización de respuestas (manuales) • Investigación • Conjunto de herramientas de despliegue • API abierta	●	●
Funcionalidad de Kaspersky Endpoint*	Detección automatizada, semiautomatizada y manual		●
	Supervisión de endpoints protegidos		●
	Contención de la amenaza		●
	Opciones de recuperación		●
	Protección y administración de dispositivos móviles		●
	Detección y bloqueo de servicios en la nube		●
	Seguridad para MS Office 365, detección de datos		●
	Formación en ciberseguridad para administradores IT		●

* La disponibilidad de las funciones varía según el método de implementación

Kaspersky XDR Core

Kaspersky
Unified Monitoring
and Analysis Platform

Componentes XDR

Kaspersky Next XDR Expert

Kaspersky
Unified Monitoring
and Analysis Platform

Kaspersky
Endpoint Detection
and Response
Expert

Kaspersky Next
EDR Foundations

Componentes XDR

Presentación de Kaspersky Next

Kaspersky Next
EDR Foundations

Seguridad sólida para todos

Proteja todos sus endpoints

Si necesita

- Una protección sólida de endpoints
- Controles de seguridad básicos
- Una automatización máxima

Kaspersky Next
EDR Optimum

Construya sus defensas

Impulse la seguridad con una investigación y respuesta esencial

Si necesita

- Capacidades mejoradas de visibilidad y respuesta
- Seguridad en la nube expandida
- Controles de clase empresarial

Kaspersky Next
XDR Expert

Equipe a sus expertos

Proteja su empresa contra las amenazas más complejas y avanzadas

Si necesita

- Detección de amenazas avanzadas
- Integración perfecta
- Herramientas potentes de búsqueda de amenazas

¿Por qué elegir Kaspersky XDR?

La más probada. La más premiada. 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; recibimos incontables premios y 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. ISG define empresas "líderes" como aquellas que tienen una oferta integral de productos y servicios y que representan una fortaleza innovadora y estabilidad competitiva.

Aprenda más

Kaspersky Extended Detection and Response

Solicitar una demostración

latam.kaspersky.com

#kaspersky
#bringonthefuture