






Kaspersky MXDR









kaspersky preparados
para el futuro

Capas de Kaspersky Next MXDR Optimum







Características de protección en endpoints

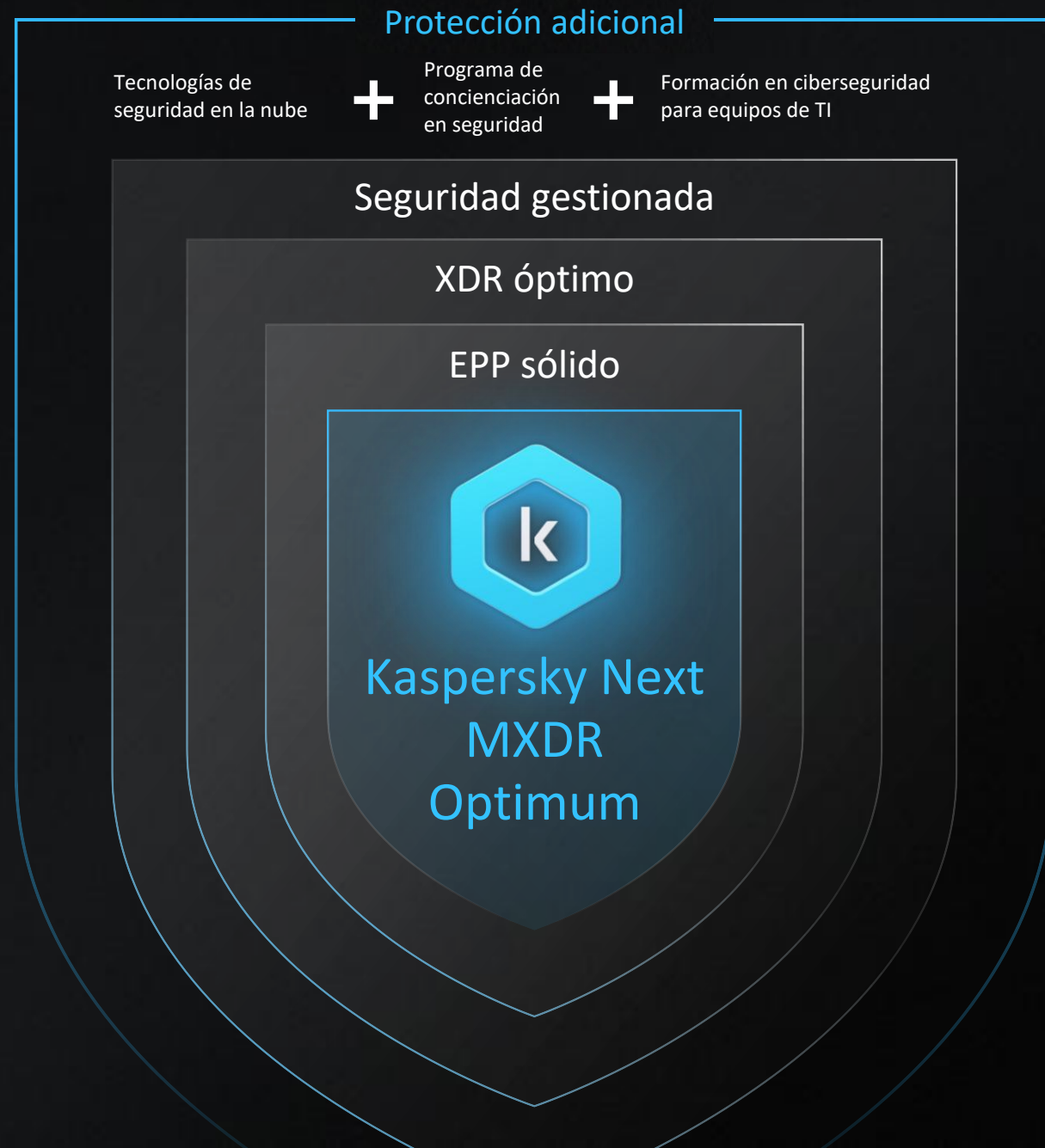
-  Antimalware mejorado
-  Refuerzo ampliado
-  Valoración de las vulnerabilidades
-  Controles de endpoints
-  Protección de datos
-  Gestión de parches

Detección, análisis y respuesta

-  Detección de comportamientos
-  Unificación de alertas
-  Sandbox basado en la nube
-  Descubrimiento de pruebas de amenazas (IoC) e IoC personalizados
-  Análisis de la causa raíz
-  Rango de acciones de respuesta

Protección gestionada

-  Supervisión y detección de amenazas continuas
-  Vista general de todos los recursos protegidos
-  Almacenamiento de telemetría sin procesar durante 3 meses
-  Comunicarse directamente con el equipo SOC sobre los incidentes
-  Envío de incidentes
-  Respuesta guiada automatizada



Reducción de la superficie de ataque

Refuerzo del sistema

Los diversos componentes de control (entre ellos, Control de Anomalías Adaptativo y algoritmos de ML) permiten adaptar el refuerzo del sistema y la configuración de las directivas de seguridad de forma automática según el comportamiento de los usuarios.

Gestión de parches y vulnerabilidades

La administración de vulnerabilidades y parches simplifica las actualizaciones y optimiza las operaciones de seguridad y TI al admitir la instalación de SO y software de terceros en los hosts.



Características de detección y respuesta en endpoints



Indicadores IoC

Búsqueda de indicadores de vulneración (IoC) con respuesta automática en todos los endpoints.



Análisis de la causa raíz

Datos y herramientas de visualización para confirmar la causa raíz de la amenaza y la necesidad de tomar acciones de respuesta adicionales.



Respuesta automática

Guía de respuestas y automatización incorporadas.



Enriquecimiento

Acceso a Threat Intelligence Portal



Consultas en sandbox basado en la nube



La integración con **Kaspersky Cloud Sandbox** permite realizar diversas acciones mediante **Kaspersky Threat Intelligence Portal**.

Detección automática de tipos de archivos

Administración de tareas ejecutables obsoletas

Carga y ejecución de archivos en Cloud Sandbox

Carga de un archivo desde una dirección web y posterior ejecución en Cloud Sandbox

Características de antievasión para contrarrestar el malware diseñado para eludir entornos aislados

Ejecución de un archivo extraído del informe de Cloud Sandbox

Exportación de resultados de los análisis

Consultas en sandbox basado en la nube

Send to TIP Sandbox

Operations / Repositories / Quarantine

Refresh Delete Download Restore **Send to TIP Sandbox** Search...

File name	Status	Device name	Current action	Object	Placed in repository	Entry added by	Size, in bytes	Restoratic
report_annual_2023_01.xlsx	Disinfected	WIN11-25-0000	Deleting	EICAR-File	02/11/2025, 12:28:41 PM	KES	0	C:\Users\...
invoice_05487_2024-01-15...	Infected	gt-ksc-qc-sles	Disinfecting	EICAR-File	02/14/2025 07:56:44 PM	kesl	73	C:\Users\...
task_list_31-12-2024.docx	Warning	win11-25-0000.avp.ru	Scanning	EICAR-File	07/05/2025 05:30:23 AM	KES	12	/opt/kasp...
data_backup_20-01-2025...	Probably infected	Analytics-PC-001	Restoring	EICAR-File	05/06/2025 03:10:21 AM	kesl	43	C:\Users\...
meeting_notes_Q1_2025.p...	Added by user	Admin-PC-005	--	EICAR-File	04/11/2025 01:18:12 PM	kesl	65	C:\Windo...
user_feedback_20250120...	False positive	Corp-Laptop-Beta	--	EICAR-File	07/31/2025 03:47:27 AM	KES	87	C:\Progra...
project_plan_v2.5.mpp	Not infected	Corp-PC-004	--	EICAR-File	12/29/2025 12:08:11 AM	kesl	0	C:\Progra...
contract_draft_rev3.pdf	Password-protected	Design-Laptop-002	--	EICAR-File	11/24/2025 08:03:44 PM	kesl	1260	C:\Temp\...
analysis_results_2024_v1.xl...	Deleted	DevOps-Laptop-002	--	EICAR-File	09/04/2025 09:54:45 PM	KES	73	C:\Users\...
error_log_21012025.txt	Must be send to Kaspersky	Engineering-Laptop-001	--	EICAR-File	08/18/2025 02:29:07 AM	KES	74	C:\Users\...
financial_summary_Y2024...	Infected	Finance-Laptop-002	--	EICAR-File	08/03/2025 07:28:21 PM	KES	12	C:\Recycl...
team_roster_January_202...	Infected	HR-PC-002	--	EICAR-File	05/10/2025 05:51:32 AM	kesl	93	C:\System...
presentation_final_202501...	Infected	IT-Desktop-001	--	EICAR-File	03/27/2025 06:03:16 AM	kesl	63	C:\Windo...
design_mockup_v4.fig	Infected	Legal-Laptop-003	--	EICAR-File	05/20/2025 09:48:56 AM	kesl	23	C:\Users\...
event_schedule_2025-03-...	Infected	Marketing-PC-Omega	--	EICAR-File	04/03/2025 04:47:34 AM	KES	0	C:\Users\...
dashboard_report_01-202...	Infected	Sales-Laptop-004	--	EICAR-File	01/22/2025 06:11:28 PM	kesl	0	C:\Progra...
security_patch_2025-01-21...	Infected	Security-PC-Alpha	--	EICAR-File	08/16/2025 11:49:13 PM	kesl	23	C:\Users\...
case_study_final.pdf	Infected	Support-PC-003	--	EICAR-File	03/15/2025 04:25:53 AM	KES	24	C:\Users\...
media_assets_2024_Q4.zip	Infected	WIN2019-0128	--	EICAR-File	11/19/2025 08:43:39 AM	kesl	90	C:\Windo...
risk_assessment_rev2.xlsx	Infected	LIN2016-0054	--	EICAR-File	03/05/2025 10:17:01 PM	KES	45	C:\Users\...
error_log_21234234025.txt	Infected	LIN2015-0024	--	EICAR-File	01/17/2025 03:23:21 PM	KES	82	C:\inetpul...
analysis_results_2025_v1.xl...	Infected	WIN2017-0102	--	EICAR-File	05/20/2025 09:48:56 AM	KES	0	C:\Users\...
case_study.pdf	Infected	MAC2024-0244	--	EICAR-File	09/04/2025 09:54:45 PM	kesl	1	C:\Windo...

Total 287 / Selected 0

Para investigar archivos maliciosos con facilidad y obtener un contexto más amplio y más detalles, ofrecemos la integración con Cloud Sandbox. Desde la interfaz del producto, el usuario puede cargar muestras que puedan ser maliciosas para verificar su reputación en segundos.

Los datos generados pueden usarse para analizar IoC posteriormente.

Sandbox

Support for file: eicar.com

Summary

Detects

1 Total

- Malware 1
- Adware and other 0

Suspicious activities

0 Total

- High 0
- Medium 0
- Low 0

Extracted files

1 Total

- Malware 1
- Adware and other 0
- Clean 0
- Not categorized 0

Network activities

0 Total

- Dangerous 0
- Not trusted 0
- Adware and other 0
- Good 0
- Not categorized 0

Uploaded: May 28 2025 08:57
 Analyzed: --
 Database update: May 22 2025 23:13
 File size: 68.00 B (68 B)
 File type: cmd

Execution environment: Auto (Windows 7 x64)
 Execution time: Auto (100 sec)
 File extension: cmd
 HTTPS decryption: Yes
 Click links: Yes
 Internet access options: Auto (RU)

MD5: 44d88612faa8f34de2e1278eb02f
 SHA1: 339f856e612b73825ee726027f9864214140
 SHA256: 275a021ba8b6489e5464718997db9d16636c99Sec2f62a2c4535aaf6511d0f

Integración de Security Awareness

En Automated Security Awareness Platform, se pueden asignar cursos de formación a usuarios. Visualiza los datos sobre los cursos completados y programados de cada integrante del personal cuando sea que lo necesites.

The screenshot displays the 'Alert details' page for a 'Success: Deleted' alert. The interface is divided into several sections:

- Alert details:** Shows the alert result, date and time (11.12.2019 15:31:00), category (PDM:Worm.win32.TestBBVerdict), object name (C:\test\sw+test_2.exe), scan mode (On System Watcher Scan), and object type (Memory process).
- Computer:** Lists computer name, network interfaces (address 192.168.0.1, netmask 255.255.255.0), OS (MAC OS 12.0), group name (Managed devices), and policy name (KES for Win).
- Process:** Shows startup parameters and system PID.
- User:** Displays user name (Igor Ivanov), login session ID (13745905), and privileged user status (No).
- File:** Provides file name and size (C:\test\KL_DEMO.exe (2MB)), MD5 and SHA256 hashes, trust check result (Invalid signature), and creation/modification dates.
- Information from Kaspersky TIP:** Shows the file is trusted and provides statistics on users having the application.
- Download and File modification:** Lists application details and modification history.

A central modal window titled 'KASAP' is open, showing a list of actions: 'Assign KASAP group', 'Active Directory', 'Lock account', 'Reset password', 'Add user to security group', and 'Delete user from security group'. A blue arrow points from the 'Select response actions' dropdown in the 'User' section to this modal.

To the right, a 'User details' panel for 'Igor Ivanov' is visible, showing his KASAP group (HR managers), education status, email, and a list of assigned and completed courses, including 'Phishing 2 level' and 'Secure passwords 1 level'.

Integración con Active Directory

Nuevos escenarios de respuesta desde Active Directory

KASAP

- Assign KASAP group
- Active Directory
- Lock account
- Reset password
- Add user to security group
- Delete user from security group

Add user to security group

Specify the distinguished name (DN) of the security group to which you want to add the user. Note that it may take up to 12 hours to update the information about the user's security group.

Security group DN *

Seguridad de Office 365

- Protección avanzada frente a amenazas
- Antiphishing, antimalware, antispam y eliminación de archivos adjuntos maliciosos
- Para las principales aplicaciones de MS Office 365

Information panel **Getting started** Monitoring

REQUIRED: establish a connection to Microsoft Office 365

01

Microsoft Office 365
Access to your Office 365 organization is granted.

[Settings](#)

REQUIRED: configure security policies for Microsoft Office 365

02

Exchange Online protection
Protection of your Exchange Online mailboxes is configured.

[Exchange Online Protection](#)

03

OneDrive protection
Protection of your OneDrive users is configured.

[OneDrive Protection](#)

04

SharePoint Online protection
Protect your SharePoint Online sites from malware.

[SharePoint Online Protection](#)

05

Teams protection
Protect all your SharePoint Online and OneDrive files transmitted via Teams from malware.

[Online Help](#)

La Joya de La Corona...

Kaspersky MDR

Es una solución integral que ofrece protección avanzada y continua incluso contra las amenazas más innovadoras

Supervisión continua las 24 horas del día, los 7 días de la semana en busca de actividades sospechosas

Detección y análisis de amenazas para evitar posibles sistemas vulnerados

Priorización de alertas para filtrar falsos positivos y asignar recursos de forma eficiente

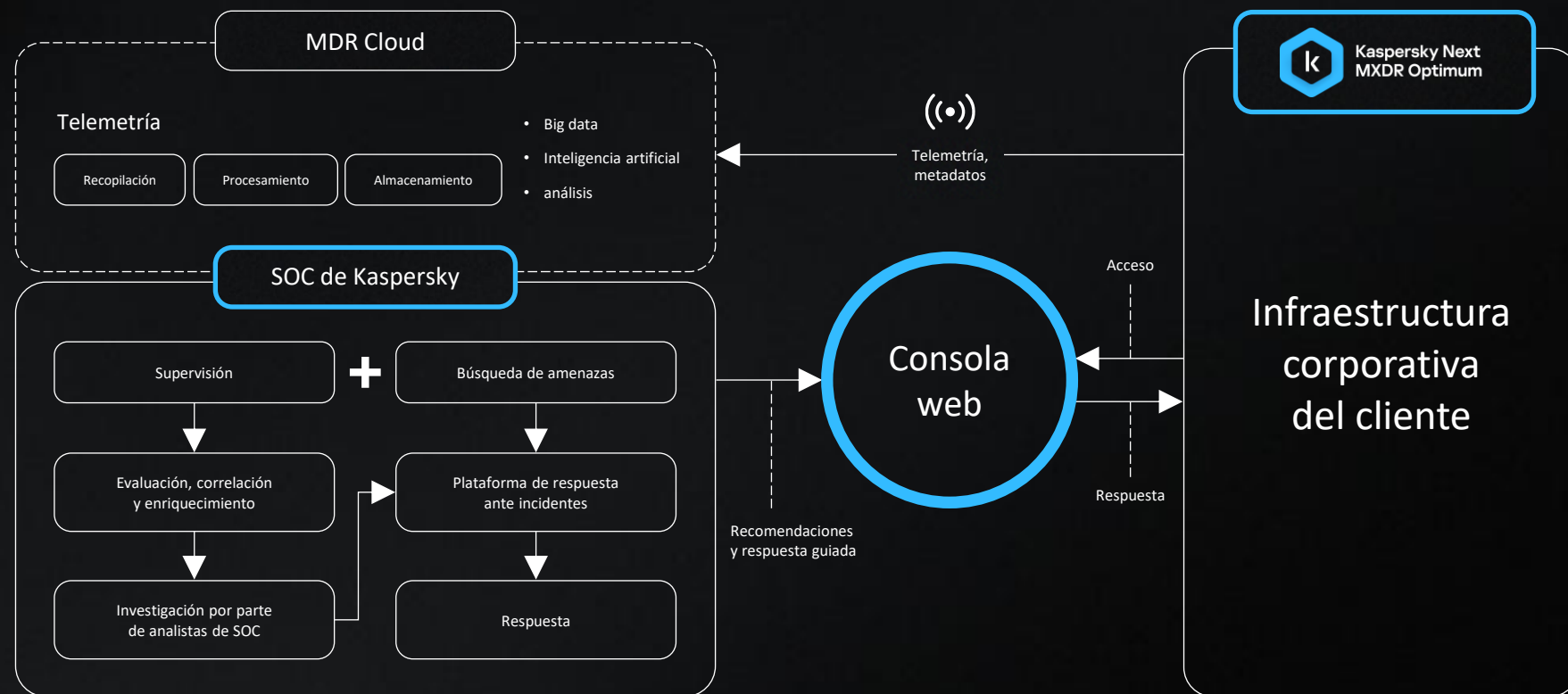
Búsqueda de amenazas y respuesta por expertos en seguridad de Kaspersky

Seguridad gestionada

1 Kaspersky Next MXDR Optimum captura y envía los datos al SOC de Kaspersky.

2 La telemetría, los metadatos y la priorización de alertas se analizan con herramientas de ML/IA, con la participación activa de los expertos del SOC de Kaspersky.

3 El equipo del SOC de Kaspersky investiga alertas e informa al cliente acerca de actividad maliciosa, además de ofrecer recomendaciones y respuesta guiada paso a paso.



Motores de inteligencia artificial (IA)

Los mecanismos de IA filtran automáticamente los falsos positivos, lo que permite mejorar considerablemente la productividad de los analistas y reduce el tiempo medio de priorización, detección y respuesta (MTTD/MTTR)



Eventos



Alertas

Correlación
de datos



Análisis
de IA

Priorización de alertas



Desglose
de alertas



Incidentes

Confirmación del
estado del disparador:
Verdadero/Falso

Capacidades de las tecnologías de IA

1

Detección más rápida

La IA analiza objetos sospechosos en el momento en que ingresan los datos

2

Resuelven entre el 35 y 40 % de alertas

Aumenta de forma significativa el rendimiento de los analistas, lo que genera SLA de tiempo de reacción reducidos

3

Priorización de alertas

Permite a nuestros analistas enfocarse en las alertas más importantes

4

Resolución de alertas automática

No es necesario recurrir a analistas humanos

Escenarios de respuesta

Nuestro equipo examina incidentes y crea respuestas que puedes aceptar o rechazar, como:

Tipo de respuesta

Description

Obtener archivo

Copiar un archivo de tu infraestructura al SOC de Kaspersky

Aislar

Aislar el activo especificado de la red

Desactivar aislamiento

Desactivar el aislamiento de la red del activo especificado

Eliminar clave de registro

Eliminar una clave de registro o una rama de registro en el activo especificado

Volcado de memoria

Crear un volcado de memoria y enviarlo al SOC de Kaspersky

Terminar proceso

Terminar un proceso en el activo especificado con Kaspersky Endpoint Security for Windows

SLA

Nivel de prioridad	Tiempo de reacción	Valor objetivo
Alto (ejemplo: ataque dirigido)	1 hora	90 %
Medio (ejemplo: malware común)	4 hora	90 %
Bajo (por ejemplo: software publicitario, riskware, etc.)	24 horas	90 %

Tiempo de reacción

El tiempo que transcurre desde la detección del incidente (“Hora de creación”) hasta su publicación en la consola de MDR (“Hora de actualización”).

Valor objetivo

Porcentaje de incidentes en los que el tiempo de reacción y el tiempo de respuesta satisfacen el valor objetivo.

kaspersky

¡Muchas Gracias!



Javier Sanz

