

Lista de características

Kaspersky Next EDR Optimum

kaspersky cybersecurity true to business

Para pequeñas y medianas empresas

Contenido

Acerca de Kaspersky Next EDR Optimum 3

Kaspersky Next EDR Optimum forma parte de la línea de productos Kaspersky Next Optimum 3

Opciones de administración 4

Características 5

- Protección de endpoints 5
- Controles de seguridad 6
- Administración de dispositivos móviles avanzada y defensas contra amenazas móviles 6
- Características de EDR avanzadas 9
- Seguridad en la nube y protección del correo electrónico 11
- Características y formación en materia de concienciación sobre seguridad 12

Dispositivos y sistemas operativos compatibles 12



Acerca de Kaspersky Next EDR Optimum

Kaspersky Next EDR Optimum ofrece una sólida protección de endpoints, formación para el personal de TI, seguridad en la nube y mucho más. Todo potenciado por características de EDR esenciales que incluyen el análisis de IOC y la respuesta automatizada y guiada para ayudar a ponerle fin a los ataques con rapidez. Hemos desarrolado Kaspersky Next EDR Optimum para los equipos de ciberseguridad más pequeños que necesitan mejorar sus capacidades de respuesta ante incidentes y desarrollar conocimientos sin que les lleve demasiado tiempo.

Para las organizaciones que necesiten:

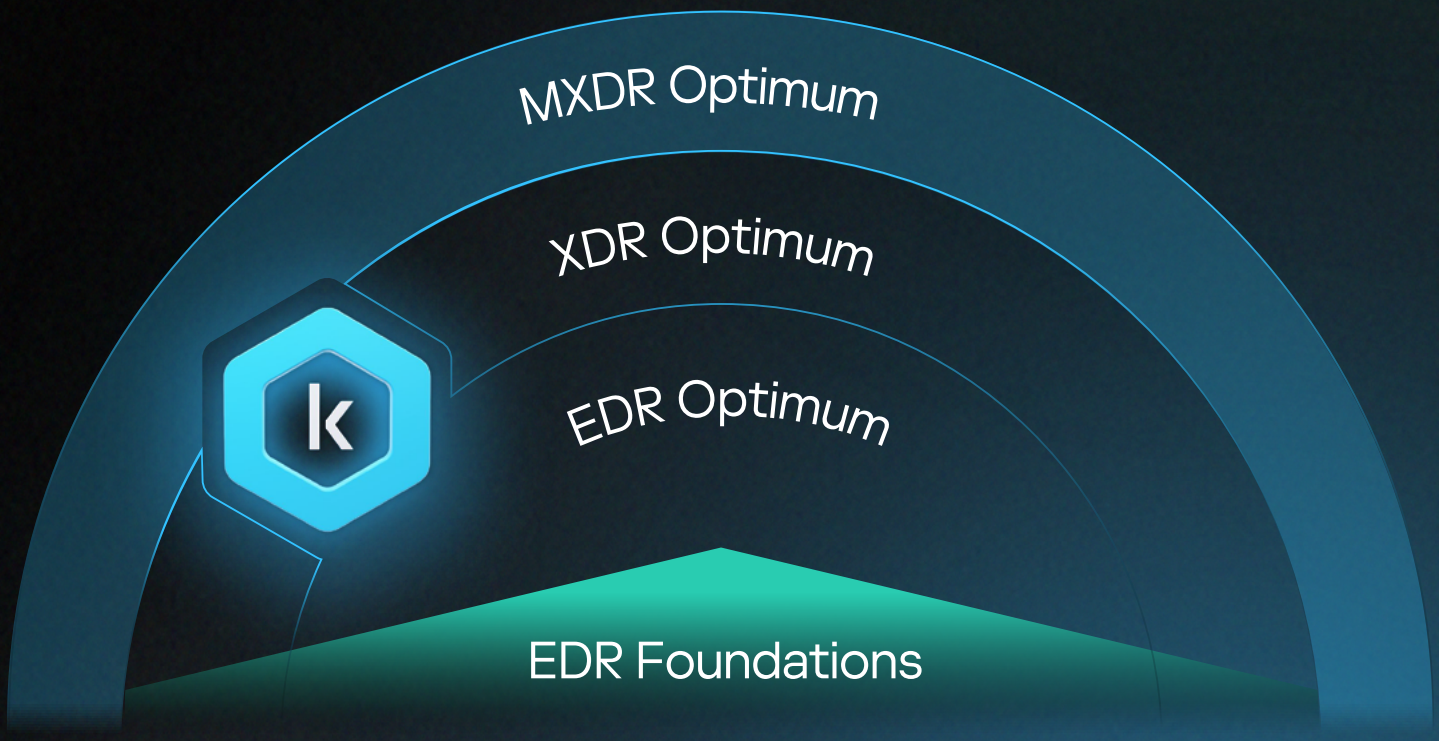
Para proteger una cantidad cada vez mayor de endpoints sin dejar de expandirse digitalmente

Para mejorar la resiliencia frente a ciberataques complejos y difíciles de detectar

Para desarrollar conocimientos especializados internos y operaciones de seguridad sin añadir complejidad

Kaspersky Next EDR Optimum: parte de la línea de productos de Kaspersky Next Optimum

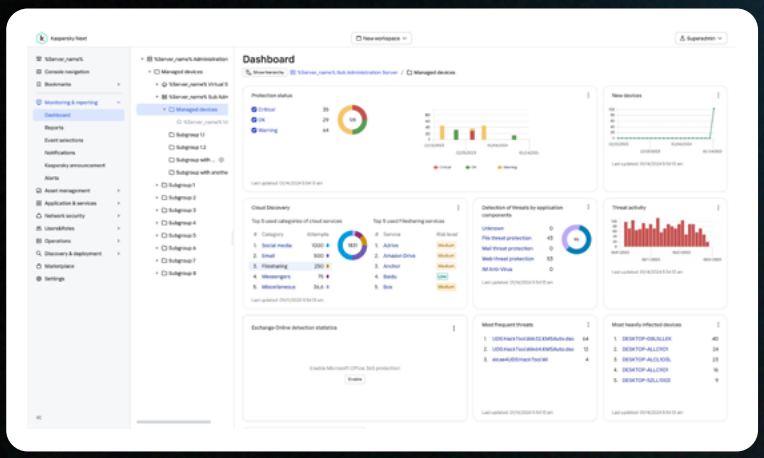
Kaspersky Next Optimum está destinada a pequeñas y medianas empresas que cuentan con equipos de ciberseguridad básicos que desean escalar su protección sin mayores complicaciones. El primer nivel ofrece una sólida protección de endpoints, mientras que el segundo nivel cuenta con características de detección y respuesta en endpoints y permite mejorar a funcionalidades de XDR esencial o MXDR para disfrutar de un nivel de ciberseguridad avanzado.



Opciones de administración

Independientemente de la opción que escoja o de la cantidad de hosts, Kaspersky Next EDR Optimum se administra a través de una única consola unificada con dos modos: Pro View y Expert View.

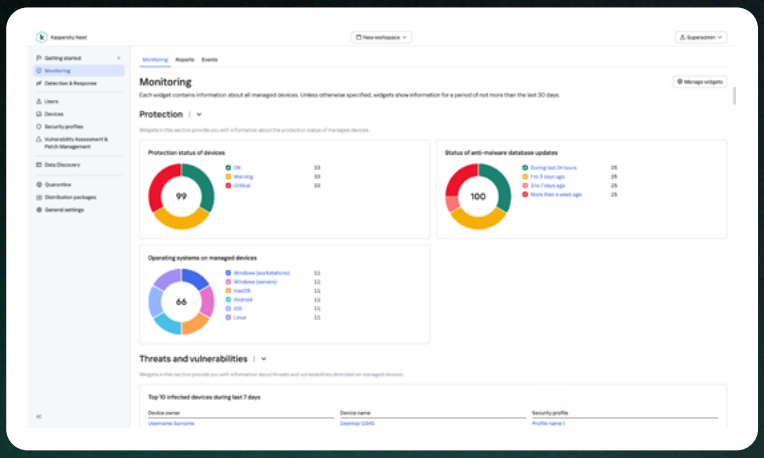
Este enfoque le permite empezar con una interfaz simplificada y pasar sin problemas a funciones más avanzadas a medida que crece su infraestructura o evolucionan sus necesidades de seguridad, sin tener que migrar ni realizar configuraciones adicionales.



Pro View

Una consola sencilla y fácil de administrar alojada en la nube.

Cantidad recomendada de hosts: **1–3000**



Expert View

Una consola personalizable con controles detallados, que ofrece dos opciones:

Basada en la nube

No supone ningún requisito de hardware para instalar el servidor de administración ni requiere que su equipo dedique tiempo a las actualizaciones: Kaspersky se encarga de alojarlo todo y de ofrecer soporte técnico.

Cantidad mínima de hosts administrados: **100**

En instalaciones locales

Ofrece una interfaz web para crear y administrar el sistema de protección.

* La solución está disponible tanto en las instalaciones como en la nube, pero aquí nos centraremos sobre todo en la implementación en la nube, ya que es la opción más habitual y flexible.

Características

Protección de endpoints

Característica	Descripción
Antimalware multicapa	Nuestro motor antimalware más reciente combina una protección basada en firmas, análisis exhaustivo y de comportamiento y tecnologías con asistencia en la nube para proteger sus equipos Windows contra amenazas de malware conocidas, desconocidas y sofisticadas. La tecnología de detección basada en patrones mejora las tasas de detección y ayuda a reducir el tamaño de las actualizaciones que descarga, para que pueda beneficiarse de una seguridad fiable que consume menos ancho de banda de comunicaciones.
Detección del comportamiento	Recolecta información sobre las acciones de las aplicaciones en el ordenador de un usuario y ofrece esta información a otros componentes para una protección más eficaz.
Prevención de exploits	Realiza un seguimiento de los archivos ejecutables que inician las aplicaciones vulnerables. Cuando se produce un intento, que no ha sido iniciado por el usuario, de abrir un archivo ejecutable desde una aplicación vulnerable, el componente impide que el archivo se ejecute.
Motor de remediación	Revierte las acciones que realiza el malware en el sistema operativo y protege frente a criptolockers.
Protección contra amenazas de archivo	Detecta y elimina amenazas en un dispositivo en tiempo real con las bases de datos antivirus de la aplicación y el servicio de nube de Kaspersky Security Network.
Protección contra amenazas de correo	Analiza los mensajes de los correos electrónicos entrantes y salientes en busca de amenazas. Se inicia junto con la aplicación, reside en la RAM del dispositivo y analiza todos los mensajes enviados o recibidos a través de los protocolos POP3, SMTP, IMAP y NNTP.
Protección contra amenazas web	Protege los datos entrantes y salientes que se envían hacia y desde un dispositivo a través de los protocolos HTTP, HTTPS y FTP, y evita que se ejecuten scripts peligrosos en el dispositivo.
Firewall	Controla las comunicaciones de red entrantes y salientes, bloquea las conexiones no autorizadas y ayuda a evitar que se propague el malware, al tiempo que garantiza el cumplimiento de las políticas de seguridad de la empresa.
Prevención de intrusiones basada en host (HIPS)	La prevención de intrusiones en el host evita que las aplicaciones realicen acciones que puedan ser perjudiciales para el sistema operativo y controla el acceso a los recursos del sistema operativo y a los datos personales.
Protección contra amenazas de red	Analiza el tráfico de red entrante en busca de actividades sospechosas y detecta patrones habituales de ataques a la red, como los ataques de fuerza bruta o los intentos de acceso remoto no autorizados. Cuando se detecta alguna actividad maliciosa, la aplicación bloquea la comunicación con el dispositivo atacante.
Prevención de ataques BadUSB	Evita que se utilicen en el ordenador dispositivos USB potencialmente maliciosos que emulan teclados. Cuando se reconoce un dispositivo USB como teclado, la aplicación le pide al usuario que introduzca un código para autorizar su uso.
Protección AMSI	Es compatible con la interfaz de análisis antimalware (AMSI) de Microsoft. AMSI permite que las aplicaciones de terceros compatibles con AMSI envíen objetos (por ejemplo, scripts de PowerShell) a Kaspersky Endpoint Security para que los analice de nuevo y, a continuación, reciban los resultados.
Kaspersky Security Network	Millones de clientes y miles de empresas permiten que el sistema basado en la nube Kaspersky Security Network (KSN) reciba datos anonimizados sobre comportamientos sospechosos y malware presentes en sus equipos. Este flujo de datos en tiempo real nos ayuda a proporcionar una respuesta más rápida al nuevo malware, además de lograr una tasa baja de falsos positivos.
Defensa contra amenazas móviles	Un conjunto de funciones de protección para asegurar los dispositivos Android y iOS contra malware, criptolockers, mineros de criptomonedas, spyware y otras amenazas. Eche un vistazo a los detalles por tipo de sistema operativo a continuación.
Integración con sistemas SIEM	Los eventos se pueden exportar a sistemas SIEM de terceros que se ocupan de cuestiones de seguridad a nivel organizativo y técnico (por ejemplo, los SOC). Se admiten los protocolos Syslog y CEF/LEEF.

Controles de seguridad

Característica	Descripción
Evaluación de vulnerabilidades	Proporciona una descripción general de las aplicaciones instaladas en los dispositivos corporativos, así como una lista de los parches disponibles para actualizar estas aplicaciones a las últimas versiones.
Administración de parches	Ofrece administración remota de las actualizaciones y la instalación de parches en los dispositivos corporativos para asegurarse de estar utilizando únicamente los productos más actualizados. La lista de aplicaciones está en la sección de evaluación de vulnerabilidades de la consola en línea del producto.
Administración del cifrado	Ofrece una administración centralizada del cifrado en los dispositivos de los empleados mediante los componentes de cifrado nativos de Windows (BitLocker) y Mac OS (FileVault), para ayudar a proteger los datos corporativos en caso de pérdida o robo de un dispositivo.
Control de aplicaciones	Administra el inicio de aplicaciones en los equipos de los usuarios y reduce el riesgo de infección de los ordenadores al restringir el acceso a aplicaciones. Esto le permite aplicar su propia política de seguridad corporativa al utilizar las aplicaciones.
Control web	Controla a qué recursos web pueden acceder los usuarios según las categorías, el contenido o la ubicación de los sitios web. Las listas de sitios permitidos o bloqueados ayudan a restringir el acceso a páginas web maliciosas o no autorizadas, al tiempo que permiten acceder únicamente a recursos de confianza en Internet.
Control de dispositivos	Controla el acceso del usuario a dispositivos externos y extraíbles conectados a la computadora. Los administradores pueden permitir o bloquear el uso de ciertos dispositivos según el tipo, o crear una lista de confianza.
Borrado remoto	Permite borrar de forma remota y definitiva los datos corporativos de los dispositivos de los usuarios sin posibilidad de recuperación, lo que ayuda a proteger la información confidencial en caso de pérdida o robo de un dispositivo.
Administración de dispositivos móviles avanzada	Le permite administrar los dispositivos móviles de los empleados, para que pueda aplicar los requisitos de seguridad corporativos, controlar el cumplimiento normativo, proteger los dispositivos frente a amenazas y evitar la filtración de información corporativa.

Administración de dispositivos móviles avanzada y protección contra amenazas móviles

Característica	Descripción
Android	
Protección antivirus	Detecta y neutraliza las amenazas en dispositivos, utilizando las bases de datos antivirus y el servicio en la nube Kaspersky Security Network. Protege el dispositivo contra amenazas, virus y otras aplicaciones maliciosas en tiempo real, analiza nuevas aplicaciones y paquetes de distribución en la carpeta Descargas. Analiza todos los archivos que el usuario abre, modifica, mueve, copia, ejecuta y guarda en el dispositivo. Bloquea el adware y las aplicaciones que pueden utilizar los criminales para dañar el dispositivo y los datos del usuario.
Protección con contraseña	Protege el acceso al dispositivo con una contraseña de desbloqueo de pantalla.
Protección antirrobo	Protege la información almacenada en el dispositivo contra el acceso no autorizado en caso de pérdida o robo. Bloquee y localice el dispositivo a distancia, active una alarma o borre los datos de forma remota.
Control de aplicaciones	Administre las aplicaciones de los dispositivos de los usuarios con un conjunto de reglas. Puede configurar dos tipos de reglas de control de aplicaciones: reglas de aplicaciones y reglas de categorías.

Control avanzado de cumplimiento normativo*	Comprueba que la configuración de los dispositivos de los usuarios cumpla los requisitos de seguridad corporativa. Por ejemplo, si el dispositivo está "liberado" (rooted) o tiene las bases de datos antivirus desactualizadas, se pueden configurar acciones de protección.
Control web	Bloquea el acceso a páginas web de phishing y maliciosas, y controla el acceso a las páginas web según su contenido y ubicación.
Modo Propietario del dispositivo con control avanzado de características*	Le permite bloquear el uso de la cámara y los módulos de Bluetooth y Wi-Fi en un dispositivo para minimizar el riesgo de filtración de datos confidenciales, así como configurar la conexión automática a una red Wi-Fi corporativa en Android.
Configuración de la red Wi-Fi	Define la configuración de la red Wi-Fi cuando el dispositivo se conecta a Internet.
Sincronización y actualización de bases de datos en itinerancia	Le permite sincronizar el dispositivo con el Servidor de administración y actualizar la base de datos antivirus mientras está en zona de itinerancia. Además, el usuario puede ejecutar estas funciones manualmente cuando así lo desee.
Detección de rooting	En un dispositivo pirateado, los archivos del sistema no están protegidos y se pueden modificar, y se podrían instalar en él aplicaciones de terceros procedentes de fuentes desconocidas. Al detectar un intento de obtener ingreso como usuario de dispositivo "liberado", se recomienda restablecer la operación normal del dispositivo inmediatamente.
Configuración del correo	Le permite configurar un buzón de Exchange para administrar el correo, los contactos y el calendario corporativos en su móvil.
Compatibilidad con KNOX/ Exchange ActiveSync (EAS)	La aplicación Kaspersky Endpoint Security for Android se puede instalar a través de la consola Samsung KNOX Mobile Enrollment. El protocolo Exchange ActiveSync se puede usar para configurar restricciones en las características del dispositivo, con el fin de garantizar la seguridad de un dispositivo EAS.
Compatibilidad avanzada con el perfil de trabajo de Android*	Le permite configurar un contenedor independiente (mediante el perfil de trabajo de Android) para sus apps y datos corporativos, con funciones adicionales de protección de datos para las apps instaladas en el perfil de trabajo, incluida la obligación de usar un código PIN independiente y la posibilidad de restablecerlo.
Integración de PKI*	Le permite configurar la conexión con su MS CA y transferir los certificados para el correo electrónico, la VPN y la autenticación Wi-Fi a los dispositivos móviles conectados.
Asistencia remota*	Permite a los administradores conectarse de forma remota a dispositivos Android para solucionar problemas y brindar asistencia técnica.
Geocercado*	Aplica restricciones basadas en la ubicación y permite el seguimiento de la ubicación del dispositivo y la visualización de la ruta en un mapa.
Administración de aplicaciones avanzada*	Permite optimizar la administración del ciclo de vida de las aplicaciones, incluida la instalación y la desinstalación automáticas, la configuración de aplicaciones (incluidas las del perfil de trabajo de Android), la administración de permisos de las aplicaciones y funciones ampliadas de Google Chrome en los dispositivos.
Modo quiosco*	Limita el uso de los dispositivos a una o varias aplicaciones autorizadas, para que los empleados solo puedan acceder a las apps autorizadas en sus dispositivos.
Administración de recortes web y fondos de pantalla*	Permite a los administradores administrar los fondos de pantalla de los dispositivos y crear clips web (atajos a aplicaciones web y sitios web) en los dispositivos de los usuarios.
Administración de la transferencia de archivos*	Permite la transferencia segura de archivos a los dispositivos, incluida la creación de directorios y la eliminación remota de archivos.
iOS	
Control web	Supervisa el acceso a sitios web dependiendo del contenido y de la ubicación. La configuración se aplica solo en dispositivos supervisados.

* De momento, solo está disponible para su implementación en las instalaciones

Protección anti-phishing y antimalware web	Protege los dispositivos iOS contra el phishing y el malware que puedan estar dirigidos a sus empleados.
Protección con contraseña	Protege el acceso al dispositivo con una contraseña de desbloqueo de pantalla.
Configuración del proxy	Protege el tráfico al conectar el dispositivo a Internet a través de un proxy HTTP global. La configuración se aplica solo en dispositivos supervisados.
Funcionalidad antirrobo	Las funciones de bloqueo y borrado remotos se pueden aplicar a un dispositivo robado para proteger la pérdida de datos.
Características avanzadas de administración*	Restringe el acceso del usuario a las funciones nativas del dispositivo iOS, como el control de la cámara, la instalación de apps, las capturas de pantalla, AirDrop, iCloud, etc. Admite políticas de restricción de dispositivos muy completas, aunque algunos controles solo están disponibles para los dispositivos supervisados.
Control de cumplimiento*	Comprueba que la configuración del dispositivo del usuario cumpla con los requisitos de seguridad corporativos y le permite configurar acciones de protección.
Administración del Modo perdido*	Activa el Modo perdido para evitar el acceso no autorizado, muestra un mensaje personalizado e información de contacto, desactiva temporalmente Apple Pay y rastrea la ubicación del dispositivo.
Modo quiosco*	Limita el uso de los dispositivos a una o varias aplicaciones autorizadas, para que los empleados solo puedan acceder a las apps autorizadas en sus dispositivos.
Administración de actualizaciones de iOS	Permite a los administradores programar o posponer las actualizaciones del sistema operativo iOS en los dispositivos administrados.
Configuración de la VPN	Permite a los administradores configurar el cliente VPN nativo de iOS y definir políticas de túnel de tráfico VPN para cada aplicación.
Administración de aplicaciones avanzada*	Permite instalar aplicaciones desde la App Store o mediante archivos IPA, y admite la configuración centralizada de las aplicaciones.
Omisión del bloqueo de activación	El bloqueo de activación es una característica de seguridad de iOS que impide que usuarios no autorizados utilicen o reactiven un dispositivo perdido o robado. Esta característica permite a los administradores autorizados desactivar el bloqueo de activación en dispositivos iOS supervisados mediante un código de desactivación, sin necesidad del Apple ID ni de la contraseña del usuario.
Configuración del nombre del punto de acceso	Configura el nombre del punto de acceso (APN) al conectarse a servicios de datos en una red móvil.
Configuración de AirPrint	Configura AirPrint para imprimir documentos desde el dispositivo.
Configuración de la red Wi-Fi	Define la configuración de la red Wi-Fi cuando el dispositivo se conecta a Internet.
Configuración del correo electrónico	Configura las cuentas de correo electrónico pertenecientes al usuario del dispositivo.
Configuración de CalDAV	Configura las cuentas CalDAV pertenecientes al usuario del dispositivo para gestionar el calendario.
Suscripciones a calendarios	Configura la suscripción a calendarios de terceros para agregar eventos al dispositivo.
Detección de jailbreak	Los archivos del sistema no están protegidos en un dispositivo pirateado y se pueden modificar. Al detectar un jailbreak, se recomienda restablecer de inmediato la operación normal del dispositivo.

* De momento, solo está disponible para su implementación en las instalaciones

Característica	Descripción
Visibilidad e investigación	
Tarjeta de alerta con análisis de causas raíz	**Descripción general de la tarjeta de alerta** Cada incidencia se abre y se rellena con información recolectada automáticamente después de detectar una actividad maliciosa o sospechosa en el dispositivo. La tarjeta de alerta la genera la consola de administración e incluye, entre otras cosas, la siguiente información: • Gráfico de propagación de amenazas con capacidad de desglose • Eventos de alerta (elementos registrados: detalles de archivos o procesos, información de URL, modificaciones del registro, etc.) • Información del host (nombre, dirección IP, dirección MAC, lista de usuarios, función de controlador de dominio del sistema operativo, etc.) • Información general sobre las detecciones, incluido el modo de detección (ODS/OAS/AMSI/al ejecutar, etc.) • Cambios en el registro, detección de ejecución automática • Estado de la respuesta (por ejemplo, en cuarentena, desinfectado) • Datos sobre el archivo, como el nombre y la ruta, el hash MD5/SHA256, el historial de versiones, etc. La mayoría de las acciones de investigación y respuesta se llevan a cabo en esta tarjeta de alerta. **Descripción general del análisis de causas raíz** Esta sección, situada en la parte superior de la tarjeta de alerta, incluye el gráfico de propagación de amenazas, que muestra los procesos clave, las conexiones de red, las DLL y las ramas del registro afectadas por la alerta o relacionadas con ella. Todas las detecciones aparecen resaltadas en el gráfico, lo que les ofrece a los analistas un contexto completo del incidente y facilita el proceso de identificar qué componentes se han visto afectados. El gráfico permite profundizar en los datos y ofrece información adicional sobre los procesos, etc. Todos los datos relacionados con las alertas que se hayan recolectado se pueden ordenar por grupo (procesos, registro, conexiones, etc.) o por lista.
Información de inteligencia de amenazas	La reputación de un archivo de nuestro Kaspersky Threat Intelligence Portal está integrada en la tarjeta de alerta para analizar las causas raíz de forma más rápida y precisa. La información disponible incluye: • Estado en Kaspersky Security Network • Número de usuarios de KSN que han interactuado con este archivo • Distribución geográfica de los usuarios de KSN afectados por el archivo • Fecha de primera detección del archivo Para obtener detalles adicionales sobre el archivo detectado, acceda al enlace integrado del Portal de Inteligencia de Amenazas de Kaspersky (versión gratuita o de pago).
Indicadores de compromiso (IoC)	
Enfoque reactivo	Los indicadores de amenaza (IoC) para una alerta concreta, o para un archivo que aparezca en el gráfico de propagación de amenazas, se pueden generar automáticamente y se puede iniciar un análisis de IoC basado en ese indicador. La lista de indicadores se genera a partir de los datos recolectados para la alerta correspondiente y se la muestra al responsable de seguridad para que tome medidas adicionales, como buscar un incidente similar en otros hosts o activar una respuesta automática en todos los endpoints. La lista de IoC se encuentra en la tarjeta de alerta. Busque incidentes similares analizando la infraestructura mediante los IoC generados automáticamente por el sistema. El usuario puede seleccionar los indicadores antes de que comience el proceso de análisis. Si se utilizan varios IoC, el usuario puede configurar reglas lógicas para la detección. El usuario también puede configurar acciones de respuesta automáticas al ejecutar análisis de IoC (consulte la sección Respuesta más abajo).

Enfoque proactivo	Para facilitar el trabajo de los responsables de seguridad a la hora de identificar los IoC, se pueden subir al sistema IoC de terceros en formato OpenIOC (por ejemplo, de cualquier proveedor de inteligencia sobre amenazas, organismo regulador u otro origen, como securelist.com). La búsqueda se ejecuta mediante indicadores de amenazas asociados a archivos, (hashes criptográficos) Kaspersky puede compartir la lista de términos de OpenIOC compatibles. Se realizan comprobaciones de validez de los términos de IoC para garantizar que la sintaxis sea correcta y que haya compatibilidad total al importar el archivo o la lista de archivos. Tenga en cuenta que, en Pro View, para añadir un IoC hay que pegar el hash del archivo en un simple cuadro de texto. En Expert View, se debe crear o modificar un archivo OpenIOC ya existente (formato XML).
Análisis de IoC: análisis programado	El escaneo por IoC en la infraestructura de endpoints se ejecuta según una programación definida. El proceso de análisis ocurre directamente en los endpoints y se comprueba su estado actual.
Exportación de IoC	Los archivos generados automáticamente relacionados con la alerta se pueden exportar y guardar en formato OpenIOC.

Respuesta

Orientación de respuesta	La tarjeta de alerta tiene una sección con recomendaciones de respuesta. Las acciones recomendadas se presentan en forma de instrucciones paso a paso con enlaces en los que se puede hacer clic y que indican dónde se puede realizar cada acción. Esto le permite al usuario aprender rápidamente a utilizar la solución y contar con orientación en caso de una amenaza urgente y de rápida evolución.
Respuesta con un solo clic	Las acciones de respuesta rápida reducen los tiempos de respuesta de horas a minutos y disminuyen la cantidad de tareas manuales rutinarias gracias a una amplia gama de acciones de respuesta automatizadas. La mayoría de las acciones de respuesta están disponibles en la tarjeta de alerta o en el desglose del gráfico de propagación de la amenaza, y se pueden llevar a cabo con solo unos clics. En la tarjeta de alerta, hay varias acciones de respuesta disponibles en forma de botones independientes: **Impedimento de ejecución** El objeto se añade a la lista de bloqueados. La tarea se puede llevar a cabo en toda la infraestructura de endpoints. **Aislamiento de host** El host actual o remoto pueden aislarse del resto de la red para evitar que la amenaza se propague aún más. En este caso, se mantiene la conexión con la consola de administración. Se pueden configurar reglas personalizadas de exclusión para el aislamiento de hosts (por ejemplo, añadiendo recursos de red específicos a las exclusiones, como DNS, o seleccionando perfiles predefinidos). **Poner archivo en cuarentena** Trasladar un objeto al repositorio especial destinado a guardar objetos sospechosos. Los archivos en cuarentena se guardan en el dispositivo protegido de forma cifrada y, por lo tanto, no ponen en riesgo la seguridad del dispositivo. Disponible en Expert View.
Respuesta de la consola	Hay algunas acciones de respuesta que están disponibles fuera de la tarjeta de alerta, que incluyen, entre otras: **Agregar a la lista de permitidos** Inclusión del objeto en la lista de permitidos mediante las funcionalidades de Protección de endpoints y Gestión de sistemas desde la consola de administración. **Obtener archivo** Permite al responsable de seguridad recuperar archivos de los dispositivos de los usuarios. Por ejemplo, puede configurar la obtención de un archivo de registro de eventos creado por una aplicación de terceros. Al terminar la tarea, el archivo se guarda en Cuarentena. Puede descargar este archivo desde Cuarentena a su dispositivo a través de la consola de administración. En el dispositivo del usuario, el archivo se queda en su carpeta original.

	Eliminar archivo Los objetos se pueden eliminar de forma remota de un solo endpoint o un grupo de hosts. **Iniciar proceso** Cualquier software adicional se puede ejecutar de forma remota en el host. **Terminar el proceso** Detener la ejecución de procesos sospechosos: se puede cerrar cualquier proceso de forma remota en un dispositivo, para contener la amenaza en ese dispositivo y bloquear en tiempo real los intentos de filtración de datos y de movimiento lateral.
Respuesta automática entre endpoints con análisis de IoC	Los indicadores de amenaza (IoC) para una alerta concreta, o para un archivo que aparezca en el gráfico de propagación de amenazas, se pueden generar automáticamente y se puede iniciar un análisis de IoC basado en ese indicador. Estas acciones de respuesta incluyen lo siguiente: **Aislamiento de host** Consultar la información arriba mencionada **Análisis de áreas críticas** Análisis de áreas críticas con la función de Protección de endpoints. Solo disponible durante el análisis de IoC. **Poner archivo en cuarentena** Consultar la información arriba mencionada
Verificación de objetos vitales del sistema	Si se ejecutan ciertas acciones de respuesta, como Terminar proceso o Eliminar archivo, sobre un objeto legítimo que sea esencial para el funcionamiento del sistema, dicha acción se bloqueará para no afectar al funcionamiento normal del sistema. Este ajuste se puede cambiar en el grupo de opciones Reglas de prevención.
Recuperación	
Recuperar archivo de la cuarentena	Cualquier objeto que esté en Cuarentena se puede recuperar y volver a instalar en el dispositivo en cualquier momento.
Eliminar el aislamiento de red	El responsable de seguridad puede habilitar los hosts aislados en la red. Se puede configurar el tiempo de espera de las reglas de aislamiento. Por ejemplo, esta acción se puede realizar con un botón de la tarjeta de alerta, una vez que hayan finalizado la investigación y la respuesta.

Seguridad en la nube y protección del correo electrónico

Característica	Descripción
Detección de uso de nubes	Permite detectar y restringir el consumo de recursos de nube inapropiado o no autorizado, además del tiempo en redes sociales y aplicaciones de mensajería. Supervisa más de 2.700 servicios de nube. Ahora, cada servicio en la nube detectado tiene una puntuación que indica lo peligroso que es utilizarlo, lo que facilita a los administradores evaluar los posibles riesgos y decidir si permiten o bloquean determinado servicio.
Cloud Blocking	Bloquee el acceso de usuarios a recursos de nube, redes sociales o aplicaciones de mensajería inapropiadas o no autorizadas.
Data Discovery	El descubrimiento de datos en tiempo real otorga visibilidad inmediata y control sobre información confidencial (texto o imágenes) en Exchange Online, SharePoint Online, OneDrive y Teams.
Protección avanzada para correo electrónico	Protección avanzada para el servicio de correo de Microsoft 365 mediante sólidas funciones antiphishing, antispam y antimalware, así como de autenticación de remitentes y otras tecnologías.

Funcionalidades y módulos de formación en cultura de seguridad

Característica	Descripción
Campañas de phishing simuladas	Comprueba si los empleados están preparados para hacer frente a los ciberataques mediante simulaciones realistas de phishing que reflejan las amenazas actuales. Incluye plantillas personalizables, que abarcan desde opciones de solo clic y basadas en archivos adjuntos hasta páginas de destino personalizadas, además de análisis detallados sobre el nivel de preparación ante el phishing. Asigna automáticamente la formación en función de los resultados de las simulaciones, lo que convierte los clics de los empleados en aprendizaje y, al mismo tiempo, ofrece información sobre los riesgos para medir la mejora de la cultura de seguridad a lo largo del tiempo.
Formación en ciberseguridad para especialistas de TI	Esta formación en línea les proporciona a los especialistas de asistencia técnica, a los administradores de sistemas y a los miembros no especializados del equipo de TI las habilidades prácticas necesarias para detectar ciberataques ocultos en los incidentes cotidianos de las computadoras y recolectar datos relevantes para pasárselos al equipo de seguridad de TI. Los módulos incluyen teoría, consejos prácticos y ejercicios sobre seis temas: software malicioso, conceptos básicos de investigación, programas potencialmente no deseados y exploits, seguridad de servidores, phishing e inteligencia de código abierto, y seguridad de Active Directory.

Tenencia múltiple

El modo operativo multitenencia permite que la solución proteja la infraestructura de varias organizaciones desde una única implementación. En Kaspersky Next EDR Foundations, permite a los proveedores de servicios gestionados (MSP) ofrecer protección gestionada de endpoints como servicio. La consola multicliente, muy fácil de usar, le permite administrar varios clientes desde una sola cuenta. Admite hasta 300 usuarios en espacios de trabajo independientes y aislados, cada uno con su propio perfil de seguridad basado en las mejores prácticas.

Dispositivos y sistemas operativos compatibles

	Windows	macOS	Linux	iOS	Android
Disponible para					
Requisitos del sistema	Más información	Más información	Más información	Más información	Más información

Característica	Pro view	Expert View en la nube	Expert View en las instalaciones
Protección de endpoints			
Detección del comportamiento	✓	✓	✓
Prevención de exploits	✓	✓	✓
Control de anomalías adaptable*	✓	✓	✓
Motor de remediación	✓	✓	✓
Protección contra amenazas de archivo	✓	✓	✓
Protección contra amenazas de correo	✓	✓	✓
Protección contra amenazas web	✓	✓	✓
Firewall	✓	✓	✓
Prevención de intrusiones basada en host (HIPS)*	✓	✓	✓
Protección contra amenazas de red	✓	✓	✓
Prevención de ataques BadUSB	✓	✓	✓
Protección AMSI	✓	✓	✓
Kaspersky Security Network	✓	✓	✓
Defensa contra amenazas móviles	✓	✓	✓
Integración de SIEM		●	●
Integración de EMM		●	●
Reforzamiento del sistema			
Evaluación de vulnerabilidades	✓	✓	✓
Administración de parches	✓	✓	✓
Administración del cifrado	✓	✓	✓
Control de aplicaciones	✓	✓	✓
Control web	✓	✓	✓
Control de dispositivos	✓	✓	✓
Borrado remoto	✓	✓	✓
Administración de dispositivos móviles (MDM)	✓	✓	✓
Resolución de problemas remota		✓	✓
Instalación de sistemas operativos y aplicaciones			✓
Inventarios de hardware y software		✓ Linux: solo inventario de software	✓ Linux: solo inventario de software
Formación sobre ciberseguridad			
Formación en ciberseguridad para especialistas de TI	●	●**	●**

Característica	Pro view	Expert View en la nube	Expert View en las instalaciones
Seguridad para nubes			
Detección de uso de nubes	●	●	●**
Cloud Blocking	●	●	●**
Data Discovery	●	●**	●**
Seguridad para Microsoft Office 365	●	●**	●**
EDR esencial: visibilidad e investigación			
Tarjeta de alerta con análisis de causas raíz	Windows	Windows, macOS, Linux	Windows, macOS, Linux
Información de inteligencia de amenazas	Windows	Windows, macOS, Linux	Windows, macOS, Linux
EDR esencial: indicadores de compromiso (IoC)			
Enfoque reactivo	Windows	Windows, macOS, Linux	Windows, macOS, Linux
Enfoque proactivo	Windows	Windows, macOS, Linux	Windows, macOS, Linux
Análisis de IoC: análisis programado	Windows	Windows, macOS, Linux	Windows, macOS, Linux
Exportación de IoC		Windows, macOS, Linux	Windows, macOS, Linux

* No disponible para servidores

** Si está usando Expert View en la nube, puede cambiar a Pro View y usar esta función allí

Descubra otras soluciones de Kaspersky Next

Más información

latam.kaspersky.com

© 2026 AO Kaspersky Lab.
Las marcas comerciales registradas y las marcas de servicio pertenecen a sus respectivos propietarios.

#kaspersky
#truetobusiness