kaspersky PREPARADOS PARA EL FUTURO

EDR: Guía del comprador

Todo lo que necesita saber para obtener una protección EDR optima para su empresa

Resumen ejecutivo

Durante años, las pymes y las empresas medianas han podido confiar en su plataforma de protección de endpoints (EPP) para defender a sus empresas de una amplia variedad de amenazas básicas. Sin embargo, debido a que los cibercriminales recurren cada vez más a amenazas nuevas, desconocidas y evasivas que pueden eludir el EPP, es momento de actualizar estas defensas con soluciones de detección y respuesta en endpoints (EDR, por sus siglas en inglés) o de detección y respuesta gestionadas (MDR, por sus siglas en inglés) capaces de proteger contra dichas amenazas.

En esta guía del comprador se explica cómo identificar la seguridad de clase EDR óptima para su empresa en ocho sencillos pasos. Deberá comenzar por revisar la protección de sus endpoints existente para identificar cualquier brecha importante en sus defensas para endpoints. También deberá tener claro lo que desea lograr e identificar la protección que mejor se adapte a sus necesidades teniendo en cuenta sus casos de uso. Además, debe analizar seriamente el MDR y el EDR, considerar estas soluciones en su entorno de seguridad más amplio y obtener una lista de las capacidades clave necesarias de los posibles proveedores.

Al leer esta guía, comprenderá claramente por qué y cómo actualizar sus defensas, las ventajas de las soluciones disponibles y cómo crear una solución de seguridad óptima que no solo se adapte a las necesidades de su empresa, sino también a las habilidades de seguridad especializadas de su equipo de IT.

¿Por qué mejorar sus defensas y por qué ahora?

Las soluciones avanzadas de ciberseguridad, como la detección y la respuesta en endpoints (EDR), son uno de los temas más importantes del mercado y por un buen motivo. Especialmente si la suya es una pequeña o mediana empresa (pyme).

¿Por qué estos segmentos en particular? Los cambios en el panorama de la ciberseguridad implican que los atacantes, en la actualidad, se están centrando en organizaciones de todos los tamaños, ámbitos de actividad y niveles de preparación. Más concretamente, las pymes de gama alta y las empresas de tamaño mediano se encuentran en el punto de mira de amenazas evasivas más avanzadas previamente dirigidas solo a organizaciones mucho más grandes.

Como respuesta, los equipos de seguridad de IT han complementado sus plataformas de protección de endpoints (EPP) existentes con soluciones de EDR o de detección y respuesta gestionadas (MDR), lo que les permite detectar e investigar incidentes de seguridad, contener la amenaza en el endpoint y recibir una respuesta automatizada o una guía para solucionar el problema.

Lamentablemente, la adopción de estas soluciones a veces puede causar tantos problemas como los que resuelve, al alertar a los equipos de seguridad de enormes volúmenes de amenazas, que, aunque sean sospechosas y requieran investigación, finalmente resultan inofensivas. Este puede ser un problema en particular para los equipos de IT con limitaciones en la experiencia en seguridad interna o en el tiempo con el que lidiar con estas alertas.

Optimice los recursos clave y céntrese en el negocio de la ciberseguridad, en lugar de perseguir los falsos positivos y los abrumadores volúmenes de alertas

Por lo tanto, la solución ideal es la que complementa la protección de endpoints con una seguridad EDR que aligera significativamente la carga de trabajo de EDR, dado que cuantas más amenazas se prevengan, menor será el ruido creado que deberán investigar los equipos de seguridad. Esto, a su vez, significa que los equipos de seguridad de IT pueden optimizar los recursos clave y centrarse en el negocio de la ciberseguridad, en lugar de perseguir falsos positivos y enormes volúmenes de alertas.

Entonces, ¿qué cambios en el panorama de amenazas están impulsando la necesidad de una protección más avanzada? ¿Cómo varían dichos cambios para los diferentes tipos de empresas? Y (quizás lo más crítico de todo, debido a la escasez global de talentos en ciberseguridad), ¿cómo puede abordar estas amenazas de manera eficaz con una solución que se adapte mejor a su organización, al tamaño y a las habilidades de seguridad de su equipo de IT y a los tipos de ciberataques a los que está potencialmente expuesto?

Esta guía del comprador le ayudará, al describir:

- Por qué la seguridad de endpoints existente no garantiza la protección contra el nuevo panorama de amenazas.
- Cómo evaluar sus requisitos de seguridad en evolución.
- Cómo identificar la protección que mejor se adapte a sus necesidades, tanto en términos de las amenazas a las que está cada vez más expuesto como las habilidades de seguridad de su equipo de IT.
- Qué hacer si solo tiene tiempo, personal o experiencia en seguridad interna limitados.
- Cómo encajan las soluciones más recientes en el panorama de seguridad más amplio.

Por qué la seguridad de endpoints existente no garantiza la protección contra el nuevo panorama de amenazas

Cuando se trata de mejorar la seguridad de sus endpoints, es fácil pensar que se trata simplemente de identificar e implementar una solución EDR que parezca una buena opción para su empresa. Sin embargo, de la misma manera en que no sería aconsejable añadir una planta adicional a un edificio sin antes revisar los cimientos, su primer paso debe ser revisar la EPP existente.

IDC[1], por ejemplo, ha sugerido:

- Antes de analizar las consideraciones para el EDR, IDC recomienda que primero analice su solución de EPP existente. La expectativa para el EPP debe ser que proteja los endpoints como una solución independiente.
- No acepte un EPP de calidad inferior o insuficiente ya que dañará los resultados de toda la solución de endpoint. Una empresa no debe compensar un EPP insuficiente con EDR (y mucho tiempo de analistas de seguridad).

No acepte un EPP de calidad inferior o insuficiente ya que dañará los resultados de toda la solución de endpoint[1]. Una empresa no debe compensar un EPP insuficiente con EDR (y mucho tiempo de analistas de seguridad).

El EPP juega un papel vital a la hora de permitir que cualquier empresa se proteja contra una amplia gama de amenazas básicas y minimice las cargas de trabajo de seguridad de IT. Pero cuando se trata de amenazas evasivas, necesita ir más lejos.

Para reducir los riesgos que presenta el nuevo panorama de amenazas, por lo tanto, debe comenzar por evaluar la eficacia de su protección de endpoints existente e identificar posibles brechas en sus defensas.

Por qué es posible que no esté tan protegido como piensa

Si bien es posible que piense que su empresa está bien protegida, se estima que solo en el primer semestre de 2019 hubo casi **4000** robos de datos[2], poniendo en riesgo más de cuatro mil millones de datos de usuarios.

Esta cifra alarmante aparece en la introducción a la economía de la seguridad de IT en 2019, el informe de Kaspersky que resume los resultados de nuestra Encuesta de riesgos globales de seguridad de IT empresarial anual. La encuesta incluyó entrevistas con casi 5000 pymes y grandes empresas de 23 países, y reveló algunas estadísticas propias preocupantes. Por ejemplo:

55 %

de las organizaciones están "completamente seguras" de que su red no ha sido pirateada, a pesar de que el 38 % siente que carecen de suficientes conocimientos sobre las amenazas a las que se enfrenta su empresa.

12 %

de las empresas están preocupadas por la infección de malware, a pesar de que sea el incidente de seguridad más costoso para ellas.

51 %

de las empresas y el 47 % de las pymes están de acuerdo en que es cada vez más difícil distinguir entre un ataque de seguridad genérico o dirigido.

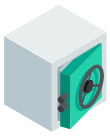
66 %

tanto de las empresas como de las pymes estaban buscando aumentar su inversión en personal especializado de IT en 2020, a pesar de la escasez global crítica, sobre todo en ciberseguridad.

1 IDC Doc # US45794219 - Seguridad de endpoints 2020: el resurgimiento de la EPP y el destino manifiesto de la EDR, enero de 2020

2 https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

Lo que estas cifras sugieren es una peligrosa desconexión entre las percepciones de las organizaciones sobre el panorama de las ciberamenazas, los tipos de ataques que plantean los mayores riesgos potenciales (incluidos los financieros) y su preparación y capacidad para defenderse.



Para las empresas, la infección por malware en los dispositivos propiedad de la empresa es, en realidad, la forma de robo de datos con el mayor impacto financiero, con un coste de **2,73 millones de dólares** en 2019, a pesar de que solo el 12 % de las empresas sentía una "gran preocupación" por la infección por malware como una amenaza.

Las pymes también ignoran sus formas de ataque más costosas. El tipo más costoso de robo de datos para pequeñas empresas fue el de incidentes que afectaban la infraestructura de IT alojada por un tercero, que ascendió hasta **162 000 dólares**. Sin embargo, las pymes solo clasificaron esta medida como la quinta más importante; estaban más preocupadas por los problemas de protección de datos, como la pérdida de un dispositivo físico o la pérdida de datos a través de un ataque dirigido.

El hecho de que a las empresas y a las pymes les resulte más difícil distinguir entre los ataques de seguridad genéricos y dirigidos, hace que les resulte más difícil detectar o evaluar el daño potencial de los incidentes que están experimentando, una posible razón por la que se están volviendo susceptibles a niveles cada vez mayores de amenazas de malware, tanto moderadas como avanzadas.

El informe concluyó diciendo que "es de vital importancia que las empresas sigan invirtiendo y reconsiderando sus procesos de seguridad de IT con el fin de mantenerse un paso por delante de las crecientes tasas de ciberataques y limitar las pérdidas financieras en las que se incurre". Sin embargo, solo pueden lograrlo si abordan de manera eficaz las amenazas reales a las que están cada vez más expuestas, es decir, si invierten en la seguridad de clase EDR necesaria para protegerse contra amenazas evasivas.

Paso 1: Revisar su protección de endpoints existente

Con tantas soluciones avanzadas de ciberseguridad disponibles en el mercado, es fácil olvidar el papel fundamental que cumple su protección para endpoints. ¿Por qué son tan importantes los endpoints? No solo son los puntos de entrada más comunes a la infraestructura de una organización (y el objetivo principal de los cibercriminales), sino que también son las fuentes clave de los datos necesarios para una investigación eficaz sobre incidentes complejos.

Como resultado, cada organización debe elegir un EPP que proporcione protección automatizada contra el gran número de posibles incidentes provocados por las amenazas básicas, incluidas las amenazas sin archivos y el ransomware.

Debido a que este tipo de configuración requiere personal o conocimientos de seguridad especializados relativamente limitados, satisface las necesidades de seguridad de endpoints de pequeñas y medianas empresas sin un equipo de seguridad especializado, o de organizaciones con muy bajos niveles de experiencia en ciberseguridad.

También es una etapa fundamental para empresas medianas y grandes donde, al abordar automáticamente una gran cantidad de amenazas menores, la solución puede despejar el camino para que los equipos de seguridad se centren en una defensa más avanzada cuando sea necesario.

Cuando revise su EPP para evaluar si está ofreciendo las capacidades previstas, debe considerar lo siguiente:

¿Qué nivel de eficacia tiene?

¿Cuántos falsos positivos recibe usted?

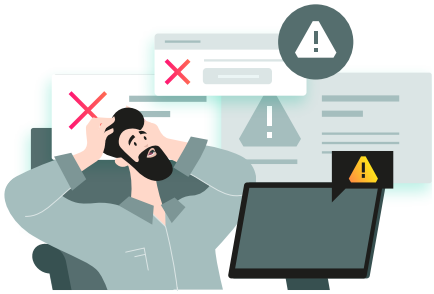
¿Ofrece capacidades eficaces de reducción de la superficie de ataque como controles de sitios web, aplicaciones y dispositivos?

¿Ayuda a automatizar las tareas rutinarias?

¿Es fácil de utilizar y ayuda a minimizar los costes y los gastos generales de su equipo de IT?

¿Ayuda con tareas críticas como la evaluación de vulnerabilidades y la gestión de parches?

Paso 2: Identificar cualquier brecha crítica en sus defensas para endpoints



Si bien su EPP va a proteger frente a una amplia variedad de amenazas básicas, también debe considerar su defensa contra amenazas nuevas, desconocidas y evasivas que están eludiendo su EPP.

Preparar un ataque cada vez es más barato para los cibercriminales, lo que pone más organizaciones en riesgo. Además de volverse más frecuentes, estos tipos de ataques son ahora mucho más eficaces debido a la combinación, las pruebas y el uso de técnicas variadas por parte de los criminales, con el fin de eludir eficazmente la seguridad de los endpoints.

La urgente necesidad de hacer frente a estas amenazas también se ha vuelto cada vez más crítica debido a los cambios, como la disolución de los perímetros corporativos provocados por el teletrabajo.

Por lo tanto, las señales inequívocas que apuntan a que es el momento de ampliar sus defensas más allá de los EPP tradicionales incorporan:

- Su EPP no logra frenar un número cada vez mayor de amenazas nuevas, desconocidas y evasivas.
- Tiene una visibilidad limitada de lo que está sucediendo en sus endpoints. Esto incluye no poder llevar a cabo el análisis de la causa raíz, la investigación y la respuesta a amenazas en tiempo real, o tener que hacerlo manualmente, con herramientas de sistema operativo estándar (SO) caso a caso, que son lentas, complejas y propensas a errores.
- No cuenta con las habilidades ni la capacidad de seguridad de IT especializada necesarias para hacer frente a amenazas cada vez más sofisticadas.
- Está preocupado por posibles multas o la amenaza a la reputación de su empresa como resultado de un incidente de seguridad importante.

El mejor uso de todas las funciones que realmente necesita, en lugar de pagar una gran cantidad de funciones que realmente no desea

Para implementar una solución eficaz con el fin de defenderse contra estas amenazas, deberá considerar aspectos de su organización, como su tamaño, perfil corporativo, preparación en materia de seguridad, recursos y experiencia existentes y, en particular, el nivel de conocimientos de seguridad (o "madurez") de su IT o de su equipo de seguridad de IT.

También querrá una solución que haga el mejor uso de todas las funciones que realmente necesita, en lugar de pagar una gran cantidad de funciones que realmente no desea, y luego tener que tratar de contratar a expertos en seguridad de IT con las habilidades necesarias para trabajar con ellas.

Paso 3: Tener claro lo que se desea lograr

Según Gartner[3], las herramientas de EDR proporcionan un método para que los profesionales técnicos en materia de seguridad y gestión del riesgos respondan dos preguntas clave sobre la seguridad de su entorno:

- ¿Qué ha sucedido aquí?
- ¿Qué está sucediendo en este momento?

Muchas organizaciones tienen experiencia limitada (o un departamento de seguridad de IT pequeño y no tienen planes de ampliarlo), pero deben comprender lo que sucede en su infraestructura y ser capaces de responder a amenazas evasivas antes de que se produzca el daño.

Agregar las capacidades apropiadas de EDR al EPP puede proporcionar una defensa altamente eficaz contra amenazas más avanzadas y evasivas. Esto debería proporcionar a los especialistas en seguridad de IT la información y los conocimientos necesarios para una investigación eficaz, así como las herramientas necesarias para el análisis de la causa raíz, la creación de indicadores de compromiso (IoC) personalizados, la importación de IoC y el análisis de los mismos en todos los endpoints. Además, debe permitir respuestas automáticas, rápidas y precisas con un solo clic, como la puesta en cuarentena de archivos, el aislamiento de hosts, la detención de un proceso, la eliminación de un objeto, etc.

Paso 4. Identificar la protección que mejor se adapte a sus necesidades

Es posible que muchas organizaciones no tengan contratado a nadie dedicado específicamente a la seguridad de IT. Puede que algunas estén comenzando a crear su departamento de seguridad de IT. Y puede que otras ya hayan formado y cualificado equipos de seguridad de IT. Por lo tanto, la calidad de la experiencia disponible de estas organizaciones en relación con las defensas contra amenazas variará ampliamente, al igual que la cantidad de tiempo que pueden dedicar a esta tarea.

Para hacer frente a estas diferentes circunstancias, organizaciones sin personal dedicado a la seguridad de IT o aquellas cuyo personal de seguridad de IT está sobrecargado con tareas rutinarias, deberán utilizar de manera estratégica la automatización para hacer frente a las amenazas evasivas más recientes.

Esto significa complementar su EPP con herramientas EDR adicionales que, a la vez que protegen contra estas amenazas, también incorporan niveles adecuados de automatización (total o parcial).

3 Gartner: Comparación de soluciones para tecnologías y soluciones de detección y respuesta en endpoints, enero de 2020

Herramientas que son lo más sencillas y claras posible: ahorre tiempo y reduzca la frustración

De manera alternativa, en lugar de invertir en una solución EDR demasiado compleja para la que es posible que no tengan el tiempo o las habilidades necesarios, la detección y la respuesta gestionadas (MDR, por sus siglas en inglés) les permite acceder a capacidades como la supervisión de seguridad ininterrumpida por parte de expertos del sector, la búsqueda automatizada y gestionada de amenazas y escenarios de respuesta guiados y remotos, ya sea de un proveedor, de un proveedor de servicios gestionados (MSP) o de un proveedor de servicios de seguridad gestionados (MSSP).

Una tercera opción es combinar EDR y MDR. Muchas organizaciones no cuentan con la experiencia necesaria para la búsqueda de amenazas, por lo que la externalización al tiempo que se implementan las capacidades de detección y respuesta en la empresa es a menudo una solución perfecta. Esto puede ser particularmente beneficioso para las empresas que quieran desarrollar su propio equipo de ciberseguridad, pero que carecen de los recursos, el personal o las habilidades para respaldar una detección y respuesta especializadas.

Sea cual sea la opción que mejor se adapte a su situación particular, querrá herramientas que sean lo más sencillas y claras posible, lo que le ahorrará tiempo y frustración. Para minimizar la fatiga de las alertas, también querrá una solución que se encargue automáticamente de una gran cantidad de posibles amenazas.

Paso 5: Pensar en sus casos de uso

Para identificar la protección que mejor se adapte a sus necesidades, debe establecer requisitos claros. Esto significa que hay que tener en cuenta los aspectos críticos del rendimiento y el uso habitual de la solución, como los casos de uso que necesita que cumpla y los resultados que espera de ella.

Por ejemplo, cuando reciba una alerta de seguridad, EDR o MDR deben permitirle responder preguntas clave como:

¿Cuál es el contexto de la alerta?

¿Qué acciones se han realizado ya ante la alerta?

¿Sigue activa la amenaza detectada?

¿Se ha atacado a otros hosts?

¿Qué camino llevó el ataque?

¿Cuál es la causa raíz de la amenaza?

También debería ayudarle a comprender el alcance total de la amenaza. Por ejemplo:

Si corre el riesgo de una amenaza global, es probable que su equipo de gestión quiera estar seguro de que no está siendo víctima de un ataque, para lo que necesitará la capacidad de encontrar un indicador de compromiso (IOC) en línea, ejecutar un análisis y responder correctamente a sus preocupaciones.

Si una autoridad reguladora le pide que realice un análisis para un IOC específico, debe poder importar IOC de fuentes de confianza y ejecutar análisis periódicos para detectar indicios de un ataque.

Si ha investigado a fondo una alerta y ha generado un IOC basado en la amenaza descubierta, en lugar de ejecutar análisis en toda la red para buscar si otros hosts se han visto afectados, esto se debería hacer automáticamente.

De igual forma, debería ser capaz de responder rápidamente a amenazas prolíficas y de propagación rápida mediante:

- Contención de la amenaza aislando al host, poniendo en cuarentena el archivo o impidiendo la ejecución de archivos durante la investigación.
- Respuesta automática de endpoints cruzados basada en análisis de IOC, que le permite responder a amenazas evasivas en cuanto se descubren.
- Y, lo que es más importante, escenarios de respuesta guiada y remota si está usando MDR.

Los resultados clave que debe esperar de su solución son los siguientes:

- Protección contra las amenazas evasivas más frecuentes y que más interrupciones generan.
- Ahorro de tiempo y recursos con una herramienta sencilla y automatizada.
- Visión del alcance completo de las amenazas evasivas en toda su red.
- Comprensión de la causa raíz de cada amenaza y cómo ocurrió realmente.
- Elusión de daños adicionales con una respuesta automática rápida.

¿Qué hacer si solo tiene experiencia en seguridad interna limitada?

Supongamos que tiene experiencia interna limitada en seguridad de IT o un pequeño equipo de uno o dos especialistas en seguridad. Supongamos también que está intentando decidir si debe complementar su EPP con EDR o MDR. ¿Qué tipo de beneficios puede esperar y qué sería lo adecuado para usted?

Paso 6: Examinar con detalle el EDR y el MDR

Si prefiere un enfoque más práctico (y su equipo de IT tiene habilidades de seguridad de IT suficientemente desarrolladas), la EDR puede ayudar a prevenir las interrupciones de la actividad y los daños al negocio mediante la eliminación de los riesgos que representan amenazas nuevas, desconocidas y evasivas; además, proporciona al personal de seguridad la visibilidad necesaria para la investigación de amenazas, el análisis de la causa raíz y la respuesta.

Con ello se puede lograr impulsar la eficiencia de los costes al permitir que su equipo de seguridad trabaje de manera más eficaz sin tener que hacer malabares con múltiples herramientas y consolas, y maximizar la capacidad mediante la automatización de una amplia variedad de procesos. También le da tranquilidad, ya que le facilita la supervisión y la detección de amenazas, además de responder a ataques y prevenirlos.

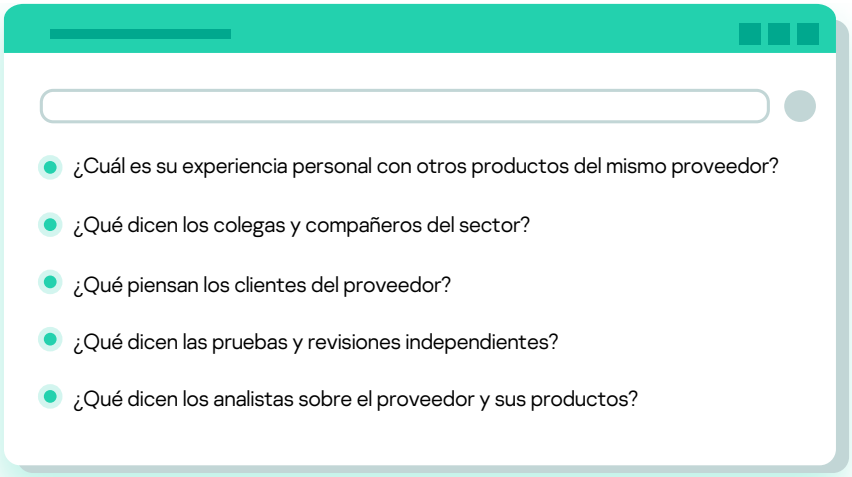
Si busca ampliar su capacidad de seguridad de IT interna mediante la descarga de tareas clave de respuesta y de detección, el MDR puede ofrecer protección avanzada las 24 horas del día contra amenazas que, de otro modo, podrían eludir barreras de seguridad automatizadas. Esto puede ayudar a potenciar su negocio resolviendo la crisis de talento de ciberseguridad y proporcionando todos los beneficios importantes de un centro de operaciones de seguridad (SOC) de forma ininterrumpida, sin costes prohibitivos.

La MDR también puede impulsar la eficiencia de los costes al permitir que los recursos internos se centren en las tareas críticas que realmente exigen la participación de su equipo de seguridad de IT y maximizando la capacidad al aprovechar los modelos de aprendizaje automático avanzados para aumentar significativamente el rendimiento de los analistas y minimizar el tiempo promedio de respuesta. Además, puede ofrecer supervisión continua de la seguridad por parte de expertos del sector, junto con una búsqueda automatizada y gestionada de amenazas. Esto incluye el análisis de amenazas complejas, no relacionadas con el malware, y de amenazas peligrosas y difíciles de detectar que utilizan herramientas legítimas del sistema operativo en los ataques.

La combinación de EDR y MDR le permite adaptar sus respectivas capacidades de clase EDR a sus necesidades particulares, por ejemplo, mediante la externalización de la búsqueda de amenazas (para lo cual es posible que no tenga la experiencia necesaria) mientras implementa las capacidades de detección y respuesta en endpoints en la empresa.

¿Qué sucede con el panorama general?

Una vez que haya establecido sus preferencias por EDR o MDR, también tendrá que evaluar cómo ve el mercado las diversas soluciones disponibles. Cuando busca un producto tan crucial como es la ciberseguridad, las opiniones de expertos independientes y de usuarios existentes deben superar cualquier reclamo de marketing de un posible proveedor. Por ejemplo:



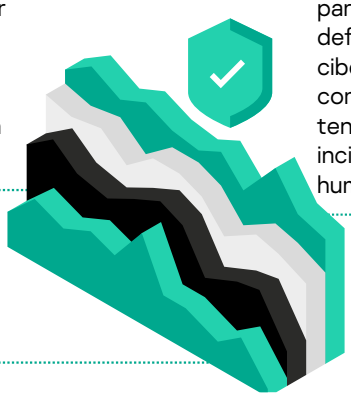
Paso 7: Considerar su panorama de seguridad más amplio

En muchas organizaciones, las soluciones EPP, EDR o MDR tendrán que integrarse y funcionar como parte de un marco de seguridad mucho más amplio.

Junto con estas soluciones, usted podría, por ejemplo, beneficiarse de:

Un sandbox automatizado, que aporta un nivel avanzado de detección a sus endpoints al revelar las amenazas que permanecen latentes en presencia de la seguridad de los endpoints, pero que se activan una vez que el host se vuelve vulnerable y, por lo tanto, se deben analizar en un entorno controlado y aislado.

Inteligencia frente a amenazas, que le permite abordar de mejor manera los problemas como las ciberamenazas en archivos, direcciones URL, IP y dominios sospechosos, e investigar las amenazas de manera más rápida y exhaustiva.



Formación de concienciación en seguridad para sus empleados, que ayuda a subsanar las deficiencias de concienciación en materia de ciberseguridad y a transformar los comportamientos de los empleados, sobre todo teniendo en cuenta que la gran mayoría de los incidentes cibernéticos se deben a errores humanos.

También debería pensar en cómo se gestionará su solución, por ejemplo, al entregarle una consola unificada y compatible con la nube para todos los diferentes componentes, e incluso opciones de gestión web, en las instalaciones y de forma aislada.

Paso 8: Preguntar a su proveedor si ofrece todo esto:

Los distintos proveedores ofrecen soluciones de EDR y MDR con distintas capacidades (a veces muy amplias). Como regla general sencilla, lo ideal es que una solución integral incorpore lo siguiente.

- Implementación rápida y sin complicaciones
- Herramientas fáciles e intuitivas que no requieran mucho tiempo para familiarizarse con ellas o para recibir formación sobre ellas
- Una consola de gestión unificada para configurar sus herramientas de ciberseguridad y reaccionar a incidentes desde un solo lugar
- Capacidad para satisfacer sus necesidades y requisitos específicos con cada opción de implementación posible: en la nube, en las instalaciones, híbrida, aislada
- Visibilidad ante amenazas
- Análisis de la causa raíz que incorpora capacidades de visualización y exploración en profundidad para la realización de un análisis más cómodo y rápido
- Importación, generación y análisis de IOC
- Capacidades de respuesta rápidas y preferiblemente automatizadas
- Escenarios de respuesta guiada
- Búsqueda automatizada de amenazas, respaldada por especialistas del proveedor/MS(S)P
- Protección de endpoints perfectamente integrada y funcionalidad de detección y respuesta en endpoints
- Funcionalidad de sandbox
- Protección integrada contra ataques sin archivos
- Tecnología antiexploits
- Protección contra ransomware
- Gestión de parches y vulnerabilidades
- Control de aplicaciones, dispositivos y sitios web, y otros métodos de refuerzo del sistema
- Alto rendimiento para evitar la ralentización del usuario y la red
- Soporte técnico eficaz en el idioma local

Cómo puede ayudar Kaspersky Optimum Security

En pruebas independientes, Kaspersky demuestra constantemente una mayor calidad de protección en comparación con cualquier otro proveedor.

En 2019, obtuvimos el reconocimiento Gartner Peer Insights Customers' Choice de plataformas de protección de endpoints[4] por tercer año consecutivo y el de proveedor de seguridad más probado y galardonado por séptimo año consecutivo.

En 2020, también fuimos uno de los seis únicos proveedores del mundo en recibir el reconocimiento Gartner Peer Insights Customers' Choice para las soluciones de detección y respuesta en endpoints[5], con la puntuación más alta de todos los proveedores en cuanto a servicio y asistencia.

Otros premios recientes son:

- Clasificación de producto AA en las pruebas de protección avanzada de terminales realizadas por NSS Labs en 2020
- La máxima puntuación en protección contra ciberamenazas avanzadas en las pruebas en condiciones reales de AV-Comparatives
- Premio anual Best Enterprise Endpoint de SE Labs en 2020

Kaspersky Optimum Security protege su empresa frente a amenazas nuevas, desconocidas y evasivas sin utilizar sus recursos en exceso. Con ella, puede adoptar rápida y fácilmente una solución eficaz de prevención, detección y respuesta ante amenazas, respaldada por asistencia de expertos de Kaspersky para una supervisión de seguridad ininterrumpida, búsqueda automática de amenazas y escenarios de respuesta guiada y remota.

Además, si busca EPP, EDR y MDR, gestionadas desde una consola en la nube y complementadas por un sandbox, un portal de inteligencia de amenazas y formación de concienciación sobre la seguridad, Kaspersky Optimum Security permite una protección completa para todos sus endpoints en una solución unificada que ofrece prevención, detección y respuesta automáticas, protección gestionada y formación en ciberseguridad.

Protección avanzada frente a amenazas

- Los mecanismos avanzados de prevención y detección (aprendizaje automático, análisis de comportamiento, sandbox, búsqueda automatizada de amenazas con indicadores de ataque (IoA)) maximizan la protección contra amenazas evasivas peligrosas, lo que se construye sobre una sólida protección de EPP contra amenazas básicas de seguridad con Kaspersky Endpoint Security for Business.
- La visibilidad mejorada de las amenazas proporciona contexto y detalles sobre las amenazas detectadas, mientras que las herramientas simples de análisis de causa raíz y visualización le permiten investigar y comprender la amenaza de forma rápida y eficaz, y conocer cómo se desarrolló.
- La búsqueda automatizada de amenazas ayuda a establecer y mejorar la detección y respuesta ante amenazas de forma temprana y eficaz, a través de una supervisión continua ininterrumpida por parte de expertos líderes del sector.
- Las opciones rápidas de respuesta automatizada de un solo clic entre endpoints y el análisis de IoC en toda la infraestructura le ayudan a responder rápidamente a las amenazas que se mueven rápidamente en su infraestructura.
- Los escenarios de respuesta guiada y remota le proporcionan a sus equipos de seguridad un análisis experto y respuestas a amenazas nuevas, desconocidas y evasivas.
- La concienciación en aumento de los empleados sobre las ciberamenazas, los métodos que utilizan los cibercriminales y el modo en que los empleados pueden ayudar a prevenir que ocurran ataques reduce los riesgos de errores humanos y de ingeniería social.

Protección lista para usar rápida y escalable

- Funciona en estaciones de trabajo, portátiles y servidores, máquinas físicas y virtuales, nubes públicas y contenedores.
- La seguridad de endpoints a varios niveles consolidada prioriza incidentes y agiliza la detección e investigación de amenazas con información sobre las mismas mediante un cómodo portal web.
- Detiene las amenazas nuevas y emergentes utilizando tecnología de vanguardia que se ha demostrado que evita el ramsomware, los ataques de exploits, los ataques invisibles (sin archivos) y otros tipos de ataques de malware.

4 Gartner Peer Insights "Voice of the Customer": Plataformas de protección de endpoints, 10 de diciembre de 2019
5 Gartner Peer Insights "Voice of the Customer": Soluciones de detección y respuesta en endpoints, 1 de mayo de 2020

Minimiza las necesidades de personal o experiencia adicional

- Los sencillos procesos de análisis y respuesta dentro de una única consola compatible con la nube ayudan al personal de seguridad a optimizar el tiempo y el esfuerzo dedicados a la investigación y la corrección.
- La consola unificada permite gestionar desde un solo panel las principales aplicaciones de seguridad de Kaspersky. Las herramientas de ciberseguridad pueden configurarse y reaccionar ante incidentes desde un solo lugar, y satisfacer las necesidades específicas con todas las opciones de implementación posibles, incluidas la nube, las instalaciones, la híbrida y la aislada.
- La supervisión de seguridad ininterrumpida proporciona protección constante, incluso para organizaciones carentes de personal de seguridad de IT.

Por qué invertir en Kaspersky Optimum Security
Con **Kaspersky Optimum Security** podemos llevarle de una situación en la que se encuentre bajo un riesgo significativo de un ataque evasivo a una en la que haya renovado su confianza en su seguridad para endpoints. En lugar de no estar seguro de lo que sucede en su entorno, tendrá visibilidad y control de todos sus endpoints, estén donde estén. Y, en lugar de estar reticente a actualizar su seguridad debido a la complejidad que ello conlleva, tendrá una solución simplificada y consolidada que le ayudará a optimizar sus recursos.

Puede obtener más información sobre cómo obtener la protección avanzada que su empresa necesita, a la vez que minimiza las necesidades de recursos adicionales, visitando go.kaspersky.com/optimum.

Noticias sobre ciberamenazas: www.securelist.com
Noticias sobre seguridad de IT: www.kaspersky.es/blog
Threat Intelligence Portal: opentip.kaspersky.com
Introducción a las tecnologías: www.kaspersky.com/TechnoWiki
Premios y reconocimientos: media.kaspersky.com/en/awards
Herramienta de portfolio interactivo: kaspersky.com/int_portfolio/es

www.kaspersky.es

kaspersky PREPARADOS PARA EL FUTURO