Kaspersky Enterprise Cybersecurity

KASPERSKY lab

# Guía de soluciones de detección y respuesta en endpoints para empresas 2018

www.kaspersky.es
#truecybersecurity

# Índice

# Introducción

Un objetivo empresarial clave de cualquier organización es mantener la disponibilidad constante de datos y sistemas en los que se pueda confiar para tomar decisiones. El cambiante panorama de amenazas ha derivado en una mayor concentración en la ciberseguridad, que ha llegado hasta el nivel directivo. Los equipos de seguridad y de operaciones de IT deben demostrar una metodología global y coherente en su respuesta ante los incidentes de seguridad y el robo de datos.

*Hoy en día, la ciberseguridad es una de las tres principales prioridades reconocidas por las personas que ocupan puestos de dirección en su búsqueda de la continuidad del negocio para alcanzar el éxito.*

Los equipos directivos de las empresas actuales deben comprender el panorama de ciberamenazas específico de sus organizaciones. Se deben plantear preguntas como estas:

- ¿Mi organización comprende las principales amenazas y riesgos de seguridad que afectan a nuestro sector y a nuestra propia empresa?
- ¿Podemos detectar y detener rápidamente los ciberataques?
- ¿Cómo posicionamos la reducción del ciberriesgo en nuestra estrategia global de desarrollo empresarial?

## Los endpoints en el filo

En los endpoints corporativos (servidores, equipo de trabajo, teléfonos móviles, etc.), se produce la sinergia entre datos, usuarios y sistemas corporativos que generan e implementan los procesos empresariales, y esos innumerables dispositivos individuales siguen siendo el elemento clave de cualquier red, desde el punto de vista tanto empresarial como de seguridad.

Para proteger esos endpoints y evitar su uso como puntos de entrada ilícita en su infraestructura, sus equipos de seguridad de la información deberían empezar a adoptar procesos y tecnologías asociados con la detección avanzada, la búsqueda de amenazas, el análisis de IOC, el análisis de malware, los datos forenses de incidentes, la implementación de inteligencia global de amenazas y el establecimiento de un proceso formal de respuesta ante incidentes.

Pero ¿por dónde debería empezar? ¿Deberían subirse al carro del aprendizaje automático avanzado? ¿Mejorar la búsqueda de amenazas? ¿Centrarse en ampliar la supervisión y el SOC? Quizá lo mejor para abarcar estas áreas y mucho más sería utilizar una de las nuevas soluciones de detección y respuesta en endpoints (EDR). ¿Qué se puede esperar de EDR y por qué tipo de solución debería decidirse?

Este documento puede ayudarle a elegir la solución de EDR más adecuada. Nuestro objetivo es resaltar las diferencias fundamentales entre los distintos tipos de capacidades de EDR disponibles en el mercado y ayudarle a identificar las tecnologías que resultarán más valiosas para garantizar la continuidad del negocio y la seguridad en su organización.

# Todo sobre la detección y la respuesta en endpoints

## Un nuevo enfoque para la seguridad de endpoints

Para evitar ataques, proteja su perímetro. Este consejo parecía razonable: si su perímetro de IT está bien defendido, la protección de endpoints es tan solo un nivel más de su estrategia de seguridad global.

Sin embargo, este enfoque se queda corto en un mundo donde, gracias a tecnologías como los dispositivos móviles, los dispositivos conectados (IoT) y la computación en nube, la definición del perímetro de IT, por no hablar de su defensa, se ha convertido en todo un desafío y donde la evolución de las amenazas ha hecho que el enfoque defensivo basado en el perímetro se haya quedado obsoleto.

Los ataques dirigidos, un fuerte aumento de las técnicas de penetración complejas, el malware sin archivos y el uso de software legítimo, el robo de credenciales de usuarios normales, el uso de derechos legítimos, la explotación de problemas de las políticas de seguridad y los errores de configuración han llevado a las organizaciones a reconocer la importancia de las estrategias y soluciones de seguridad integradas. Esto, a su vez, ha provocado el crecimiento de la implementación de SIEM y de los centros operativos de seguridad (SOC). La necesidad ha hecho que la ciberseguridad corporativa haya pasado a ser proactiva, polifacética y altamente especializada.

El mundo está cambiando y está dispuesto a aceptar un nuevo paradigma de seguridad de endpoints. La atención se ha desplazado de nuevo al endpoint. Siempre ha habido departamentos de IT visionarios que han considerado que cada endpoint requiere su propio perímetro de seguridad. No obstante, gracias en parte a las organizaciones que **no** han adoptado este enfoque, y cuya mala visibilidad de los dispositivos individuales ha llevado a bajos niveles globales de seguridad, los endpoints nunca han dejado de ser el principal objetivo inicial para los cibercriminales.

## Una actitud más proactiva

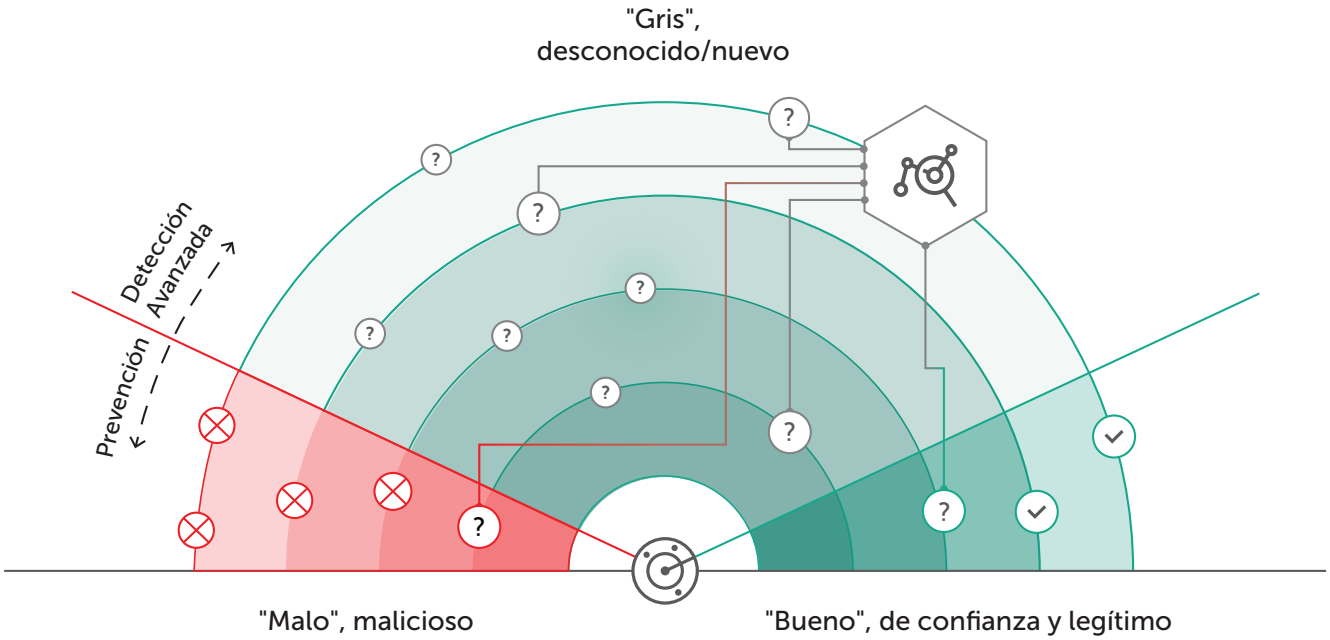
Mientras tanto, los reguladores están introduciendo nuevos requisitos (GDPR, PCI DSS, etc.) que pueden requerir la supervisión y el registro continuos de incidentes en todos los endpoints de la red. Para la mayoría de las empresas, el número de eventos o incidentes registrados por su solución de seguridad actual sigue en aumento, por lo que verificar y analizar cada evento registrado se convierte en un problema en sí mismo. Tampoco ayuda el hecho de que los expertos en seguridad con los conocimientos necesarios en ingeniería inversa, análisis de malware, ciencia forense digital y respuesta ante incidentes que deben encargarse de gestionar estas tareas escaseen y no sean fáciles de encontrar.

En este punto, la mayoría de los procesos de seguridad centrados en las amenazas avanzadas y la mayoría de enfoques de supervisión de SOC funcionan básicamente a base de alertas y con una actitud reactiva. Los expertos en seguridad esperan a tener pruebas de una brecha antes de alertar al analista de seguridad, después de lo cual el equipo de respuesta ante incidentes puede tomar medidas. En el mejor de los casos, los responsables de respuesta ante incidentes identifican los artefactos de un ataque en la última etapa de la "cadena de destrucción". En el peor de los casos, simplemente esperan a hacer el recuento de los daños, a veces meses después de que se haya producido la brecha en los sistemas. Resulta evidente que esto es insatisfactorio. Por lo tanto, las organizaciones están revisando sus procesos de seguridad, especialmente en el ámbito de la detección proactiva de incidentes, así como de la respuesta proactiva ante ellos.

## ¿Cómo afecta esto a las soluciones para endpoints?

*La búsqueda de amenazas ayuda a descubrir amenazas avanzadas ocultas dentro de la organización mediante funcionalidad de búsqueda proactiva de amenazas llevada a cabo por profesionales de seguridad altamente cualificados y experimentados.*

La última generación de soluciones para endpoints se centra en la detección eficaz de nuevas amenazas dirigidas hacia la organización, patrullando y analizando eventos en la "zona gris" donde puede haber amenazas desconocidas e indefinidas al acecho, es decir, se centra en la "búsqueda de amenazas" proactiva.




# Más allá de la protección de endpoints

La búsqueda de amenazas eficaz está directamente relacionada con las capacidades de un SOC maduro. La actualización de soluciones de seguridad compradas no es suficiente. No se pueden imponer nuevos requisitos a las soluciones tradicionales de protección de endpoints (EPP), porque no se podrán cumplir o no funcionarán de manera eficaz.

Echemos un vistazo a algunos problemas clave resueltos por la EPP tradicional y a los nuevos desafíos a los que se enfrenta la seguridad de endpoints:

| Temas de control y protección cerrados por las soluciones de EPP tradicionales: | Nuevos desafíos avanzados para la seguridad de endpoints: |
|---|---|
| Cómo protegerse automáticamente (tanto prevención como reversión) contra las amenazas existentes, incluido el ransomware y los bloqueadores de cifrado | Cómo buscar de manera proactiva pruebas de intrusiones, como indicadores de compromiso, en toda la red en tiempo real |
| Cómo gestionar y aplicar controles de seguridad para web/aplicaciones/ dispositivos de manera centralizada | Cómo detectar y corregir una intrusión antes de que el intruso tenga la oportunidad de causar daños importantes |
| Cómo gestionar los procesos de análisis de vulnerabilidades y gestión de parches de manera centralizada | Cómo correlacionar las alertas de los controles de seguridad de red para comprender qué está sucediendo en el endpoint en tiempo real |
| Cómo proteger la información y los datos corporativos en los dispositivos | Cómo validar las alertas y los posibles incidentes detectados por las soluciones de seguridad |
| Cómo implementar políticas de protección de web y correo en el nivel de endpoint | Cómo investigar rápidamente y gestionar de manera centralizada los incidentes en miles de endpoints |
| Cómo proporcionar a los usuarios de endpoints conjuntos específicos de dominios de seguridad ajustados a sus necesidades | Cómo hacer que el proceso de respuesta ante incidentes (trabajo manual, habilidades de nivel 3, sobrecarga de alertas, etc.) sea menos costoso mediante la automatización de las operaciones de rutina del equipo de seguridad |

¿Cómo puede enfrentarse a estos nuevos desafíos?

# Su estrategia de ciberseguridad de endpoints: adaptable, avanzada, predictiva

*Difíciles de detectar y, a menudo, incluso más difíciles de eliminar, los ataques dirigidos y las amenazas avanzadas exigen una estrategia de seguridad adaptable y exhaustiva.*

Uno de los marcos de seguridad adaptable más eficaces se basa en la arquitectura de seguridad viable descrita por Gartner. Su enfoque es proporcionar un ciclo de actividades en cuatro áreas clave: prevención, detección, respuesta y predicción.

- **Prevención**: bloqueo de las amenazas habituales y refuerzo de los sistemas básicos para reducir el riesgo de amenazas avanzadas
- **Detección**: descubrimiento rápido de actividades que podrían indicar que hay un ataque dirigido o una brecha
- **Respuesta**: contención precisa de la amenaza, realización de investigaciones y respuesta apropiada a los ataques
- **Predicción**: saber dónde y cómo podrían producirse nuevos ataques dirigidos


**Modelo de seguridad adaptable**

Básicamente, este enfoque da por supuesto que la prevención tradicional, sobre todo en el caso de los endpoints, debería funcionar en coordinación con tecnologías de detección avanzadas, análisis de amenazas, capacidades de respuesta y técnicas de seguridad predictivas. El resultado es un sistema de ciberseguridad que se adapta y responde continuamente a los desafíos empresariales emergentes.

Las tecnologías basadas en la prevención en varios niveles siguen siendo un elemento fundamental de este nuevo enfoque proactivo para la protección contra ataques dirigidos. No obstante, si el atacante está suficientemente motivado y quizá incluso contratado por un tercero para llevar a cabo un ataque con éxito, un enfoque centrado exclusivamente en la prevención no bastará. También debe ser capaz de identificar rápidamente las amenazas, tomar decisiones y contar con la posibilidad de que se produzca una penetración, a la vez que simplifica las operaciones manuales actuales y automatiza las herramientas de respuesta.

# Definición de EDR

## Características clave de una solución de EDR

Como hemos visto, según la definición de Gartner, las soluciones de EDR deben tener las siguientes capacidades principales:

- detectar incidentes de seguridad
- contener el incidente en el endpoint, de manera que el tráfico de red o la ejecución de procesos pueda controlarse de manera remota
- investigar los incidentes de seguridad
- corregir los endpoints a un estado anterior a la infección

### Detección de incidentes de endpoints

Detectar incidentes de seguridad mediante la **supervisión de actividades** y objetos de endpoints e infracciones de las políticas, o mediante la validación de indicadores de compromiso (IOC) proporcionados externamente

### Investigación de incidentes

Investigar los incidentes de seguridad. La función de investigación debe incluir una **cronología histórica** de todos los eventos de endpoints primarios para determinar tanto los cambios técnicos producidos como el efecto en el negocio

*(derivación de privilegios, propagación, exfiltración, geolocalización de mando y control, y atribución de adversario si es posible)*

### Prevención y respuesta a incidentes

**Contener** el incidente en el endpoint y **corregir** los endpoints a un estado anterior a la infección.

*Eliminar archivos maliciosos, deshacer y reparar otros cambios, o crear instrucciones de corrección que puedan ponerse a disposición de otras herramientas para su implementación*

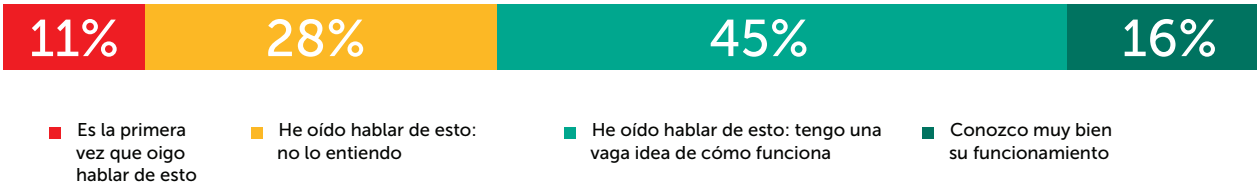
### Recopilación de datos forenses

**Recopilar** conjuntos de datos, volcados de memoria RAM, instantáneas de disco duro, etc. para su análisis posterior

¿Cuál es el grado de conocimiento de las organizaciones sobre el funcionamiento de EDR y cómo contribuyen estas tecnologías a la continuidad de la actividad? Una encuesta de Kaspersky Lab entre las organizaciones empresariales a lo largo de 2016 arrojó algunos resultados preocupantes.

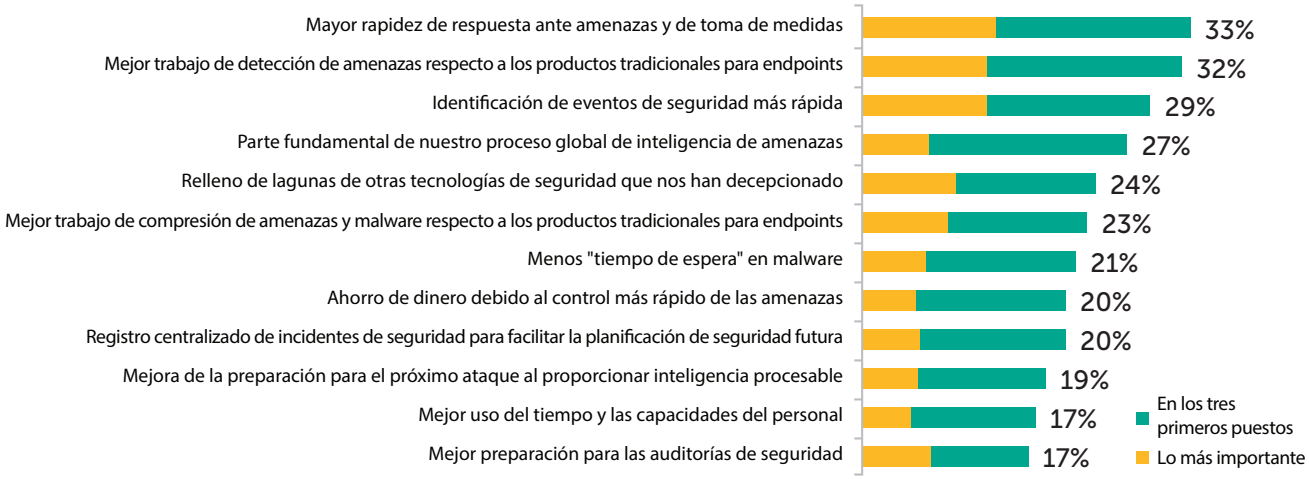
**Pregunta de la encuesta: "¿Conoce la clase de soluciones de EDR?"**

Respuesta:




Fuente: Expertos en IT de empresas con más de 250 empleados

Al mismo tiempo, los representantes de empresas entrevistados formularon claramente los fundamentos básicos de sus expectativas y los resultados que les gustaría obtener con el uso de soluciones de EDR en sus organizaciones:




Esta combinación de conocimientos limitados y expectativas claras es fuente de preocupación. Como es natural, los proveedores de soluciones de EDR están bien dispuestos a satisfacer estas expectativas y desarrollan "funciones de destrucción" que prometen mucho y parecen emocionantes en la fase piloto, pero que a menudo resultan mucho menos prácticas y rentables cuando se incorporan en los procesos de respuesta ante incidentes, investigación o búsqueda de amenazas nuevos o ya establecidos del cliente.

*Como resultado, en algunos ambientes, las soluciones de EDR ya se contemplan con cierta sospecha.*

# Auge y caída de las soluciones de detección y respuesta en endpoints

*Por desgracia, los primeros en adoptar las soluciones de EDR no siempre son sus más grandes admiradores. Las primeras soluciones de EDR tenían muchas carencias, lo que hizo que algunos clientes quedaran decepcionados y frustrados.*

Por desgracia, aún no existe un análisis comparativo establecido o un informe independiente que expongan todas las funciones clave y las posibles variaciones de las tecnologías de EDR disponibles en el mercado hoy en día. Además, muchos productos de "primera generación" en este mercado todavía inmaduro no consiguieron cumplir inicialmente en la práctica las expectativas de los expertos y las organizaciones.

La mayoría de soluciones empezaron con algunas "funciones de destrucción" en lugar de funciones complejas. En lugar de una solución integrada con la capacidad de unificar y automatizar las capacidades de inteligencia de amenazas, búsqueda de amenazas, antimalware, respuesta ante incidentes y análisis forense de la seguridad de red, en la práctica, EDR resultó ser un conjunto de herramientas de análisis e investigación. Así, este kit de herramientas tecnológicas acabo saliendo caro para lo que ofrecía y extremadamente difícil de dominar para los profesionales de seguridad corrientes.

Algunas soluciones de EDR tampoco cumplían lo prometido en cuanto a eficiencia. Al responder a un incidente de malware, una solución de EDR recopilará información de los endpoints (firmas y comportamiento del malware) que se puede utilizar para identificar infecciones futuras. Sin embargo, si la solución no está estrechamente integrada con tecnologías de detección y sistemas de seguridad, existe un alto riesgo de superposición y duplicación, lo que genera más procesos manuales y obstaculiza el flujo de trabajo, en lugar de aumentar la eficiencia y la eficacia. La solución de EDR acaba siendo un depósito de almacenamiento adicional de datos relacionados con la seguridad, que en sí mismos no pueden indicar cómo se originó el evento ni cómo evitar que se repita. Sin la integración de la resolución de casos raíz en el flujo de trabajo, una organización no puede corregir el problema de manera concluyente ni reducir el riesgo de que se repita.

Otra deficiencia ha sido que algunas de las primeras soluciones en el mercado no estaban diseñadas realmente para detectar o investigar amenazas avanzadas persistentes (APT). Con este fin, los propietarios de soluciones de EDR tenían que seguir externalizando actividades a expertos, posiblemente pertenecientes al proveedor, o comprar formación adicional cara. Si se debe recurrir a un equipo externo de respuesta ante incidentes cada vez que se identifica una brecha, la rentabilidad de la solución de EDR podría cuestionarse.

Una tendencia que ha ido en aumento es el uso de versiones de las soluciones de EDR en la nube, con la transferencia de ciertos datos y registros a la nube del proveedor en lugar de almacenarse en los agentes instalados o en un repositorio centralizado. No obstante, eso tiende a generar más incidentes, con tiempos de reacción más lentos (y a veces sin reacción en absoluto).

Sin embargo, muchos de estos resultados son agua pasada y las empresas que examinen actualmente el mercado de EDR no deberían juzgar los posibles resultados de su inversión por las experiencias de aquellos pioneros. El mercado ha crecido y ha madurado.

*Entonces, ¿qué debe buscar en las soluciones de EDR hoy y qué debe tener en cuenta? Veamos cinco desafíos que debe tener en cuenta a la hora de poner en marcha su proyecto de EDR.*

# Los cinco desafíos principales al iniciar un proyecto de EDR

Es inevitable que surjan nuevos desafíos para las organizaciones que adopten una nueva tecnología o procesos desconocidos. Además, como las soluciones de EDR son más caras que sus homólogas tradicionales de EPP, puede ser complicado justificar su inversión en EDR en cuanto a valor añadido, al sopesarla con los costes de un producto de información de seguridad y gestión de eventos (SIEM) o herramientas de análisis forense.

La función principal de una solución de EDR de categoría empresarial es **la capacidad de ayudar al equipo de seguridad en las investigaciones basadas en preguntas:** los consejos de búsqueda son iterativos y comienzan con preguntas o hipótesis para lograr visibilidad. Una pregunta o hipótesis inicial podría basarse en los pasos de la cadena de ciberdestrucción y ser algo así como "¿Se está produciendo una exfiltración de datos o una comunicación maliciosa?" o "Si hay una conexión sospechosa al dominio externo, lo más probable es que pase por esta parte de la red, pero ¿desde qué endpoint y proceso?".

Para ofrecer esta funcionalidad, la solución de EDR debe tener **funciones de asistencia a la investigación**, así como **funciones de recopilación de datos** y **almacenamiento**. Asimismo, la **detección de incidentes** debe incorporar elementos manuales y automatizados. Por último, cuando se detecta el incidente inicial, el equipo de seguridad y el responsable de respuesta ante amenazas deben estar equipados para **contener fácilmente** la amenaza, **corregir** los endpoints e **impedir** que la actividad específica ocurra de nuevo.

Echemos un vistazo a los cinco desafíos más habituales que las organizaciones deberían tener en cuenta al elegir soluciones avanzadas de EDR o al mejorar en general su seguridad de endpoints actual en cuanto a detección y respuesta.


## Datos de endpoints: demasiada visibilidad

Cualquier método de protección de endpoints comienza con la recopilación de nuevos datos, su almacenamiento y análisis. En teoría, cuantos más datos pueda recopilar, mayores serán las ventajas. La misma teoría también se solía aplicar a los sistemas SIEM. Sin embargo, para interpretar grandes volúmenes de datos recopilados, el operador de EDR también necesita el contexto pertinente. Por ejemplo, la detección rápida de una conexión maliciosa a un dominio incorrecto es mucho menos valiosa si no sabemos en qué endpoint se ha originado, cómo se ha iniciado el proceso, cuál es la causa raíz y qué activos pueden haber sido afectados.

Las soluciones de EDR inmaduras disponibles en el mercado recopilan algunos datos, pero no proporcionan el contexto correcto. Por ejemplo, pueden permitir al operador detectar rápidamente qué equipos tienen un archivo con una cierta suma de verificación, pero sin proporcionar información sobre cómo apareció el archivo en esos equipos. Es posible que se proporcione una lista de procesos generados para el objeto y las actividades, pero sin visualización. O bien, puede que se proporcionen alertas complejas sobre comportamientos atípicos o desviaciones, pero sin análisis ni veredictos básicos.

Algunas soluciones recopilan todos los datos de los endpoints y luego los presentan directamente en la interfaz, como una ventana directa a la base de datos. A menos que el operador sea científico de análisis de datos o especialista en Big Data, además de experto en seguridad, no podrá tomar una decisión informada sobre la base de estos datos sin procesar.

A menudo, estos sistemas generan miles de mensajes y millones de alertas que alguien tendrá que validar. Incluso en las organizaciones más grandes, es improbable que el equipo de supervisión y respuesta pueda gestionar más de 50-60 incidentes de gravedad media a muy crítica de manera simultánea. Como resultado, tenemos una solución que lo encuentra todo, pero que poco o nada puede hacer acerca de lo que ha encontrado: hay demasiadas y a la vez insuficientes datos por examinar.

En ese caso, una concesión podría ser compartir las alertas entre su propio equipo de seguridad y un MSSP externo, pero tendrá que encontrar un proveedor con la formación y la experiencia adecuadas. Además, sin la priorización de los incidentes, eso podría implicar una inversión enorme y un despilfarro de recursos en alertas no críticas. Otro factor preocupante, como ocurre con cualquier MSSP, es la cuestión de confianza, privacidad de datos y restricciones de conformidad.

**Recomendaciones:**

- Busque soluciones que no solo le permitan exponer automáticamente el riesgo a través de alertas, sino que también permitan una personalización en profundidad: configurar distintas funciones de usuario, asignar grupos VIP y configurar rápidamente listas blancas. Esto le permitirá resaltar correctamente lo importante, reducir lo innecesario y comprobar que el MSSP externo solo pueda visualizar la información crítica.
- Piense en qué medida espera realizar análisis de datos en la organización y en la cantidad de datos que espera almacenar y procesar. La preparación para manejar terabytes de datos internamente puede significar importantes costes adicionales de hardware.

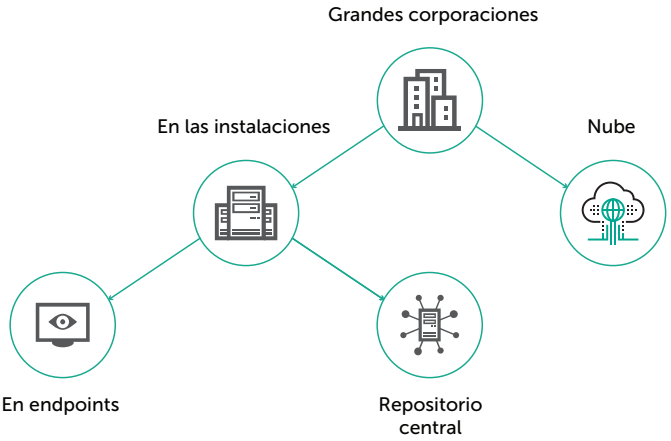
2

# Responsabilidad de los datos unificados y almacenados

Otra característica importante relacionada con los datos es cómo se recopilan y almacenan. Las preguntas que debe formular a un proveedor de EDR en este ámbito son:

- ¿Cuántos datos se almacenan y por qué?
- ¿Qué datos se almacenan?
- ¿Dónde se almacenan?

Hay varios enfoques posibles en cuanto al almacenamiento:




Veámoslos más de cerca.

## Nube

Muchos proveedores ofrecen soluciones en la nube para almacenar datos o incluso para gestionar agentes EDR (los llamados MDR). Son cómodas, pero limitadas por la cantidad de datos que pueden cargar en un momento dado. Esto también implica el tener un conducto abierto que transmite datos fuera de la organización, lo cual puede ser un problema en algunos entornos. Al sopesar esta opción, debe plantearse las siguientes preguntas:

- ¿Estamos preparados para enviar datos de seguridad a una nube pública? ¿Cuánto control tendremos?
- ¿Podemos confiar en el proveedor de la solución o el proveedor del servicio en la nube (podría ser un tercero) que almacenará los datos? ¿Cómo son sus disposiciones de ciberseguridad?
- ¿El uso de este servicio podría infringir el cumplimiento de estándares de seguridad internos o de requisitos normativos?
- Si solo se envían pequeños volúmenes de datos no críticos a la nube, ¿será eficaz la solución?

## En agente

Una caché local en cada dispositivo ofrece una solución de compromiso entre el almacenamiento intenso y la nube. Este enfoque tiene un menor impacto en la red y puede aceptar un gran número de agentes simultáneamente. La información importante se registra en la caché del endpoint y todos los análisis tienen lugar en tiempo real mediante consultas. No obstante, el almacenamiento descentralizado no siempre es la manera más rápida y eficaz de analizar y responder a la información. Por ejemplo, si un subsegmento de la red no está disponible, no será posible incorporar los datos de los equipos afectados en el análisis global.

## Repositorio centralizado en las instalaciones

Un servidor dedicado con un repositorio acumula y analiza toda la información esencial. Una base de datos local y herramientas de análisis (por ejemplo, un sandbox) hacen todo el trabajo. Este enfoque local tiene una serie de ventajas: los datos no se almacenan en dispositivos que puedan estar infectados, como en teoría podría suceder con el almacenamiento basado en agentes. Los recursos del equipo no reciben ninguna carga y el usuario puede realizar consultas en los endpoints y "búsquedas rápidas" a través de la propia base de datos en tiempo real. Las soluciones en las instalaciones como esta son especialmente útiles cuando las normativas o los estándares de seguridad exigen que no se transfieran datos fuera de la organización.

**Recomendaciones:**

- Para el almacenamiento en la nube, evalúe a su proveedor de EDR en la nube en cuanto a la privacidad y el control de los datos.
- Para entornos confidenciales y en los casos en los que el cumplimiento de normativas aplique posibles restricciones a la transferencia de datos externos, la evaluación podría incluir la exploración de opciones para una implementación en las instalaciones totalmente aislada y la entrega privada de inteligencia de amenazas.
- Para el almacenamiento de datos basado en agentes, compruebe qué ocurrirá si un endpoint no está disponible o se ha visto comprometida por el atacante (cómo están protegidos el propio agente, el PC y los datos).
- Para las soluciones en las instalaciones, compruebe la capacidad de almacenamiento interno de datos y la cantidad de datos enviados desde cada dispositivo.

*El número de agentes dictará los requisitos de hardware: si una solución de EDR requiere solo un pequeño servidor para admitir cientos de miles de agentes, hay algo que no cuadra. Como promedio, un endpoint genera alrededor de 10 megabytes de telemetría útil al día. Por lo tanto, si tiene 10 000 nodos, se generarían unos 100 gigabytes de datos al día, o 3 TB para una base de datos retrospectiva de un mes.*

3

# Detección: búsqueda manual frente a motores automatizados

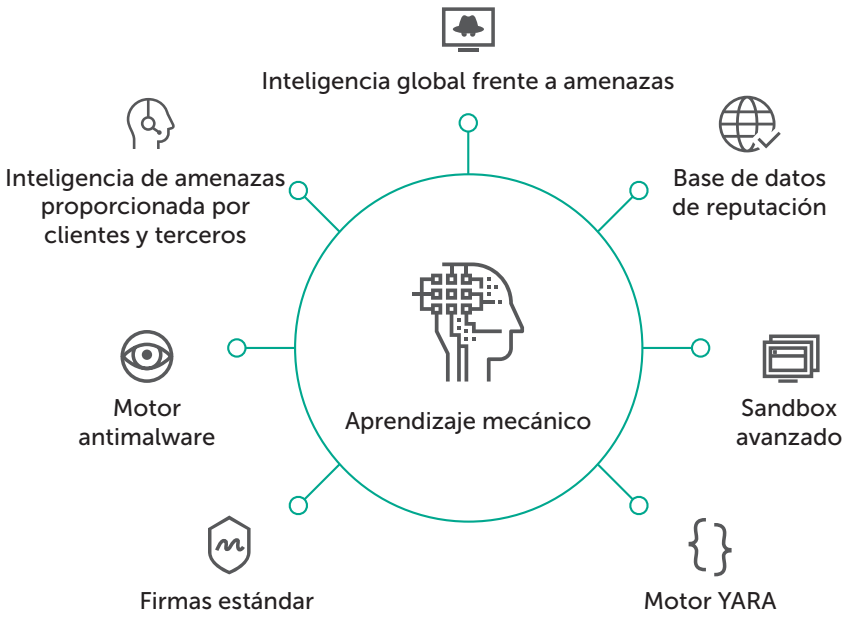
Ya hemos visto qué pasa con los datos y el almacenamiento. Ahora pasaremos al análisis de datos, es decir, la búsqueda y supervisión de las amenazas realizadas manualmente con los kits de herramientas, las bases de datos y los recursos de su proveedor, y automáticamente a través del propio sistema de EDR. Cuanto antes detecte un ataque, menores serán el impacto financiero y las interrupciones causadas. Por ello, la velocidad y la eficacia de la detección son primordiales, y las técnicas de detección manual por sí solas no suelen ser el enfoque más rápido o eficiente. Muchos proveedores ofrecen las llamadas "técnicas de detección avanzada", es decir, el análisis de IOC de endpoints en tiempo real o la búsqueda rápida en bases de datos forenses almacenados de manera centralizada, que añaden un elemento automatizado a las funciones de detección de incidentes.

Para aprovechar al máximo los datos unificados, necesitará potentes técnicas automatizadas de análisis de datos que ayuden a los analistas a revelar los riesgos y las amenazas que se presentan a través de la red. Un análisis multidimensional en varios niveles debería proporcionar continuamente no solo nuevos incidentes de seguridad, sino también inteligencia procesable, a fin de ayudar a su equipo de seguridad a tomar las decisiones correctas y evitar que tenga que invertir un tiempo innecesario en eventos no críticos.

Esas tecnologías de detección avanzada y descubrimiento de amenazas no solo deberían detectar las habituales actividades maliciosas, sino ir "más allá del malware" para detectar brechas más sofisticadas. No estamos hablando de los niveles de filtro de las tecnologías de prevención que forman la base de la mayoría de las soluciones de EPP, sino de sistemas analíticos avanzados.

Las soluciones de seguridad que utilizan varias tecnologías de detección pueden aumentar enormemente sus posibilidades de detectar ataques e intrusiones más rápido, antes de que se causen graves daños a la organización. Las soluciones de EDR deben incluir varios motores de detección integrados para proporcionar una detección de amenazas avanzadas que combine el análisis estático basado en el comportamiento y el análisis dinámico, además del acceso en tiempo real a la inteligencia global de amenazas y a las tecnologías de aprendizaje mecánico.

Por lo tanto, el objetivo principal es aprovechar tantos motores de detección como sea posible para proporcionar capacidades de "laboratorio de análisis de virus" en sus instalaciones que puedan validar predicciones, iniciar nuevas investigaciones o respaldar las investigaciones en curso.




Según el proveedor, los motores y las técnicas de detección usados seguramente se compondrán de un kit de herramientas manuales y de sistemas automatizados en alguna combinación:

## Ayudas para la detección manual

- Carga y búsqueda automática/manual de indicadores de compromiso
- Búsqueda rápida en los datos retrospectivos
- Sandbox (capacidad de enviar un objeto específico a un sandbox dedicado o basado en la nube)
- Acceso a las fuentes de inteligencia de amenazas del proveedor

## Detección automatizada

- Antimalware
- Reglas YARA (personalizables por el proveedor o su equipo de seguridad)
- Inteligencia de amenazas (entregada por el proveedor automáticamente)
- Servicios de reputación (archivos o dominios)
- Análisis en sandbox automatizado de objetos sospechosos
- Aprendizaje mecánico
    - Aprendizaje en profundidad (sin firma, en red neuronal)
    - Inteligencia artificial (establecimiento de referencias, análisis del comportamiento)

**Recomendaciones:**

- Pregunte a su proveedor de EDR qué tecnologías de detección están disponibles y en vigor.
- Averigüe si utiliza motores de detección internos, de OEM o de fuente abierta.
- Explore la calidad y la inmediatez de la inteligencia de amenazas que alimenta esos motores.
- Si se aplican varias tecnologías de detección, ¿cómo se integran y correlacionan? (No querrá terminar con incidentes separados registrados en motores diferentes para el mismo evento).

4

# No reaccione, responda

La reacción ante un incidente es fácil, pero la respuesta eficaz es lo que lo resuelve. El proceso de respuesta se activa una vez que se ha validado un incidente de seguridad mediante el control selectivo y la investigación inicial. Una vez que se ha confirmado que no se trata de un "falso positivo", se requiere una respuesta rápida y precisa.

El proceso de gestión de la respuesta ante incidentes dependerá de la gravedad del incidente. La mayoría de los incidentes tendrán un impacto empresarial relativamente bajo (se detectarán directamente en la entrada). Sin embargo, habrá incidentes que podrían llevar a una situación grave: un importante robo de datos, delitos financieros, espionaje o cosas incluso peores. Estas son las situaciones críticas que requieren un proceso de respuesta e investigación ante emergencias.

Una vez que ha detectado manualmente o ha recibido una alerta de seguridad acerca de una posible amenaza, a través de una solución de seguridad de terceros o de su producto de EDR, ¿qué ocurre a continuación? ¿Ha esbozado los procesos de control selectivo, investigación y respuesta para su organización? Sin estos procesos, su equipo de seguridad puede quedar abrumado rápidamente por el flujo de trabajo que rodea a cualquier solución de EDR.


Detectar una amenaza activa es la primera etapa vital para repeler un ataque. Tras detectar la amenaza, debe responder rápidamente, posiblemente en miles de endpoints. Una solución de EDR permitirá la gestión centralizada de los incidentes en todos los endpoints de la red corporativa, con un flujo de trabajo perfecto. Además, una amplia variedad de respuestas automatizadas le ayudará a evitar el uso de procesos de corrección tradicionales (como el borrado y la repetición de la generación de imágenes), que pueden tener como resultado un costoso tiempo de inactividad y la pérdida de productividad.

La funcionalidad de respuesta básica depende del criterio del proveedor, pero debe centrarse en estas operaciones comunes:

- Prohibir el inicio de archivos PE, documentos Office y scripts
- Capacidad de eliminar de manera remota el archivo en la estación de trabajo
- Mover el archivo desde la estación de trabajo a cuarentena y recuperarlo si es necesario
- Obtener el archivo y realizar un análisis durante la investigación (por ejemplo, ejecución de sandbox forzada)
- Forzar el proceso de apagado
- Ejecutar el programa o script en la estación de trabajo

Algunos proveedores pueden ofrecer escenarios adicionales para una mayor precisión en las respuestas. Podrían incluir escenarios de aislamiento de la red, de aislamiento de procesos, de desactivación de usuarios, de reversión y de corrección.

**Recomendaciones:**

Busque:

- Proveedores con la capacidad de mantener bases de datos de inteligencia de amenazas potentes y completas, y de proporcionarle soporte técnico y asesoramiento de expertos como y cuando sea necesario.
- Soluciones de EDR respaldadas por cursos de formación eficaces que capaciten a su equipo de seguridad para que pueda establecer procesos eficaces y sacar el máximo partido de su inversión.
- Un flujo de trabajo perfecto entre los procesos de detección, búsqueda manual de amenazas, IOC de terceros y respuesta ante incidentes, sin necesidad de cambiar entre diferentes consolas o soluciones.
- Agentes que sean silenciosos para los usuarios finales, incluso durante las investigaciones, que no tengan ningún impacto en el comportamiento de los usuarios y que no contribuyan a la inactividad.

5

# Prevención: ¿EDR o EPP?

Las soluciones de EDR incorporan cada vez más elementos de prevención en un intento de ofrecer una solución "todo en uno". A medida que las funciones de prevención vayan madurando, es posible las funciones de prevención, visibilidad, detección y respuesta en endpoints converjan en un único producto para endpoints.

No obstante, aún no hemos llegado a este punto. Aunque puede ser tentador buscar una solución que incluya la prevención junto con la detección y la respuesta, no recomendamos que dé mucha importancia a este aspecto en este punto. Seleccione el producto primordialmente por sus funciones de visibilidad, detección y respuesta. Si la solución también incluye elementos de la prevención, son un extra añadido. Sin embargo, actúe con cautela ante las soluciones de EDR de "próxima generación" con funciones de prevención inmaduras. Si intenta reemplazar su EPP tradicional con una solución de EDR, es poco probable que alcance los mismos niveles de funcionalidad de prevención.

No obstante, en estos momentos muchos proveedores de EPP están comprando o desarrollando sus propios EDR. Si está satisfecho con su EPP actual y su proveedor de EPP le ofrece una solución de EDR, tiene sentido evaluar cómo interactúan ambas soluciones y cómo podrían funcionar juntas, especialmente si eso significa no tener que instalar un segundo agente para EDR.

**Recomendaciones:**

- Examine la hoja de ruta del producto de EDR y cómo puede evolucionar con el tiempo para ofrecer funcionalidad de prevención adicional.
- Si le atrae la idea de la respuesta ante incidentes, detección y protección de endpoints integradas, examine la oferta de EDR de su proveedor de EPP actual y observe qué funciones de EPP ofrecen otros proveedores de EDR.
- Examine la arquitectura de la solución de EDR y, en particular, la posibilidad de utilizar un único agente para EPP y EDR.

# El futuro de la seguridad de endpoints para empresas

*Los líderes del mercado tratarán de adoptar nuevas tecnologías y aprovechar el desarrollo interno para aumentar su funcionalidad de EDR.*

En estos momentos, los expertos en seguridad tienen la sensación de que el mercado de seguridad de endpoints está muy sobresaturado con diferentes proveedores. Es evidente que eso no puede seguir así. Los proveedores grandes acabarán devorando a las pequeñas empresas y utilizarán sus productos para llenar las lagunas de su cartera y mejorar sus marcas. Los líderes del mercado tratarán de adoptar nuevas tecnologías y aprovechar el desarrollo interno para aumentar su funcionalidad de EDR.

Una seguridad de endpoints verdaderamente de "próxima generación", que ofrezca tanto métodos tradicionales de control y protección como tecnologías avanzadas, irá evolucionando gracias a los esfuerzos de los principales protagonistas del mercado de EPP. La generación actual de agentes de seguridad de endpoints avanzada, como EDR, solo ofrecen elementos de la auténtica funcionalidad de EPP y, en este momento, no pretenden arrogarse la responsabilidad de ofrecer un paquete de protección de endpoints con funcionalidad completa.

La seguridad de endpoints ha escalado puestos en la agenda corporativa y seguirá atrayendo cada vez más atención. Los clientes futuros adaptarán y desarrollarán sus estrategias de seguridad en torno a tecnologías de protección de endpoints avanzadas combinadas con la supervisión de la actividad de endpoints.

Desde el punto de vista tecnológico, esas soluciones formarán un enfoque adaptable con respecto a la protección y, a la vez, reforzarán los sistemas, y aportarán prevención de actividad maliciosa y detección avanzada. También serán importantes la inteligencia de amenazas basada en la nube y el aprendizaje mecánico en las instalaciones, la búsqueda de amenazas, incluyendo respuestas activas e investigaciones rápidas, y el análisis profundo del comportamiento y la inteligencia de amenazas.

# Recomendaciones inmediatas

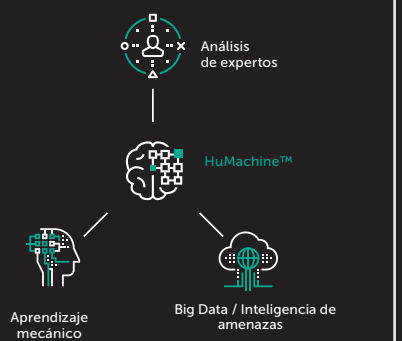
Al reconocer la creciente necesidad de un análisis y protección de endpoints más en profundidad, los profesionales de seguridad acaban teniendo una larga lista de necesidades y un presupuesto limitado con el que abordarlas todas. No obstante, aunque se carezca de presupuesto, tiene sentido evaluar las tecnologías actuales y la posible evolución futura con respecto a si se corresponden con sus objetivos empresariales y sus capacidades internas. Si investiga y prueba exhaustivamente las opciones, puede contribuir a que los responsables de la toma de decisiones generales de su empresa se centren en la funcionalidad que pueden aportar las nuevas tecnologías, a garantizar una planificación presupuestaria de seguridad futura más precisa y a saber que, cuando llegue el momento de invertir, se podrá hacer de manera inteligente.

## Acciones inmediatas

1. Evalúe sus capacidades de seguridad generales. ¿Su proceso de respuesta ante incidentes es rápido y está unificado? ¿Ejecuta actualmente las soluciones que más le convienen, dejando a un lado las consideraciones sobre EDR? ¿Cuál es su postura sobre esto en relación con su sector y con la competencia?
2. Comprenda su capacidad actual de detección a través de endpoints. Realice análisis y considere la posibilidad de probar fuentes de inteligencia adicionales, por ejemplo, examine la posibilidad de usar fuentes de datos de amenazas con su SIEM.
3. Piense en cómo puede empezar a ampliar la experiencia en respuesta ante incidentes internamente. Evalúe las capacidades de su equipo e investigue opciones de formación eficaces.
4. Empiece a formular sus requisitos actuales y sus demandas futuras, e intente seleccionar soluciones de EDR que se ajusten a ellos.

## Enlaces útiles

1. Directrices sobre respuesta ante incidentes: https://cdn.securelist.com/files/2017/08/Incident_Response_Guide_eng.pdf
2. Evalúe su seguridad con esta calculadora de seguridad de IT y descargue el informe global para empresas: https://calculator.kaspersky.com/es/




Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Noticias de ciberamenazas: **https://securelist.lat/**
Noticias de seguridad de IT: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

**www.kaspersky.es**