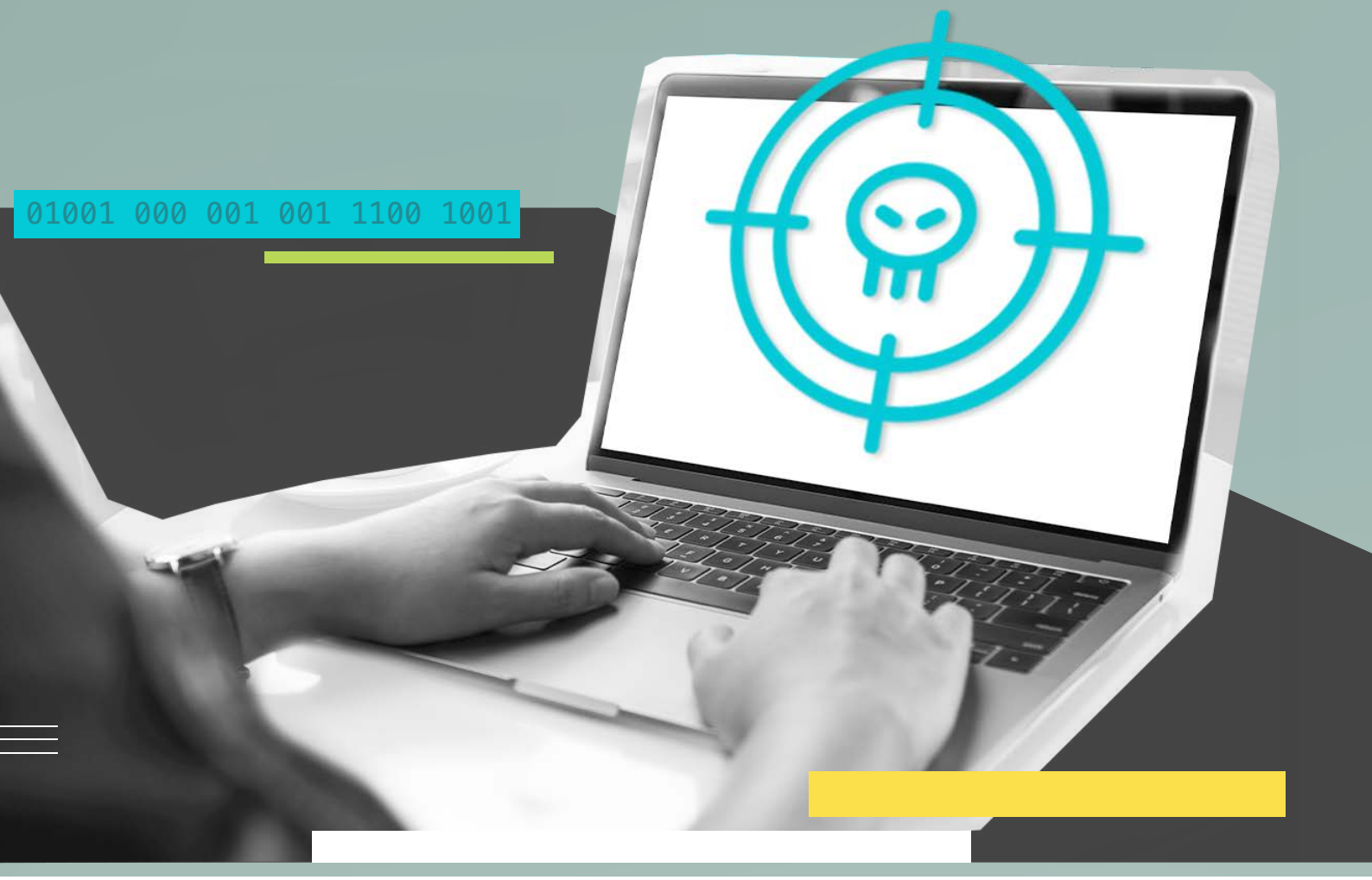
solarwinds msp

zaltor
Software Distribution



LIBRO ELECTRÓNICO

EDR o antivirus: ¿cuál es la solución ideal?

EDR o antivirus: ¿cuál es la solución ideal?

Hay diferencias considerables entre los antivirus y las herramientas de detección y respuesta en endpoints. Ambas protegen los endpoints frente a las ciberamenazas, aunque de formas diferentes. En uno de nuestros libros electrónicos, hemos analizado las diferencias a fondo. Vamos a resumirlas rápidamente aquí.

Soluciones antivirus:

- Protegen frente a malware y virus. Esta protección suele requerir un archivo que analizar.
- Tradicionalmente, dependen de firmas de virus. Esto quiere decir que el proveedor del antivirus debe haber detectado el software malicioso, enviado una actualización de firmas a su base de usuarios y el usuario final debe contar con sus firmas de virus actualizadas.
- Requiere que el administrador ejecute análisis de forma regular.
- Su coste suele ser inferior al del la EDR.

Soluciones EDR:

- Protegen frente a varios vectores de ataques, entre los que se incluyen los ataques sin archivos, los documentos maliciosos y los scripts maliciosos ejecutados fuera de una ventana de análisis. Para ello, utilizan IA para analizar los comportamientos.
- Busca de forma activa amenazas potenciales en lugar de depender de análisis. Si detecta actividad sospechosa, le alertará prácticamente en tiempo real (si la alerta está garantizada).
- Respuestas automáticas a amenazas potenciales. SolarWinds® Endpoint Detection and Response (EDR) le ofrece incluso la posibilidad de revertir los endpoints basados en Windows a estados seguros conocidos en un instante tras sufrir un ataque de ransomware.
- Su coste por puesto es ligeramente superior al del antivirus tradicional.

Cuando hablamos sobre el antivirus tradicional y la EDR, esta última puede parecer la mejor opción, ya que ofrece una cobertura más integral y algunas mejoras sobre las opciones de corrección. Sin embargo, en el mundo actual hay espacio para ambas soluciones. SolarWinds MSP le ofrece las dos opciones para que pueda decidir cuál funciona mejor para sus clientes. Pero, ¿cómo elegir?

Una estrategia basada en el riesgo

Ofrecer la cobertura más amplia que proporcionan las soluciones EDR va a reforzar la seguridad del cliente. Si es posible, debería vender esta solución a sus clientes, ya que ofrece una mayor protección a los endpoints. Además, podrá cobrar más por la solución y así compensar el coste por puesto para su empresa.

Sin embargo, no todos los clientes van a estar dispuestos a abonar un precio más elevado. Por lo tanto, merece la pena desarrollar una estrategia pragmática. Esto implica comprender los riesgos de los clientes y desarrollar planes en consecuencia. Aunque las estrategias basadas en el riesgo suelen desarrollarse para conservar los recursos administrativos tecnológicos y de seguridad o para proporcionar una experiencia a los usuarios menos intrusivas (piense de forma estratégica a la hora de usar autenticación multifactor para los ejecutivos o administradores del sistema), el riesgo también puede guiar sus decisiones en lo relativo a los recursos financieros.

En definitiva, tendrá que tener en cuenta los usuarios a los que está protegiendo, su acceso a los datos confidenciales y las consecuencias de la pérdida de esta información importante.

Para disponer de un contexto mejorado, tenga en cuenta estos perfiles:

- **Gestor de recursos humanos:** es muy probable que esta persona cuente con datos personales en su equipo, un tipo de información cuya confidencialidad debe garantizarse. Dispondrán de acceso a registros de nóminas, números de la Seguridad Social, direcciones e información confidencial en sus historiales de trabajo. Si un cibercriminal accede a estos, los individuos y las empresas podrían sufrir daños catastróficos. Por lo tanto, es probable que un gestor de recursos humanos necesite una protección más sólida que la que proporciona el antivirus, lo que incluye la posibilidad de interrumpir un proceso de forma automática, poner en cuarentena un archivo y desconectar el endpoint de la red para evitar la propagación de la amenaza. En este caso, la EDR es la elección obvia. El riesgo y el coste potencial de un ataque que se ejecute con éxito justifican el gasto extra.

- **Diseñador gráfico:** este individuo probablemente cuenta con archivos y documentos importantes, pero es probable que no almacene una cantidad significativa de datos personales en su equipo. Asimismo, su trabajo no es tan urgente como el de otros puestos. Por ese motivo, si tiene que esperar varias horas a que genere una nueva imagen de sus unidades, esto le supondrá una molestia, pero la empresa no sufriría como en el caso de un puesto orientado al cliente. En este caso, una combinación de antivirus, copia de seguridad y cifrado de disco proporciona una sólida defensa por capas. Aunque la EDR ofrece una excelente cobertura, el antivirus sigue ofreciendo una defensa excepcional con un coste menor para este perfil de usuario de menor riesgo.

- **Ejecutivo:** en caso de acceso no autorizado, este perfil cuenta con el mayor riesgo. Para empezar, pueden disponer con facilidad de acceso a datos personales en sus sistemas, así como a datos de la empresa y de propiedad intelectual muy valiosos. En este caso, no solo es necesario proteger los datos, sino que también es esencial poder recuperarlos con rapidez mediante una opción de reversión. Sin embargo, considere otra posibilidad. Imagine que establecen una conexión remota con el equipo del CEO e instalan spyware de difícil detección o crean una cuenta de administrador superusuario sin que este se dé cuenta. Esto podría otorgar un poder considerable al cibercriminal, ya que podría emplear este acceso para comprometer el resto de la empresa. Una solución EDR puede contribuir a evitar estos tipos de amenazas. En definitiva, en el caso de un usuario de alto riesgo como un ejecutivo, la protección de sus equipos con EDR es la opción más segura.

A la hora de tomar una decisión, no tiene que elegir entre una y otra opción de forma exclusiva. Si bien la EDR ofrece una mejor protección, si tiene que realizar concesiones, puede hacerlo de forma estratégica.

Las objeciones respecto al coste

Para ser objetivos, tenemos que tener en cuenta la cuestión del coste. El coste de la EDR por licencia es superior al del antivirus, pero no es algo prohibitivo. En SolarWinds RMM, el precio por plaza para la EDR puede ser más alto que el del antivirus, pero no mucho más. Algunos clientes pueden negarse a pagar el coste extra, sobre todo si tienen la sensación de que todo va bien. Sin embargo, los cibercrímenes no dejan de incrementar, tanto en presencia como en el nivel de daños que provocan. Las organizaciones pueden no ser conscientes de las amenazas a las que se enfrentan o del daño que puede causar un ataque que se ejecute con éxito. Por ejemplo, un ataque de ransomware puede propagarse dentro de una red muy rápido, para cuya reconstrucción se requerirán grandes cantidades de tiempo. Cuando la EDR evita un ataque de este tipo, justifica su precio por completo.

Si su cliente no dispone de protección de endpoints, merece la pena asesorarles para que saquen partido a la propuesta de valor que ofrece la EDR. Su cliente no tendrá que asumir costes de actualización asociados al paso de antivirus a la EDR y la tranquilidad añadida justifica la elección de sobra. Asimismo, en el caso de sus servidores, debe tratarlos de la misma forma que los recursos de alto valor que contiene. La EDR es su mejor opción.

Si detecta resistencia a la adopción de la EDR en función del coste, no se centre en lo que pierde el cliente, sino en lo que va a ganar: tiempo. Los procesos de reversión suelen tardar menos de un minuto frente a las cuatro o seis horas necesarias para recuperar cada dispositivo a partir de una imagen. Además, dispondrá de información sobre qué ha sucedido. Esto puede ayudarle a adoptar contramedidas para evitar amenazas similares en el futuro, lo que le permitirá ofrecer servicios de seguridad proactivos y sólidos, así como convertirse en el consultor que necesitan.

Por último, si bien el antivirus puede seguir desempeñando un papel, es importante tener en cuenta el riesgo para su propio negocio de no fomentar la adopción de la protección adicional. Si se enfrenta a un ataque, es muy probable que pueda perder un cliente. Sus clientes recurren a sus servicios porque consideran que es un experto. Incluso aunque tengan en cuenta el precio, quieren resolver sus problemas, entre los que se incluye la seguridad. Si no les anima a adoptar un entorno de protección más completo, se arriesga a sufrir un ataque que podría provocar que pierda el cliente.
Algunos clientes que tienen en cuenta los costes decidirán no adoptar la protección que ofrece la EDR y tendrá que mantener el antivirus para obtener ingresos. Sin embargo, merece la pena mencionar que sus relaciones con los clientes pueden basarse en algo más que ofrecer una protección más integral.

Para terminar

Hay espacio tanto para los antivirus como para la EDR. Sin embargo, con la innovación que ofrece esta última y la forma en la que gestiona el clima de amenazas actual, no debería sorprenderle que las soluciones EDR lleguen a sustituir a los antivirus como el estándar del sector. La diferencia en el coste es lo suficientemente pequeña como para que las mejoras justifiquen con facilidad un uso más generalizado de la EDR.

Por último, si bien la característica de reversión en SolarWinds EDR es muy útil en escenarios de ransomware, esta no sustituye a una buena solución de copia de seguridad basada en la nube. Realizar copias de seguridad de forma regular, almacenarlas en una ubicación externa y ejecutar pruebas de recuperabilidad deberían ser prácticas que formasen parte de cualquier práctica de ciberhigiene. Las soluciones para copias de seguridad protegen frente a mucho más que estas amenazas: la eliminación de datos accidental o maliciosa por parte de

personal de la empresa, fallos de software y hardware o situaciones de fuerza mayor como los desastres naturales. Asimismo, la reversión solo está disponible para los PC y portátiles Windows de software.

En definitiva, dispone de opciones entre las que elegir: EDR o antivirus. Incluso puede combinarlas y adaptarlas en función de las demandas de los clientes. Independientemente de su elección, SolarWinds MSP puede ayudarle.

SolarWinds RMM con EDR integrada

SolarWinds RMM ofrece tanto antivirus administrado como SolarWinds EDR a través del mismo panel basado en web. Tanto si sus clientes quieren disfrutar de las características ampliadas de la EDR o simplemente necesitan antivirus, puede proporcionar estos servicios a su base de clientes mediante el mismo panel basado en web que utiliza para supervisar y administrar su infraestructura de TI. Además, puede acceder a otras capas de seguridad integradas, como la administración de parches, la protección del correo electrónico, la protección web y la copia de seguridad integrada, puede ofrecer a sus clientes una seguridad mejorada sin llevar a su equipo más allá de sus límites.

Si desea obtener más información acerca de nuestra integración con SolarWinds EDR, visite:
https://zaltor.com/solarwinds-edr/

zaltor
Software Distribution

PÓNGASE EN CONTACTO CON NOSOTROS
ZALTOR Mayorista de Soluciones TIC
Teléfono: +34 916 625 945
Av. de la Industria 4, Edif. 1 · 28108 · Alcobendas · Madrid
Correo electrónico: comercial@zaltor.com

solarwinds msp

Obtenga más información hoy mismo en ***solarwindsmsp.com/es***

SolarWinds (NYSE:SWI) es un proveedor líder de software de administración de TI potente y asequible. Nuestros productos ofrecen a empresas de todo el mundo, independientemente de su tipología, tamaño o complejidad de TI, la capacidad de supervisar y gestionar el rendimiento de sus infraestructuras y aplicaciones, tanto si son locales como en la nube o a través de modelos híbridos. Trabajamos continuamente con profesionales del sector tecnológico (profesionales de mantenimiento y operaciones de TI, desarrollo y proveedores de servicios gestionados o MSP), con el fin de comprender los retos a los que se enfrentan a la hora de mantener aplicaciones e infraestructuras de TI de alto rendimiento y disponibilidad. Orientado a los MSP, el catálogo de productos de SolarWinds MSP ofrece soluciones de administración de servicios de TI amplias y escalables que integran seguridad por capas, inteligencia colectiva y automatización inteligente. Nuestros productos se han diseñado para permitir que los MSP proporcionen servicios de TI externalizados altamente efectivos para sus consumidores finales (pymes), así como para gestionar sus propios negocios de manera más eficaz.