CYBERSECURITY
EXPERTS ON YOUR SIDE

¿CÓMO ELEGIR LA SOLUCIÓN PARA ENDPOINTS CORRECTA?

La seguridad de su organización, datos y usuarios finales depende de que elija la solución de seguridad para endpoints apropiada. Si toma la decisión equivocada, pasará mucho más tiempo del que pensaba administrando la solución, reparando el sistema tras cada infección y manejando las quejas de los usuarios. Por eso preparamos esta guía, con información que le servirá para tomar la decisión correcta, evitando los peligros potenciales y haciendo la mejor elección para su organización y para quienes la administran.

Comienzo de la investigación

Los expertos siempre recomiendan: a) hacer la evaluación *in situ*, es decir en el entorno corporativo propio, para asegurarse de que el producto no interfiera con los procesos que se ejecutan en los sistemas; b) crear una lista de las soluciones que desea probar.

Aquí le damos algunos consejos que le serán de ayuda:

El significado de los nombres. A medida que comience su investigación, descubrirá que los productos se autodenominan antivirus, *antimalware* o de seguridad para *endpoints*. El término **antivirus** sigue siendo el más utilizado para designar estos productos de seguridad, a pesar de que las soluciones modernas han evolucionado y ahora detectan y lo defienden de mucho más que solo virus. El término ***antimalware*** describe una protección ante tipos más amplios de amenazas; y la **seguridad para endpoints** es aún más amplia. Más allá del nombre, la mayoría de los productos lo protegerán de todas las amenazas maliciosas, incluyendo *malware*, *ransomware* y virus. Por lo tanto, no se quede con la etiqueta que le ponen a los productos.

Ir más allá de las palabras de moda. También se encontrará con términos tales como heurística, sistemas expertos, redes neuronales, análisis de la reputación y otros que se basan en la inteligencia artificial, o que al menos suenan inteligentes. Los proveedores también mencionan lo que están haciendo en la nube, ya sea detección, administración, recopilación de datos telemétricos, licenciamiento o una combinación de algunos o todos ellos. No confíe a ciegas en las palabras de moda del proveedor; busque una explicación sólida de la tecnología que utiliza cada uno. El blog **WeLiveSecurity de ESET** es un excelente recurso para comprender muchos de estos términos. Una vez que logre abrirse paso a través de las palabras de moda, probablemente descubrirá que muchos productos utilizan una tecnología similar. El nombre que le pongan a las tecnologías no es lo importante, la clave está en lo bien que las implementen.

Reseñas (favorables o no). Las reseñas de productos son útiles, pero tenga en cuenta que algunos sitios online ofrecen revisiones pagas que a menudo solo se basan en una mirada superficial del producto. Busque fuentes de reseñas imparciales basadas en la experiencia del mundo real, como la comunidad de *Spiceworks o Gartner Peer Insights*.

El papel de la evaluación independiente

Para probar los productos de seguridad, los servicios de evaluación de terceros los bombardean con un conjunto de malware dentro de un entorno controlado. En su lista de candidatos debe

incluir los productos que obtengan siempre una buena puntuación en estas pruebas.

Cuando visite estos sitios, no mire solamente los resultados más recientes, lea los informes y estudios a lo largo de varios años. Tenga en cuenta que los resultados de las pruebas solo son válidos para el período en el que fueron realizadas, y para la configuración y el entorno específicos elegidos por la entidad evaluadora. A veces a un producto le puede ir mal debido a una peculiaridad de la metodología de evaluación o la plataforma utilizada para la prueba. Mire los resultados a lo largo de algunos años y vea si la solución tiene un historial consistente de éxito.

Las organizaciones de pruebas establecidas y respetadas que recomendamos son ***AV-Comparatives***, ***SE Labs*** y ***Virus Bulletin***, por las siguientes razones:

- Cada una tiene una metodología diferente de prueba, por lo que en conjunto le darán una visión completa del producto;
- Todas han estado probando productos de seguridad desde hace muchos años (como Virus Bulletin que lo hace desde la decada de 1990)
- No solo prueban la detección, sino también la incidencia de falsos positivos y el impacto en el rendimiento del sistema (hay más información sobre esto a continuación).

Consejos para probar los productos

Una vez que haya confeccionado la lista de candidatos, siga estos consejos de expertos en seguridad para probarlos. Asegúrese de hacer las preguntas correctas y probar las cosas correctas, y no pase nada por alto de lo que se pueda arrepentir luego.

Antes que nada, ¿hace falta probar el producto? Aunque existe una tendencia entre los profesionales de TI de prescindir de las pruebas, los expertos en seguridad siempre recomiendan probar la solución para endpoints antes de implementarla definitivamente. Es importante poder asegurar que el producto tenga un buen desempeño en su entorno específico, que funcione bien con sus sistemas y que el soporte técnico esté allí cuando lo necesite, antes de comprometerse a implementarlo en todos sus sistemas y firmar un contrato de varios años.

¿Cuántos productos hay que probar? Tres es un buen número debido a la gran cantidad de tiempo que lleva probar adecuadamente cada producto en secuencia. Podría considerar probar más productos si tiene una organización lo suficientemente grande y cuenta con bastante personal de TI para probarlos en paralelo.

Cómo probar los productos. Póngase en contacto con cada proveedor y solicite una prueba de 30 días. Para cada uno de ellos, haga una prueba piloto con un pequeño grupo de usuarios de distintos departamentos. No solo debe incluir los "usuarios avanzados" y de TI o técnicos, sino también a personas sin conocimientos técnicos. Además, realice pruebas con usuarios que utilicen distintos tipos de programas de línea de negocio, *software* propietario, programas heredados y otros "servicios únicos" en todos los sectores de su organización. Tómese el tiempo para evaluar las soluciones a fondo teniendo en cuenta todos los casos de uso de su entorno.

Consideraciones clave: ¿qué buscar?

En su investigación *online*, al comunicarse con los proveedores y al probar el *software* usted mismo, estos son los elementos clave que debe buscar, según los expertos:

Tasas de detección. Sin duda deseará que su *software* de seguridad sea capaz de detectar todas las amenazas que ingresan a su red. Como la mayoría del *malware* está diseñado para evadir la detección, no siempre sabrá si algo ha penetrado las defensas del *software* de seguridad a menos que el sistema de un usuario se ralentice o muestre un comportamiento errático, o si audita regularmente el tráfico de su red. Los resultados de las pruebas independientes pueden ser su mejor guía en este caso. Desconfíe de los proveedores que le

proporcionan muestras de *malware* para realizar pruebas: normalmente, sus muestras fueron creadas específicamente para que solo sus productos las detecten como maliciosas. Y si va a utilizar *malware* real para realizar pruebas, sea precavido y use una máquina de uso exclusivo para la prueba que se encuentre aislada del resto de su red y que no contenga datos valiosos.

Incidencia de falsos positivos. Un falso positivo es una alerta sobre un archivo o vínculo que en realidad no es malicioso. Algunos miembros de la industria de seguridad sostienen que no constituyen un problema grave, pero sí lo son. Un solo falso positivo puede tener serias consecuencias. Si una solución antivirus está configurada para eliminar o poner en cuarentena los archivos infectados de inmediato, cuando detecta un falso positivo en un archivo crucial del sistema es posible que impida el funcionamiento del sistema operativo o de algunas aplicaciones importantes. Y por más que los falsos positivos no generen fallos en sus sistemas, cada uno de ellos requerirá una investigación que desperdiciará valiosos recursos de TI. Si aún así elige un producto que detecta falsos positivos, pasará mucho tiempo persiguiendo amenazas inexistentes, y posiblemente volverá a crear imágenes y restaurar sistemas que no necesitan ser tocados en absoluto.

Impacto en el sistema. Las distintas soluciones de seguridad varían ampliamente en la cantidad de recursos del sistema que consumen en términos de memoria, espacio en disco, carga del procesador e impacto en la red. Durante su evaluación, preste atención a las quejas de los usuarios. Si las actualizaciones o los análisis del antivirus tienen un impacto notable en el rendimiento del sistema, lo sabrá a medida que los usuarios noten que sus equipos se ralentizan y afectan la capacidad para realizar su trabajo. La ralentización del sistema no es un precio que debe pagar por tener seguridad. Tampoco debería tener que renovar las máquinas antiguas solo para poder ejecutar el software de seguridad.

Compatibilidad. Asegúrese de que la solución funcione bien con sus aplicaciones propietarias esenciales y otro *software*, herramientas y servicios que utilice su organización. Un problema grave es que la solución bloquee las computadoras al realizar ciertas tareas. Asimismo, también puede ocurrir que surjan problemas al instalar el software o directamente no pueda instalarlo por incompatibilidad con el sistema operativo. Preste especial atención al *hardware* más antiguo: ¿la solución genera conflictos con algún *software* o *hardware* específico? Verifique que funcione de manera discreta sin afectar el rendimiento.

Costo vs. funcionalidad. El precio es siempre una consideración a la hora de elegir un producto. Si bien la mayoría de los programas de seguridad detectan las diversas formas de malware, algunos proveedores cobran aparte por la protección contra ransomware, así que asegúrese de preguntarles qué incluye la solución. También preste atención al valor total del paquete. Las funcionalidades como la protección *antimalware* para unidades USB, el control Web para bloquear amenazas provenientes de sitios maliciosos y el *firewall* de *software* para bloquear el tráfico malicioso de la red o evitar la propagación de amenazas suministran niveles adicionales de seguridad y vale la pena tenerlas.

Facilidad de administración y mantenimiento. Preste especial atención a esta consideración. No querrá tener que pasar el día corriendo de una máquina a otra para configurar, administrar, actualizar y mantener la seguridad en todos los sistemas de su entorno. Busque un producto con la capacidad de administrar todas las endpoints desde una consola central, impulsar actualizaciones, automatizar tareas rutinarias (como crear e implementar configuraciones), y elaborar rápidamente los informes que necesita.

Seguridad para móviles. Es inevitable que se usen dispositivos móviles en las operaciones laborales, más allá de que les proporcione los dispositivos a sus empleados, tenga alguna política formal para que usen sus propios dispositivos para trabajar, o los usen sin ni siquiera tener una política. Fíjese que la solución proteja todas las plataformas de sus empleados, ya sea *Android, Windows o iOS*, y pruébela en todas ellas. Por otra parte, la gestión centralizada

es imprescindible para administrar los dispositivos móviles. Si la solución tiene la capacidad de bloquear y desbloquear dispositivos en forma remota, y borrar el contenido de aquellos perdidos o robados, será una gran ventaja, ya que de esta forma evita el costo de una herramienta de administración para dispositivos móviles por separado.

Facilidad de implementación. Cuando realice sus pruebas, preste atención a la cantidad de tiempo requerido para que la solución funcione correctamente. ¿Elimina automáticamente el producto *antimalware* anterior? De no ser así, le puede traer problemas cuando llegue el momento de implementarla en toda la organización. Además, si la solución ya viene preconfigurada para garantizar las mejores prácticas desde el momento de su instalación, se ahorrará muchas configuraciones y ajustes.

Respuesta del soporte. Ponga a prueba el sistema de soporte del proveedor. Durante el período de prueba, haga algunas llamadas al soporte y abra tickets en escenarios típicos. ¿Es fácil comunicarse y resolver el problema? Si el soporte se hace desde un centro subcontratado ubicado en el extranjero, ¿con qué facilidad y rapidez estos representantes comprenden y resuelven sus inquietudes?

Consejos para probar el soporte técnico

La última consideración es fundamental: el buen soporte técnico es como una póliza de seguro para su solución de seguridad. ¿Qué ocurre si surge un problema que usted no puede resolver en el equipo portátil del presidente de la compañía justo antes de que salga de viaje de negocios? Querrá saber de antemano que el soporte técnico del proveedor lo va a ayudar.

A continuación le damos algunos consejos de expertos para poner a prueba el soporte técnico:

- Configure una computadora con la red incorrecta, no desinstale el *software antimalware* anterior antes de instalar el producto evaluado, o encuentre alguna otra forma de "romper" la instalación. Luego llame al soporte y solicite ayuda para solucionar el problema
- Desactive el *software* de seguridad en una máquina, inféctela a propósito, luego solicite al soporte que lo guíen paso a paso para desinfectarla
- Pruebe otros escenarios que le hayan resultado difíciles con su solución actual y vea si el nuevo vendedor lo maneja mejor (o peor).

No dude en solicitar soporte técnico durante su prueba gratuita. Es importante que sepa cómo responde el proveedor antes de tener un problema real con el *software* para el que ha invertido en una licencia de varios años.

Impacto empresarial

Una vez que haya tomado su decisión, todavía tendrá que hacer una revisión cautelosa, como leer detenidamente el contrato en busca de trampas ocultas, confirmar la compatibilidad con los sistemas operativos más antiguos y con los futuros lanzamientos del sistema operativo durante la vigencia del contrato. Estos detalles subrayan un punto importante: **la elección de una solución de seguridad para endpoints no es solo una decisión tecnológica, sino también comercial**. El costo de la solución de seguridad y la protección que ofrece son elementos esenciales en la decisión, pero recuerde no pasar por alto los costos ocultos, como el impacto en la productividad de sus trabajadores y el tiempo que le toma al equipo de TI administrarlo. También es importante evaluarlos, de modo que pueda tomar una decisión experta a nivel técnico y comercial que sea completa, integral e informada.

CYBERSECURITY EXPERTS ON YOUR SIDE

Por más de 30 años, ESET® ha estado desarrollando soluciones de seguridad para las empresas y los usuarios de todo el mundo, que van desde la protección de endpoints y dispositivos móviles, hasta el cifrado y la autenticación en dos fases. Los productos de alto rendimiento y fáciles de usar de ESET les ofrecen a los usuarios y a las empresas la tranquilidad que necesitan para disfrutar de su tecnología sin riesgos. ESET brinda protección y supervisión las 24 horas, los 7 días de la semana, y actualiza las defensas en tiempo real para mantener a los usuarios seguros y a las empresas funcionando sin interrupciones. Para obtener más información. Para obtener más información, visite www.eset.com/latam.