CYBERSECURITY
EXPERTS ON YOUR SIDE

9 SEÑALES DE QUE SU ANTIVIRUS ES INEFICIENTE

¿Cómo puede saber si su empresa esta expuesta?

Si alguna de estas nueve señales le resulta familiar, es hora de que reconsidere la protección actual de sus equipos.

1 Las exploraciones y actualizaciones ralentizan el sistema.

Una de las principales quejas sobre los productos de seguridad para endpoints es que afectan la velocidad y el rendimiento. Algunas soluciones ralentizan los sistemas y tienen un fuerte impacto en la productividad. Cuando evalúe las soluciones del mercado, no olvide verificar los resultados de las pruebas independientes que miden el rendimiento y el impacto en el sistema. Busque los valores más bajos, ya que pertenecen a soluciones livianas que no afectarán la velocidad de sus equipos ni causarán interrupciones.

Entre otros premios, ESET continúa ganando las pruebas de rendimiento, que demuestran lo liviana que es nuestra solución. ***ESET ha ganado la Prueba de rendimiento de AV-Comparatives en forma consistente.***

2 Los colaboradores se quejan de la solución antivirus.

Si el resentimiento se acumula, los empleados eventualmente tratarán de evadir la solución por completo en los dispositivos otorgados por la empresa o en los propios que usan para trabajar, lo que puede afectar no solo el rendimiento sino también la seguridad de toda la red.

3 La solución no funciona como debería.

No detecta virus u otros tipos de malware o marca los archivos no maliciosos como malware; tiene un alto impacto en el sistema, lo que provoca una exploración más lenta; crea tormentas antivirus en las máquinas virtuales; o usa demasiado ancho de banda y atasca toda la red.

4 La solución genera alertas sobre archivos que no son maliciosos.

Al detectar tantos archivos o vínculos no maliciosos, la solución provoca una alta tasa de los llamados falsos positivos.

Un solo falso positivo puede provocar graves problemas. 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 aunque los falsos positivos no lleguen a cerrar su sistema, cada uno requerirá una investigación que desperdiciará valiosos recursos de TI.

ESET es conocido en toda la industria por su baja tasa de falsos positivos. De hecho, ganó todas las pruebas de falsas alarmas de AV-Comparatives desde 2015, un total de seis.

5 La protección de endpoints no es productiva ni eficiente.

Un estudio* realizado en 2017 por el Instituto Ponemon demostró que:

- 3 de cada 4 organizaciones informan tener más dificultades para administrar los riesgos de seguridad de las endpoints.
- Casi la mitad de todas las alertas de seguridad son falsos positivos y las organizaciones ven los falsos positivos como el costo "oculto" número 1 de la protección de endpoints.

Necesita una solución que ponga los archivos en cuarentena en forma silenciosa y que elimine los maliciosos automáticamente, sin causar más trabajo a su equipo de TI.

6 Las infecciones vuelven tras haberlas erradicado.

Esto significa que la solución no está haciendo un buen trabajo de desinfección o no se actualiza con suficiente frecuencia.

7 La administración de la solución es compleja.

En los entornos actuales, necesita una solución de seguridad que sea fácil de administrar para minimizar la carga de trabajo. Busque un producto de seguridad para endpoints que tenga administración remota, de modo que pueda controlar toda su red de estaciones de trabajo, servidores y teléfonos inteligentes desde una única ubicación.

Por ejemplo, ESET Security Management Center o ESET Cloud Administrator (nuestra solución basada en la nube) se incluyen con todos los productos de ESET de seguridad para endpoints. Le permiten:

- Proteger los datos y dispositivos de todos los empleados, dondequiera que estén
- Bloquear, desbloquear o borrar el contenido de los dispositivos en forma remota en caso de pérdida o robo
- Administrar de manera efectiva todo el personal de su empresa en un entorno multiplataforma.

8 Las alertas de seguridad interrumpen las presentaciones y demostraciones comerciales.

Todos los colaboradores necesitan acceso ininterrumpido al equipo, por esa razón la solución de malware debe tener un modo *"silencioso"* o *"de presentación"* que sea fácil de usar, así como una herramienta confiable para restaurarse al modo normal cuando finaliza la misma.

9 La atención de soporte técnico no es accesible.

Si es difícil obtener soporte confiable o si tiene problemas con los call centers, eso afectará la productividad de los equipos de TI y los usuarios finales. Estas situaciones a su vez hacen que los empleados se frustren, lo que los lleva a eludir la solución de seguridad, en cuyo caso los dispositivos (y la red) quedarán a merced de posibles ataques cibernéticos.

* Informe "Los riesgos de la seguridad para endpoints 2017", por el Instituto Ponemon

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, visite ***www.eset.com/latam***