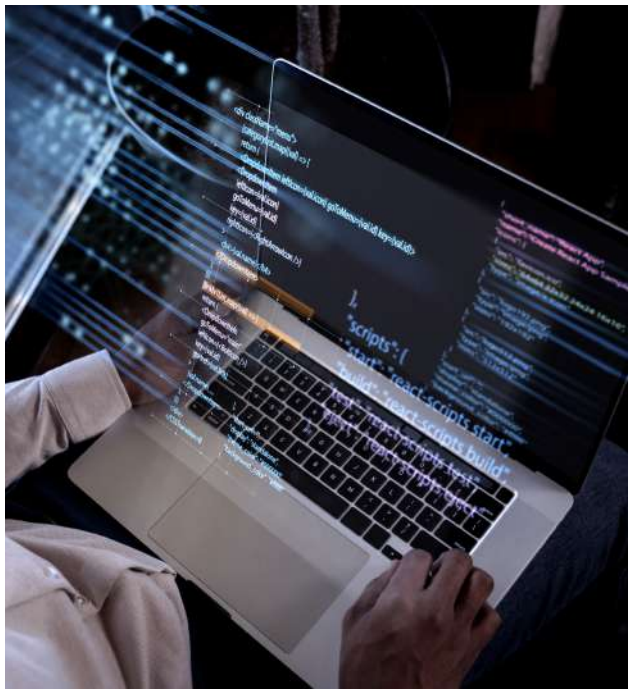
¿Por qué es importante la seguridad de endpoints?



En los últimos años aumentó el número de endpoints en las empresas.

Esto es especialmente cierto desde la pandemia de COVID-19, que provocó un aumento del trabajo a distancia en todo el mundo.

Dado que cada vez más empleados trabajan desde casa o se conectan a redes Wi-Fi públicas en sus desplazamientos, las redes empresariales tienen ahora más endpoints que nunca. Y cada endpoint puede ser un punto de entrada potencial para los ataques.
Empresas de todos los tamaños pueden ser blanco de ciberataques. Cada vez es más difícil protegerse de los ataques que ingresan por endpoints como computadoras portátiles o dispositivos móviles.

Estos dispositivos se pueden hackear, lo que a su vez puede dar lugar a filtraciones de datos. **Se calcula que el 70 % de las filtraciones de datos se originan en dispositivos de endpoint.**

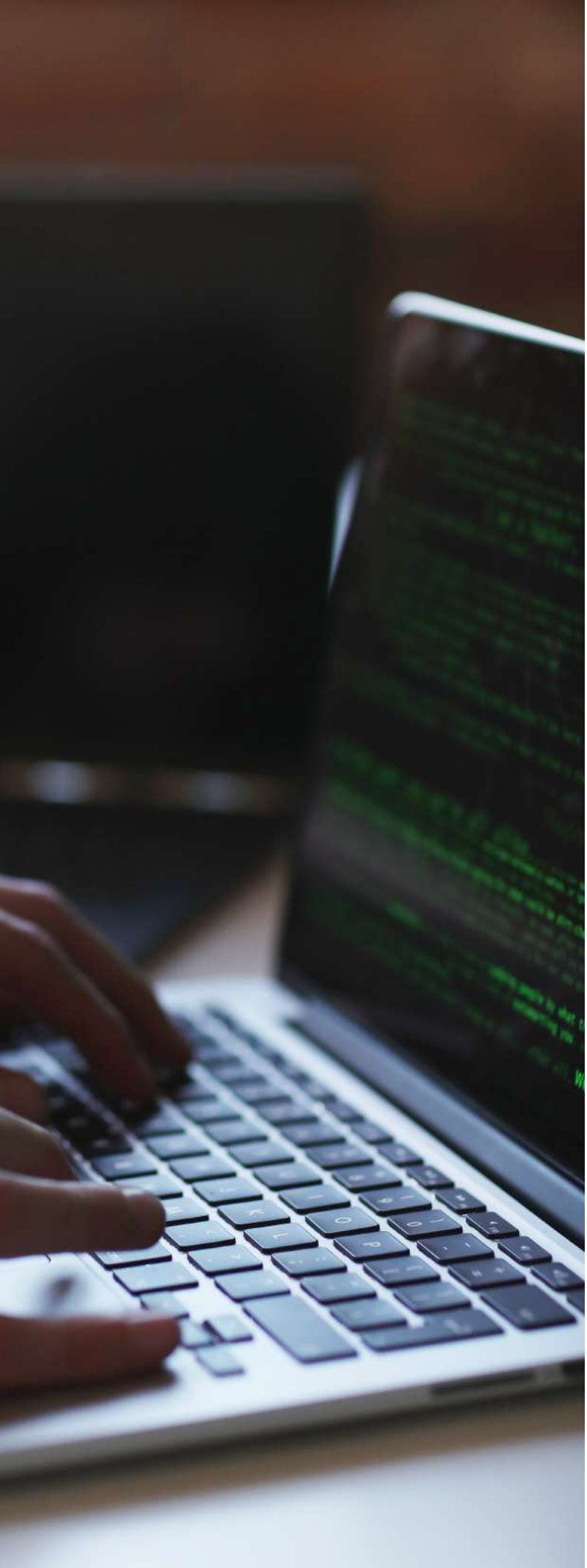
Además de causar daños a la reputación, las filtraciones de datos pueden ser costosas: Un informe descubrió que el costo medio mundial de una filtración de datos es de 3.86 millones de dólares (y más en Estados Unidos).

Los datos suelen ser el activo más valioso de una empresa, y perderlos, o el acceso a estos, puede poner en peligro todo el negocio.

No solo está aumentando el número de endpoints, impulsado por el incremento del trabajo a distancia, sino que las empresas también tienen que hacer frente a un aumento del número de tipos de endpoints, gracias al crecimiento del Internet de las cosas.

Las empresas necesitan proteger sus datos y garantizar la visibilidad de las ciberamenazas avanzadas. Pero muchas pequeñas y medianas empresas carecen de recursos para supervisar continuamente la seguridad de la red y la información de los clientes, y a menudo solo se plantean proteger su red cuando ya se produjo una filtración.

Incluso entonces, las empresas pueden centrarse en su red e infraestructura, dejando desprotegidos algunos de los elementos más vulnerables, es decir, los dispositivos de endpoint.



Los riesgos que plantean los endpoints y sus datos confidenciales constituyen un reto permanente para la ciberseguridad. Además, el panorama de los endpoints está evolucionando, y las empresas, ya sean pequeñas, medianas o grandes, son blanco de ciberataques.

Por eso es importante entender qué es la seguridad de los endpoints y cómo funciona.

¿Cómo funciona la seguridad de los endpoints?

Los términos protección de endpoints, seguridad de endpoints y plataformas de protección de endpoints suelen utilizarse indistintamente para referirse a las soluciones de seguridad gestionadas de forma centralizada que las organizaciones utilizan para proteger los endpoints.

La seguridad de los endpoints funciona examinando archivos, procesos y sistemas en busca de actividades sospechosas o maliciosas.

Las organizaciones pueden instalar una plataforma de protección de endpoints (EPP) en los dispositivos para impedir que los actores maliciosos utilicen malware u otras herramientas para infiltrarse en sus sistemas.

Un EPP puede utilizarse junto con otras herramientas de detección y supervisión para señalar comportamientos sospechosos y prevenir las infracciones antes de que se produzcan.

La protección de endpoints ofrece una consola de gestión centralizada a la que las organizaciones pueden conectar su red. La consola permite a los administradores supervisar, investigar y responder a posibles ciberamenazas.
Esto puede lograrse mediante un enfoque in situ, en la nube o híbrido:

In situ

Un enfoque local o en las instalaciones implica un centro de datos alojado localmente que actúa como un centro para la consola de gestión.

Esto llegará a los endpoints a través de un agente para proporcionar seguridad.

Este enfoque se considera un modelo heredado y presenta inconvenientes, como la creación de silos de seguridad, ya que los administradores normalmente solo pueden gestionar los endpoints dentro de su perímetro.

En la nube

Este enfoque permite a los administradores supervisar y gestionar los endpoints a través de una consola de gestión centralizada en la nube, a la que los dispositivos se conectan de forma remota.

Las soluciones en la nube aprovechan las ventajas que tiene para garantizar la seguridad detrás del perímetro tradicional, eliminando silos y mejorando el alcance de los administradores.

Híbrido

Un enfoque híbrido combina soluciones in situ y en la nube. Este enfoque aumentó su prevalencia desde que la pandemia generó un aumento del trabajo a distancia.

Las organizaciones adecuaron su arquitectura heredada y adaptaron elementos de ella a la nube para obtener algunas capacidades de nube.

Los EPP que utilizan la nube para mantener una base de datos de información sobre amenazas liberan a los endpoints de la sobrecarga asociada al almacenamiento local de esta información y del mantenimiento necesario para mantener actualizadas estas bases de datos.

Un enfoque basado en la nube también es más rápido y escalable. Algunas grandes organizaciones pueden necesitar seguridad in situ por motivos normativos. Para las pequeñas y medianas empresas, probablemente sea más adecuado un enfoque basado en la nube.

El software de seguridad para endpoints suele incluir estos elementos:

- Aprendizaje automático para detectar amenazas de día cero;
- Un firewall integrado para evitar ataques hostiles a la red;
- Una pasarela de correo electrónico para protegerse de la suplantación de identidad y otros intentos de ingeniería social;
- Protección frente a las amenazas internas de la organización, ya sean malintencionadas o accidentales;
- Protección antivirus y antimalware avanzada para detectar y eliminar malware en todos los dispositivos endpoint y sistemas operativos;
- Seguridad proactiva para facilitar una navegación segura;
- Cifrado de endpoints, correo electrónico y disco para protegerse contra la filtración de datos.

En última instancia, la seguridad de los endpoints ofrece una plataforma centralizada para los administradores, lo que mejora la visibilidad, simplifica las operaciones y permite aislar rápidamente las amenazas.

Además de las siglas EPP, también encontrarás las siglas EDR en relación con la seguridad de los endpoints.

EDR son las siglas de "endpoint detection and response" (detección y respuesta de endpoints). En general, una plataforma de protección de endpoints o EPP se considera una protección pasiva contra amenazas, mientras que el EDR es más activa, ya que ayuda a investigar y contener las filtraciones que ya ocurrieron.

Un EPP protegerá cada punto final de forma aislada, mientras que un EDR proporcionará contexto y datos para ataques que abarquen varios endpoints.

Las plataformas modernas de seguridad de endpoints suelen combinar tanto EPP como EDR.

¿Qué se considera un endpoint?

Un endpoint de red es cualquier dispositivo que se conecta a la red de una organización desde fuera de su firewall. Algunos ejemplos de dispositivos endpoint son los siguientes:

- Equipos portátiles
- Tablets
- Computadoras de escritorio
- Dispositivos móviles
- Dispositivos de la Internet de las cosas
- Portátiles
- Impresoras digitales
- Escáneres
- Sistemas de punto de venta (POS, del inglés "point-of-sale")
- Dispositivos médicos

Básicamente, cualquier dispositivo que se comunique con la red central puede considerarse un endpoint.

El panorama de las amenazas es cada vez más complicado, ya que los hackers generan nuevas formas de acceder a la información y robarla o de engañar a los empleados para que revelen información confidencial.

Dado el daño financiero y a la reputación que puede causar una filtración de datos, la seguridad de los endpoints es imprescindible para las empresas de todos los tamaños.

Fuente de información: kaspersky.com