MICRO FOCUS

Hoja de producto

ZENworks Endpoint Security Management
ZENworks Full Disk Encryption

ZENworks Endpoint Security Management y ZENworks Full Disk Encryption

Son las seis de la mañana de un viernes. ¿Sabe dónde están sus puestos finales? Uno de ellos está siendo atacado por un hacker. Es un equipo portátil. Su empleado está en una cafetería con WiFi. Está navegando por la red, convencido de que no hay riesgo, porque el nombre de la conexión aparece como "WifiCafe". Pero se trata de una falsa conexión creada desde la mesa de al lado, y el responsable de esa fachada está ahora configurando un túnel que le dará línea directa a la base de datos de su empresa.

ZENworks Endpoint Security Management y ZENworks Full Disk Encryption de un vistazo

- **Cifrado:**
  Datos de cifrado en dispositivos portátiles
- **Seguridad dinámica:**
  Aplicar medidas de seguridad que evalúan los niveles de amenaza y responden de manera adecuada en función de quiénes son los usuarios y dónde están
- **Mantenimiento de la productividad y la seguridad:**
  Dotar a los usuarios de control sobre los recursos que necesitan para ser productivos, pero impedirles que puedan eludir directivas de seguridad
- **Se puede adquirir de forma independiente o como parte de:**
  ZENworks Suite

Alguien está accediendo a su sistema sin autorización y el usuario ni siquiera lo sabe. No sabía que podía ocurrir; pensaba que estaba seguro.

Se trata de un ataque de tipo intermediario o "man-in-the-middle". Un completo desconocido se acaba de apropiar de información —quién sabe de cuál ni de cuánta— de uno de los equipos portátiles de su empresa.

Los puestos finales pueden ser terroríficos

Los dispositivos de Endpoint (puesto final) plantean uno de los riesgos de seguridad más grandes para cualquier compañía. Esto se debe a que hasta un 70% de sus datos más valiosos se transporta de un lado a otro en dispositivos de puesto final.

No hablamos de proteger los dispositivos para que no se los lleven los ladrones (aunque también tenemos que detenerlos). Hablamos de brindar protección para evitar que le roben sus datos mientras el personal de su empresa utiliza esos dispositivos.

Los ataques de intermediario son solamente una de las muchas amenazas serias contra las que debe protegerse. Hay muchos otros, como:

- **Drive bombing.** Mediante esta técnica se busca que los usuarios conecten memorias USB "encontradas" o "gratis" en sus equipos, donde la ejecución automática libera virus de todo tipo sin que usted tenga la menor sospecha.
- **Thumb sucking.** Los usuarios almacenan sus datos en memorias USB, pero eso significa que los datos están fuera de su control. De esta forma, sus datos traspasan los límites de las directivas de seguridad.
- **Robo, puro y simple.** Alguien roba un portátil. Aún peor, los empleados que no sean de fiar pueden sacar partido de puestos finales poco seguros y aprovechar puntos vulnerables para beneficio propio, desde dentro de la empresa.
- **Hacking.** Alguien introduce código malicioso en los dispositivos de su empresa desde el exterior, con la esperanza de eludir el cortafuegos, entrar en la red e infectar por completo el sistema.

Usted trata de evitarlo. Puede establecer normas y directivas. Pero no puede asegurarse de que esas directivas se sigan a rajatabla. ¿O sí? El cifrado podría ser una buena opción, pero resulta demasiado costoso, y algún usuario podría perder su contraseña. Y, como

Necesita un modo de imponer el cumplimiento de las directivas que protegen su empresa. Porque en cuanto disponga de eso, no tendrá que limitarse a confiar en que el personal seguirá las reglas. Sabrá que lo harán, porque la directiva no permitirá otra cosa.

consecuencia, nadie podría acceder a los datos. Debe haber una solución.

Directivas de verdad

Lo cierto es que no es posible dejar a la responsabilidad de los empleados el mantenerse al margen de los problemas. Los hackers son un peligro obvio, pero el personal de la empresa plantea un riesgo equivalente. La mayoría no sabe utilizar los equipos informáticos de forma segura.

Necesita un modo de imponer el cumplimiento de las directivas que protegen su empresa. Porque en cuanto disponga de eso, no tendrá que limitarse a confiar en que el personal seguirá las reglas. Sabrá que lo harán, porque la directiva no permitirá otra cosa.

Una y otra vez.

Podrá cambiar esa directiva en cualquier momento, pero sus usuarios no. Ahí está la clave: no depende de ellos. Depende de la directiva.

Compensación de errores

Los usuarios van a cometer errores. Por ejemplo, pueden dejarse un portátil en el aeropuerto. Aunque siempre resulta caro y engorroso perder un dispositivo, gracias a Micro Focus® ZENworks® Full Disk Encryption se asegurará de que sus datos más valiosos sigan siendo indescifrables para cualquiera que se encuentre el portátil. Con Full Disk Encryption no tendrá que preocuparse de en qué parte del disco duro guarda los datos el usuario: todo el disco está cifrado.

Otro caso más mundano, pero mucho más común, es que el usuario pierda una contraseña. Con otro software de cifrado, no se trata solo de pasarse el día hablando con atención al cliente. Sin esa contraseña, su disco duro es tan impenetrable como una roca. Con ZENworks, es solo otro procedimiento más del servicio de asistencia técnica. Ayude al usuario a recuperar su contraseña o gestione usted mismo el dispositivo. De cualquier manera, el cifrado que protege sus datos no los bloquea.

Los buenos y los malos

Micro Focus ZENworks Endpoint Security Management es el método ideal para imponer directivas para dispositivos de puesto final. Sabe quiénes son sus usuarios y todo lo que deben (y no deben) hacer. Además, de manera exclusiva, también sabe dónde están sus usuarios en cada momento, y se ajusta dinámicamente al nivel de amenaza de cada situación.

Son las ocho de la mañana de un miércoles. ¿Sabe lo que el empleado del cubículo seis está copiando en su memoria USB? ¿Está seguro de que su director financiero, que está de viaje, se acordará de coger su portátil cuando se baje del avión?

Al combinar el poder de imposición de directivas de Endpoint Security Management con la garantía de Full Disk Encryption, disfrutará de la confianza de saber que los intrusos no pueden acceder a sus datos al mismo tiempo que evita que los empleados que solo desean hacer su trabajo se metan en problemas. Sus datos están seguros.

Practique la productividad segura

Alcance el equilibrio perfecto entre productividad y protección. Con ZENworks Endpoint Security Management y ZENworks Full Disk Encryption podrá:

- Aplicar medidas de seguridad que evalúan dinámicamente el nivel de amenaza basándose en quiénes son los usuarios y dónde están, para a continuación responder de forma adecuada, ajustando directivas (como conexiones WiFi) sobre la marcha.
- Cifrar los datos almacenados en dispositivos portátiles.

- Aplicar estrictas directivas para evitar el uso inadecuado, como controlar qué dispositivos pueden usar los usuarios y cuáles no.
- Dotar a los usuarios de control total sobre los recursos que necesitan para hacer su trabajo, pero impedirles que puedan eludir normas y directivas de seguridad.

Seguridad inquebrantable

ZENworks Endpoint Security Management es el método ideal para imponer las directivas. No se le puede chantajear, las amenazas le traen sin cuidado, y nunca duerme. Recibe sus directivas y se asegura de que se aplican, siempre.

Son las ocho de la mañana de un miércoles. ¿Sabe lo que el empleado del cubículo seis está copiando en su memoria USB? ¿Está seguro de que su director financiero, que está de viaje, se acordará de coger su portátil cuando se baje del avión?

Con ZENworks Endpoint Security Management y ZENworks Full Disk Encryption, ya no hay que preocuparse por ello.

Acerca de Micro Focus

Desde 1976, Micro Focus ha ayudado a más de 20 000 clientes a aprovechar el valor de su lógica empresarial mediante la creación de soluciones de formación que cubren la brecha entre las tecnologías bien establecidas y la funcionalidad moderna. Las dos carteras contribuyen a un único objetivo claro: ofrecer productos innovadores respaldados por un servicio de atención al cliente excepcional. **www.microfocus.com**

“Necesitábamos proteger nuestra red de virus, hackers y demás elementos que amenazan nuestra empresa. Con Novell (ahora parte de Micro Focus) ZENworks Endpoint Security Management, obtenemos lo mejor de ambos mundos: los usuarios que se desplazan cuentan con la libertad que necesitan para disponer de acceso remoto, y nosotros tenemos la tranquilidad de que nuestra red no corre ningún riesgo”.

LAURA DAVIS
Directora de tecnología
Woolpert, Inc.

“El retorno de la inversión de Novell (ahora parte de Micro Focus) ZENworks Endpoint Security Management es asombroso. Si impedimos un solo caso de vulneración de la seguridad informática podemos habernos ahorrado una demanda de 3 millones de dólares”.

ROBB PETTIGREW
Director de Sistemas técnicos y servicio de ayuda técnica
Wyoming Medical Center

Argentina
+54 11 5258 8899

Chile
+56 2 2864 5629

Colombia
+57 1 622 2766

México
+52 55 5284 2700

Panamá
+507 2 039291

España
+34 91 781 5004

Venezuela
+58 212 267 6568

Micro Focus
Sedes corporativas
Reino Unido
+44 (0) 1635 565200

www.novell.com