White Paper

El imperativo empresarial de unos puntos de acceso seguros

Patrocinado por: Apple

Tom Mainelli Michael Suby
Septiembre de 2023

OPINIÓN DE IDC

¿Qué le quita el sueño a los responsables de las decisiones informáticas (ITDM, por sus siglas en inglés)? La seguridad. Eso es porque los ITDM inteligentes saben que no importa lo bien gestionada que esté una empresa o lo conocido que pueda ser su producto o servicio, toda la empresa puede estar en peligro de la noche a la mañana si falla la seguridad.

Por desgracia, el mundo no es cada vez más seguro. El espionaje corporativo, los estados canallas, el crimen organizado e incluso los ladrones corrientes han incrementado su nivel tecnológico. Para mantenerse por delante de los actores con fines maliciosos, el departamento de TI debe permanecer vigilante y siempre preparado para adoptar nuevos proveedores y tecnologías que mantengan a salvo a sus empleados, sus clientes y sus datos.

La lista de desafíos de seguridad a los que se enfrenta el departamento de TI es larga e incluye desde los puntos de acceso o puntos finales (ordenadores) hasta los centros de datos, las redes que lo conectan todo y el software que lo ejecuta todo. En este documento, nos centraremos en la importancia de asegurar estos puntos de acceso. Eso es porque, al final, la seguridad en todos esos otros dominios significa poco si el punto de acceso no es seguro.

Uno de los principales problemas que plantea la seguridad de los puntos de acceso es que la seguridad de estos suele suponer una molestia para la experiencia del usuario, con dispositivos bloqueados y difíciles de usar. Cuando esto ocurre, el otro punto débil de cualquier esquema de seguridad –el usuario– suele encontrar formas de eludir esa seguridad para desarrollar su trabajo. Cuando la seguridad se convierte en una tensión para los usuarios, deja de cumplir su propósito.

Los avances tecnológicos han hecho cada vez más posible conservar una experiencia de usuario de alta calidad al tiempo que se mantiene la seguridad. Los avances en la detección de malware, la protección de datos, la autenticación y la fusión de silicio y software logran que los puntos de acceso actuales no tengan que renunciar a la productividad a cambio de una mayor seguridad.

METODOLOGÍA

IDC llevó a cabo una encuesta en línea a los responsables de la toma de decisiones de TI (ITDM) en Estados Unidos y Canadá (n=513) en julio de 2023, en la que se les preguntaba su opinión sobre la seguridad en general y la importancia de proteger los terminales informáticos en particular. El grupo de encuestados representa una mezcla de empresas con 500 empleados o más de una gama de diferentes industrias. Estos ITDM admiten una combinación de sistemas operativos informáticos,

incluidos Microsoft Windows, Apple macOS y Google ChromeOS. Pueden seleccionar, comprar o implantar software de seguridad para su empresa, o bien dirigir a las personas que lo hacen.

RESUMEN DE LA SITUACIÓN

La seguridad sigue siendo un imperativo para los directivos. Las empresas con visión de futuro reconocen que una buena seguridad no es algo «que está bien tener», sino más bien un requisito para un negocio sano y próspero que opera en un panorama de amenazas en constante evolución, impulsado por malos actores coordinados y bien financiados.

Según la encuesta Future Enterprise Resiliency and Spending Survey (FERS) de IDC de marzo de 2023 sobre ITDM en empresas con un número igual o superior a 500 empleados, más del 50 % de las empresas encuestadas en todo el mundo han sufrido un ataque de *ransomware* que ha interrumpido su actividad en los últimos 12 meses. Más de un tercio de ese grupo afirmó que el ataque interrumpió el negocio durante una semana o más. A pesar de contar con protocolos de seguridad más robustos, las grandes empresas están lejos de ser inmunes a este tipo de ataques. De hecho, el mayor porcentaje de interrupciones por *ransomware* afectó a empresas de la categoría de 1000 a 2499 empleados (71 %), de 2500 a 4999 (72 %) y de 5000 a 9999 (70 %). En otras palabras, independientemente del tamaño, ninguna empresa es inmune a este tipo de ataques.

La misma encuesta señala que los puntos de acceso son el principal punto de entrada de los ataques de *ransomware*. Los puntos iniciales comprometidos incluyen la navegación web (21 %), los medios extraíbles (18 %), los archivos adjuntos a correos electrónicos (17 %), la cadena de suministro (17 %), la URL en un correo electrónico (14 %) y el acceso interno (8 %).

El cambio sostenido en el que más empleados trabajan en situaciones híbridas y remotas solo ha hecho que el *ransomware* y otros riesgos supongan un gran problema para las TI. La encuesta sobre seguridad de puntos de acceso de IDC de diciembre de 2022 mostró que más del 97 % de las organizaciones tienen parte de sus empleados trabajando en remoto. Aunque se espera que ese número se reduzca algo en los próximos doce meses, seguirá siendo muy alto en el futuro previsible.

A medida que las empresas se enfrentan a los retos constantes de una gran plantilla remota, cada vez son más las que aplican estrategias de confianza cero. Las áreas en las que se centran las mejores prácticas incluyen el establecimiento de una línea de base de controles de seguridad, defensas avanzadas de seguridad de puntos de acceso, certificación de dispositivos (garantizar que los dispositivos que se conectan a la red son legítimos) y autenticación robusta de usuarios.

Si tenemos en cuenta todo lo anterior, no es de extrañar que los encuestados hayan seleccionado de forma abrumadora mejorar la seguridad general de los datos y garantizar la seguridad de los ordenadores como sus principales prioridades informáticas, tal y como se refleja en la Figura 1.

Cabe destacar que, en la siguiente figura, el tercer tema más importante era mejorar la productividad de los empleados mediante mejores dispositivos. Cuando pedimos a los encuestados que eligieran sus tres temas principales, la opción de mejores dispositivos fue la más elegida. Esto nos lleva a un mensaje clave que los informáticos deben recordar: La seguridad es importante, pero no puede ir en detrimento de la productividad de los empleados, y los mejores dispositivos ofrecen una combinación de gran seguridad y satisfacción del usuario final que no se ve obstaculizada por esa seguridad.

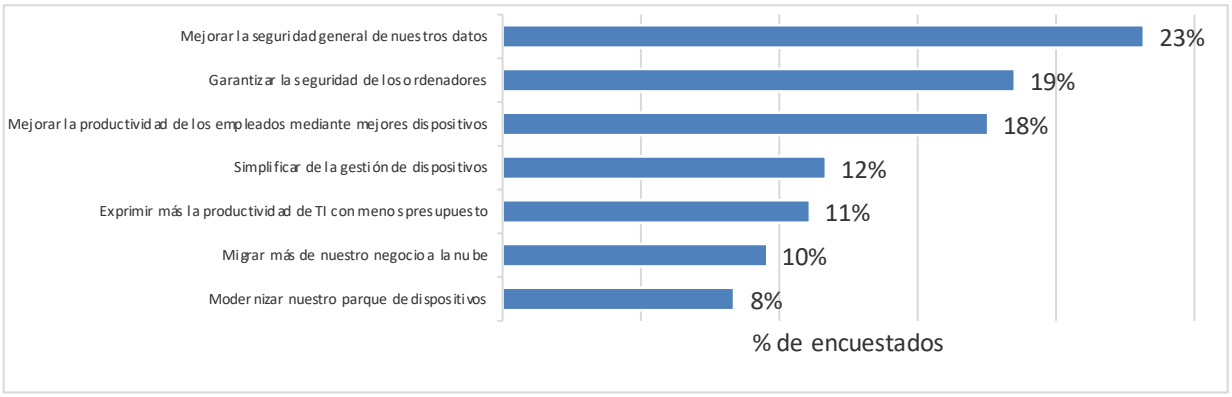
Cuando preguntamos a los ITDM por el factor decisivo al elegir su próximo proveedor informático, la seguridad ocupó el primer lugar, por delante del rendimiento, la compatibilidad con las aplicaciones existentes y la integración con la infraestructura informática existente. Quizá lo más destacable es que la opción de las especificaciones ocupaba el último lugar de la lista.

La Figura 1 muestra las prioridades de TI. Para conocer las principales consideraciones a la hora de elegir un proveedor informático, véase la Figura 2.

FIGURA 1

Las principales prioridades de TI: seguridad de los datos y los puntos de acceso

P. ¿Cuáles de los siguientes aspectos informáticos son prioritarios para su empresa en la actualidad?



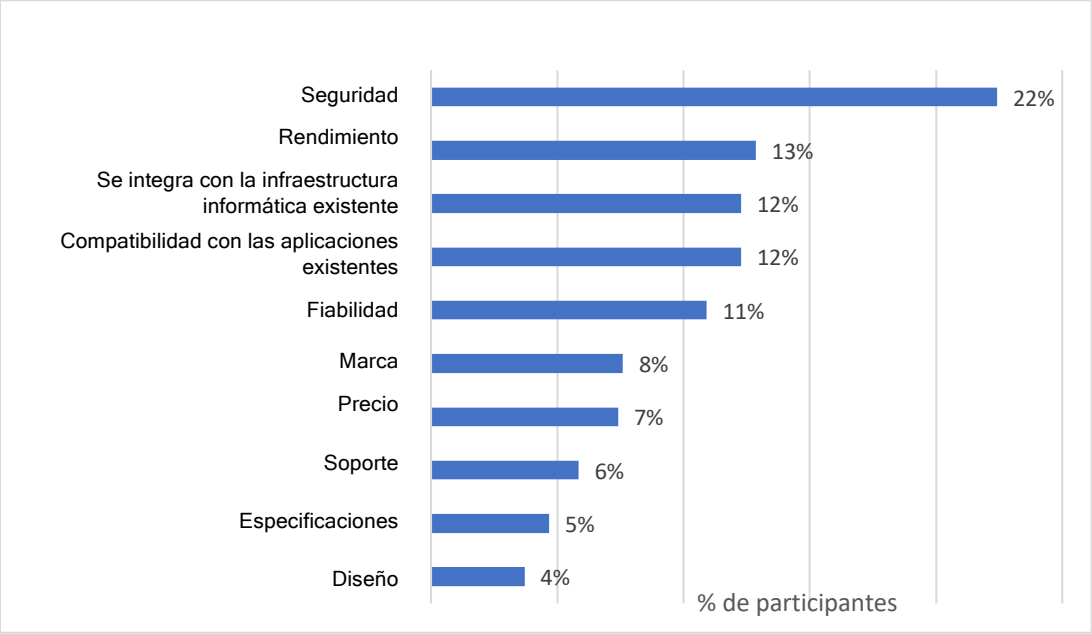
Fuente: Encuesta sobre puntos finales seguros de IDC, n=513

Nota: Los datos incluyen a los más importantes (nº 1)

FIGURA 2

Principales factores a la hora de elegir un proveedor de ordenadores

P. ¿Cuáles son los principales factores decisivos a la hora de elegir un ordenador para su empresa?



Fuente: Encuesta sobre puntos finales seguros de IDC, n=513

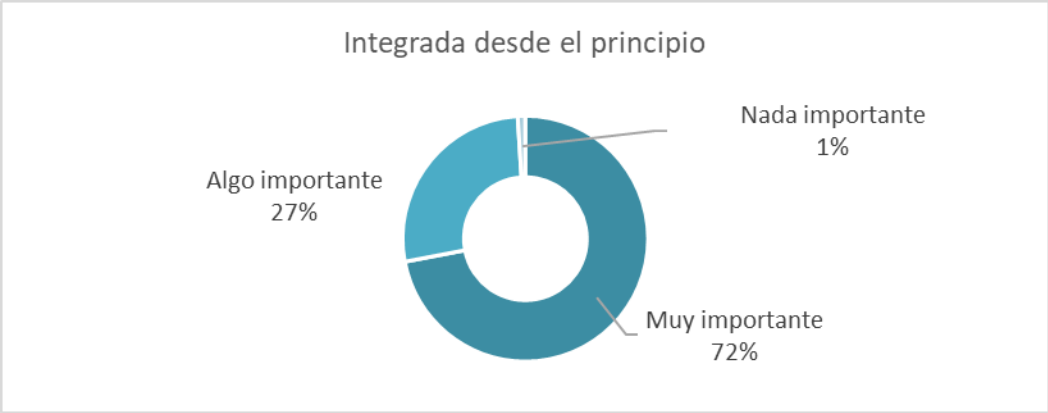
Nota: Los datos incluyen a los más importantes (nº 1)

Dos conceptos que resonaron con fuerza entre los encuestados fueron la seguridad y la protección de datos, ambas integradas. A la pregunta: «¿Qué importancia daría a la seguridad integrada en un ordenador desde el principio –incluidos el silicio, el firmware y el sistema operativo– para protegerlo de las amenazas actuales y futuras? La respuesta fue abrumadoramente positiva: el 72 % afirmó que era muy importante y el 27 % algo importante. Solo el 1 % dijo que no tenía ninguna importancia. Al profundizar en los datos, cabe destacar que entre los ITDM de organizaciones sanitarias y financieras, el porcentaje de quienes dijeron que era muy importante fue incluso mayor (84 % y 75 %). El concepto de protección de datos integrada obtuvo una puntuación igualmente alta. A la pregunta «¿Qué importancia le daría a la capacidad de cifrado de datos integrada en el hardware del ordenador?». El 71 % dijo que era muy importante, el 29 % que era algo importante y el 0 % que no era importante. Si desea más detalles sobre la seguridad integrada y el cifrado de datos integrado, consulte la Figura 3.

FIGURA 3

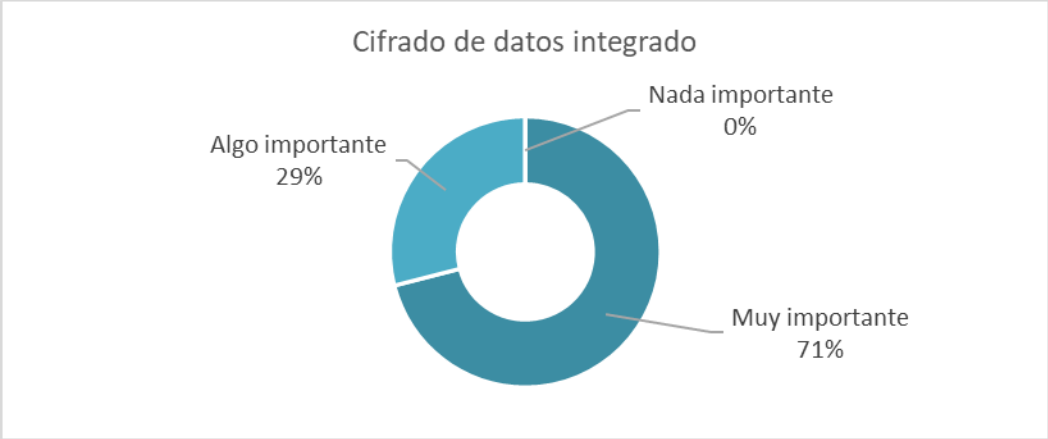
Importancia de la seguridad y el cifrado de datos integrados

P. ¿Qué importancia le daría a la seguridad integrada en un ordenador desde el principio —silicio, firmware y sistema operativo— para protegerlo de las amenazas actuales y anticiparse a las futuras?



Fuente: Encuesta de IDC sobre puntos de acceso seguros, n=513

P ¿Qué importancia le daría a la capacidad de cifrado de datos integrada en el hardware?



Fuente: Encuesta de IDC sobre puntos finales seguros, n=513

Aunque el hardware con seguridad integrada desde el principio es importante, y el cifrado de datos integrado sea un requisito clave, los expertos en seguridad saben que el eslabón más débil de cualquier cadena de seguridad suelen ser los usuarios finales. Por eso es tan importante la autenticación del usuario y por eso los proveedores de tecnología han trabajado con intensidad para que evolucione la autenticación. Desgraciadamente, se trata de un factor en el que nuestra encuesta muestra que muchas organizaciones se están quedando atrás.

Por el lado positivo, nuestra encuesta refleja que el 68 % de los encuestados afirma que su empresa exige contraseñas complejas y el 63 % dice utilizar la autenticación de dos factores. En el lado menos positivo, solo el 23 % utiliza tecnologías de inicio de sesión único (SSO) y solo el 20 % la seguridad

biométrica (como la identificación dactilar o facial). Cabe destacar que entre nuestros encuestados, el 56 % dijo que la autenticación biométrica era mucho más segura que las contraseñas, el 35 % que era un poco más segura, el 9 % que era igual de segura y nadie (0%) dijo que fuera menos segura.

Una nueva e importante tecnología de autenticación introducida recientemente es la *passkey*. Se trata de una credencial digital que aúna un par de claves para ofrecer una solución mucho más segura que una contraseña. Dado que esta tecnología es nueva, solo el 14 % de los encuestados afirma que sus empresas la utilizan, pero los ITDM inteligentes deberían estudiarla de cerca hoy en día. Para saber más sobre el uso de la autenticación de usuarios, consulte la Figura 4.

FIGURA 4

Métodos de autenticación de usuarios

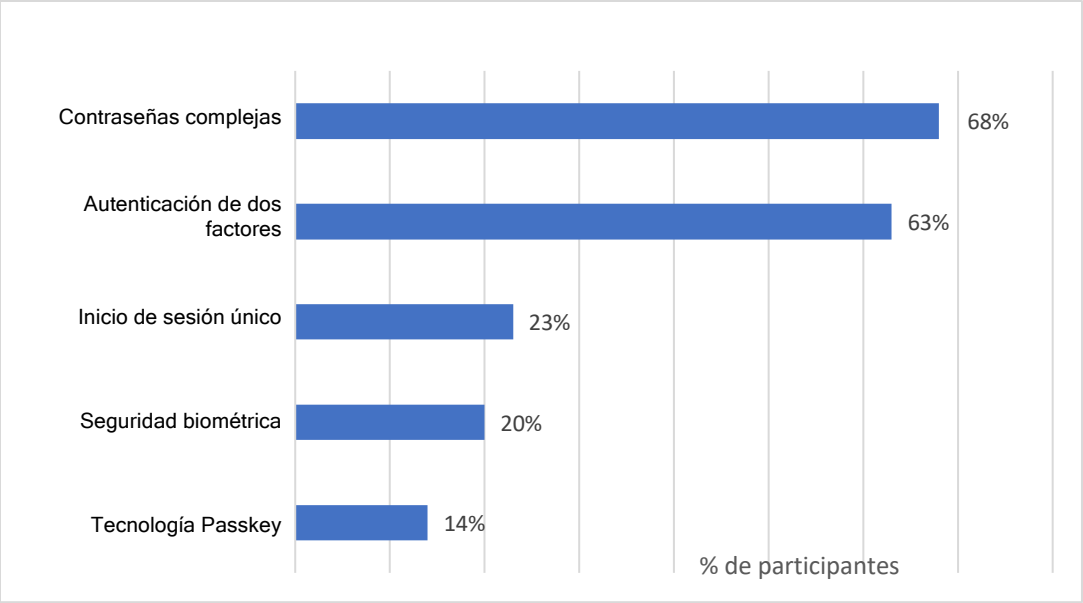
P1. ¿Exige su empresa que los empleados utilicen contraseñas complejas para acceder a su ordenador?

P2.¿Tiene su empresa ordenadores compatibles con medidas biométricas, como el escáner dactilar?

P3. ¿Su empresa ha empezado a estudiar las ventajas de utilizar la tecnología passkey?

P4. ¿Exige su empresa la autenticación de dos factores?

p5. ¿Su empresa utiliza alguna función de inicio de sesión único (SSO)? (S/N)



Fuente: Encuesta sobre puntos finales seguros de IDC, n=513

Los datos indican el porcentaje de respuestas afirmativas

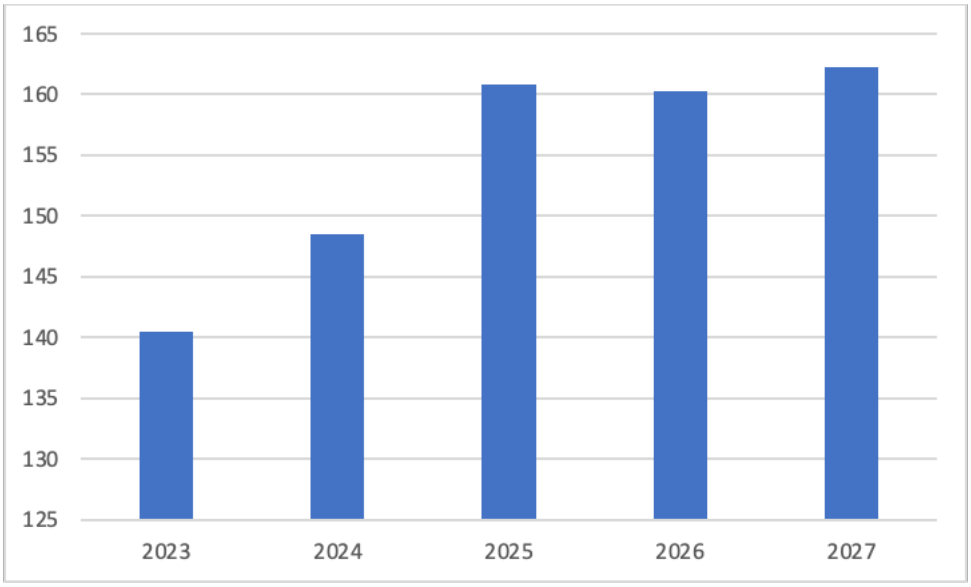
Entre los encuestados, un porcentaje sorprendentemente alto ni siquiera ha implantado protocolos básicos de autenticación de contraseñas complejas (32 %) ni autenticación de dos factores (37 %). **Una buena práctica que merece la pena seguir** es asegurarse de que su empresa ha implantado una forma homogénea de autenticación en toda la organización. Tras definir esa base, empiece a considerar en combinar las capacidades SSO con un buen protocolo de autenticación maestro. Por último, en su próxima renovación del hardware, fíjese en los ordenadores que pueden tener los niveles más altos de autenticación: seguridad biométrica y tecnología de claves de acceso. Al habilitar

ambas, tendrá un futuro en el que los empleados puedan iniciar sesión de forma rápida y segura en sus ordenadores y, desde allí, acceder inmediatamente a sus aplicaciones y sitios web.

En este último punto –la próxima actualización del hardware–cerraremos esta sección. Muchas empresas tienen una base instalada de ordenadores que envejece y necesita ser sustituida. Incluso si su organización compró un porcentaje considerable de nuevos terminales en 2020, esos ordenadores se acercan rápidamente a la marca de los cuatro años. En ese tiempo, la seguridad del hardware ha seguido evolucionando para hacer frente a las amenazas sobre el terreno. Quizás igual de importante es el hecho de que la mayoría de estos productos se enviaron antes del cambio generalizado hacia el trabajo remoto e híbrido, lo que significa que muchos carecen de cámaras, micrófonos y altavoces de alta calidad, necesarios para que los empleados utilicen las aplicaciones de colaboración y conferencias web que ahora son clave. Tras varios años de ralentización de los envíos, el rastreador de dispositivos informáticos personales de IDC prevé un crecimiento de la categoría en los próximos años. Nota: las unidades comerciales son unidades adquiridas por entidades no consumidoras. Para conocer las previsiones de IDC sobre ordenadores de consumo/comerciales, véase la Figura 5.

FIGURA 5

Previsión mundial de ordenadores comerciales



Fuente: IDC PCD Tracker, agosto de 2023

Las empresas deben reevaluar continuamente las necesidades informáticas de sus empleados para seguir siendo competitivas en el mercado y atraer y retener a los mejores talentos. Mientras que antes el departamento de TI tenía que hacer grandes concesiones entre la seguridad y la satisfacción de los empleados, hoy en día, el proveedor adecuado puede ayudar a impulsar una solución sin concesiones. Por último, **otra buena práctica que debe tenerse en cuenta** es la aplicación de los principios de acceso de confianza cero para su próxima implantación de hardware. Esta estrategia supone que siempre que un dispositivo intente acceder a un recurso de la empresa, no se debe confiar en él hasta que se verifique. La confianza cero aplica tecnologías y procesos para certificar la

seguridad del dispositivo (de forma óptima desde el silicio hasta las aplicaciones esenciales de TI y seguridad), la red de conexión (Wi-Fi pública frente a red privada) y la identidad del usuario.

Mac en la empresa

Cada vez son más los departamentos de TI que dan soporte a los Mac, y nuestra encuesta apunta a una razón clave. Entre los encuestados que representan una mezcla de sistemas operativos en su base instalada, el 76 % afirma que cree que los Mac son más seguros que otros ordenadores, y en los próximos 12 meses, la razón número uno para adoptar más Mac fue porque creen que son más seguros (47 %), seguida de cerca por la facilidad de despliegue y gestión (36 %).

Testimonio de un cliente de Apple

«Una de las características más importantes de los productos Apple es que la privacidad y la seguridad están integradas en el propio producto. No son una ocurrencia tardía, y eso es algo que apreciamos mucho» —Linda Jojo, Vicepresidente ejecutivo y directora de atención al cliente de United Airlines

Apple se centra en ofrecer una gran experiencia de usuario al tiempo que eleva la seguridad mediante la integración de la seguridad en el silicio de Apple a través del software. Un ejemplo de ello es Touch ID de Apple, una función de seguridad biométrica integrada. El hardware de Apple incorpora Secure Enclave, que cifra y protege el código de acceso utilizado para salvaguardar los datos de Touch ID.

Para hacer frente al riesgo de que el sistema operativo y las secuencias de arranque se vean comprometidos, los Mac están equipados con Secure Boot y Signed System Volume. Secure Boot garantiza que solo se inicie la versión de macOS certificada criptográficamente, y Signed System Volume protege la integridad del sistema operativo durante el tiempo de ejecución. El software desactualizado también supone un riesgo cibernético que Apple minimiza automatizando y asegurando la distribución e instalación de extremo a extremo de las actualizaciones de software.

Un buen software de terceros es esencial para la productividad de los empleados, pero también debe estar exento de malware. Apple tiene un enfoque multicapa para prevenir el malware. El Mac App Store de Apple analiza todas las aplicaciones en busca de malware. Dado que el software de los Mac también puede descargarse de Internet, Apple exige a los desarrolladores que envíen sus aplicaciones al servicio notarial de Apple, que también las analiza en busca de malware. El Gatekeeper de Apple, incluido en macOS, comprueba la notarización e impide que se ejecuten aplicaciones no firmadas. Además, XProtect –la herramienta antimalware de Apple– bloquea y elimina cualquier software malicioso conocido.

Los datos son uno de los activos más valiosos de una organización y deben protegerse en consecuencia. La combinación del cifrado FileVault reforzado con silicio, los protocolos VPN compatibles con Apple y el cifrado de extremo a extremo en los servicios de Apple (por ejemplo, iMessage e iCloud) garantiza la protección de los datos en reposo, en tránsito y en uso.

Dado que la ingeniería social es una de las habilidades más perfeccionadas de los actores de amenazas, los usuarios finales deben ser defensores vigilantes. Una responsabilidad difícil, pero a la que Apple ayuda con la advertencia de sitios web fraudulentos de Safari. Además, dado que las credenciales de autenticación suelen ser lo que roban los ciberdelincuentes, la compatibilidad con contraseñas de Apple facilita a las organizaciones la modernización de sus métodos de autenticación, de nuevo sin sacrificar una experiencia positiva para el usuario final.

Una buena seguridad se alinea con una sólida gestión de los dispositivos. Para ello, Apple ofrece una serie de capacidades de gestión de dispositivos, incluido un marco de gestión integrado con Mobile Device Management (MDM). Apple Business Manager permite el despliegue sin intervención y enlaza con soluciones MDM, mientras que las API de seguridad de puntos finales para Mac permiten a los desarrolladores crear soluciones para supervisar, analizar y responder a las amenazas de seguridad. Apple también ofrece integraciones de identidad con un marco SSO integrado que funciona con proveedores de identidad modernos (IdP).

Por último, Apple proporciona estas funciones de seguridad, incluidas las actualizaciones de software mayores y menores, con macOS sin coste adicional para los clientes empresariales o particulares.

DESAFÍOS Y OPORTUNIDADES

A pesar de un entorno de amenazas en constante evolución, el departamento de TI se enfrenta al reto de hacer más con menos: menos dinero, menos personal de TI y menos recursos. Además de hacer frente a los continuos riesgos de seguridad a los que se enfrentan todas las empresas, muchas organizaciones de TI también tienen la tarea de mejorar de forma cuantificable la productividad y la satisfacción de los empleados a través del hardware, el software y los servicios que despliegan. Tener éxito en ambas tareas —mejorar la seguridad y la productividad y satisfacción de los empleados— puede parecer insuperable. Pero también representa una oportunidad clave para TI. Una oportunidad para reevaluar el hardware, el software y los servicios que adquiere, los proveedores a los que compra y las formas en que los despliega para una plantilla cada vez más híbrida. Además, es evidente que ha llegado el momento de recalcular los modelos de coste total de propiedad (TCO) para reflejar mejor cómo compran y utilizan las empresas la tecnología hoy en día.

CONCLUSIÓN

La seguridad es, y seguirá siendo, una de las principales preocupaciones de TI. En un momento en el que los presupuestos de TI son ajustados y está pendiente una renovación significativa del hardware, tiene sentido reevaluar con qué proveedores gastará su dinero en el futuro. Considere la posibilidad de implantar las mejores prácticas en torno a la autenticación y las implantaciones sin intervención, y compre hardware que haga posibles estos cambios. No priorice la seguridad sobre la productividad y la satisfacción de los empleados cuando hay proveedores que ofrecen ordenadores con seguridad integrada y cifrado de datos con los que puede contar para proporcionar tanto seguridad como una experiencia positiva al usuario final.

Acerca de IDC

International Data Corporation (IDC) es el principal proveedor mundial de inteligencia de mercado, servicios de asesoramiento y eventos para los mercados de tecnologías de la información, telecomunicaciones y tecnología de consumo. IDC ayuda a los profesionales de TI, a los ejecutivos de empresas y a la comunidad inversora a tomar decisiones basadas en hechos sobre compras de tecnología y estrategia empresarial. Más de 1.100 analistas de IDC proporcionan conocimientos globales, regionales y locales sobre las oportunidades y tendencias tecnológicas e industriales en más de 110 países de todo el mundo. Durante 50 años, IDC ha proporcionado perspectivas estratégicas para ayudar a nuestros clientes a alcanzar sus objetivos empresariales clave. IDC es una filial de IDG, la empresa líder mundial en medios tecnológicos, investigación y eventos.

Sede mundial

Calle Kendrick 140
Edificio B
Needham, MA 02494
EE.UU.
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com