jamf

DOCUMENTO TÉCNICO

Diferencias en seguridad entre macOS y Windows

A medida que el Mac va ganando terreno en pequeñas y grandes empresas de todo el mundo, el uso de viejas herramientas de gestión para proteger dispositivos modernos está condenado a convertirse en una práctica del pasado.

Teniendo en cuenta que Microsoft dejará de prestar soporte a Windows 7 el 14 de enero de 2020, todavía serán más los usuarios y administradores de Windows que desembarcarán en un mundo totalmente nuevo para ellos: el mundo del Mac.

La seguridad es probablemente el aspecto más importante de cualquier tecnología, por lo que este documento técnico presenta las claves del modelo de seguridad de macOS y sus diferencias respecto a Windows.

LAS CLAVES DE LA ESTRUCTURA DE MACOS

Apple ha diseñado macOS partiendo de un modelo integrado de hardware, software y servicios, con la seguridad integrada en el diseño y con el objetivo de ofrecer a los equipos de IT un sistema fácil de configurar, implementar y gestionar. Al igual que los empleados esperan poder trabajar de una forma fiable y estable con sus ordenadores, los profesionales de IT buscan una experiencia similar al gestionar la plataforma para los empleados.

Apple cuenta con programas específicos para empresas diseñados para agilizar la implantación y la seguridad, asi como poner en manos de los usuarios todo lo que necesitan sin intervención alguna por su parte. La combinación de Apple Business Manager con la gestión de dispositivos móviles (MDM) se traduce en un sistema de gestión unificado y protegido en todo el ecosistema Apple.

Algunas organizaciones buscan una única herramienta para dar respuesta a las necesidades de todos los equipos macOS y Windows. El problema es que esta apuesta provoca la aparición de lagunas en la gestión, la experiencia del usuario y la seguridad. Cuando se emplea una única herramienta para gestionar varias plataformas, las funciones de seguridad no se utilizan correctamente, ya que no es así como Apple o Microsoft habían previsto proteger los dispositivos.

¿Qué es Apple Business Manager?

Apple Business Manager proporciona a los administradores de IT un único portal agrupado para la implantación automática de dispositivos Mac, iPad, iPhone y Apple TV directamente a los usuarios y configurados con sus ajustes, controles de seguridad, apps y libros.

El entorno de macOS

Para familiarizarse con el modelo de seguridad de Apple, primero es necesario entender los conceptos básicos del entorno de Apple.

DIFERENCIAS EN LA GESTIÓN ENTRE MACOS Y WINDOWS

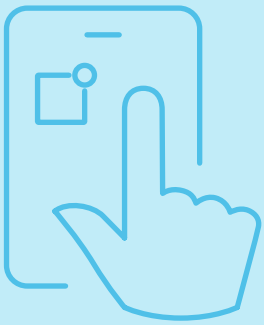
¿En qué se diferencia el modelo de Apple de la gestión tradicional de Microsoft a través de terminales PC con Windows? El secreto de la facilidad de uso de macOS está en su entorno de gestión integrado, conocido como gestión de dispositivos móviles (MDM). Con la plataforma MDM, el departamento de IT puede crear perfiles de configuración que gestionan varios ajustes del sistema operativo. Estos perfiles se distribuyen de forma inalámbrica a través del servicio de notificaciones push de Apple (APN). Las APN mantienen una conexión constante con los ordenadores Mac (y otros dispositivos Apple) para que el equipo de IT no tenga que hacerlo. La plataforma MDM abre la puerta a funciones de gestión que un administrador de Windows tradicional antes solo conseguía a través de una vinculación o de un objeto de política de grupo (GPO).

LAS APN REFUERZAN LA APUESTA POR LA SEGURIDAD DE UNA ORGANIZACIÓN

Las APN ofrecen una solución segura y altamente eficaz para distribuir información a dispositivos macOS, iOS, tvOS y watchOS. Las APN son una pieza básica de los programas de implantación de Apple y de otras funciones de seguridad, como el bloqueo remoto y el borrado remoto. En realidad, ni Apple Business Manager ni MDM funcionarán si no se utilizan las APN, ya que estos programas no pueden desplegarse a través de una conexión proxy, sino que el acceso debe producirse a través de un canal directo con Apple, como las APN.

Otras ventajas de las APN:

- Un modelo de seguridad reforzado para la gestión de ordenadores Mac propiedad de la empresa. Las APN permiten bloquear/borrar de forma remota e inalámbrica un dispositivo perdido, robado o en situación de riesgo.
- La MDM depende de las APN para el envío de comandos clave, como las instalaciones de software o las actualizaciones de inventario.
- Aunque las cargas útiles de los perfiles de configuración MDM pueden transmitirse a macOS sin conexión, este método es mucho más laborioso que una gestión inalámbrica.
- Las APN ordenan a cada dispositivo que se conecte automáticamente al servidor MDM.



Funciones de seguridad específicas del Mac

La base de macOS es un software integrado y seguro. macOS ofrece, entre otras, las siguientes funciones de seguridad integradas:

FileVault es una capa de cifrado integrada en macOS para proteger los datos del usuario en caso de pérdida o robo de un dispositivo.

La **Herramienta de eliminación del código dañino** permite a Apple eliminar el malware que consigue colarse en el sistema.

Las **actualizaciones de software** llegan directamente de Apple y llevan su firma digital, por lo que las organizaciones y el departamento de IT pueden confiar en su origen.

Las **apps del App Store** disponibles en el App Store están verificadas por Apple y los únicos recursos disponibles son los aprobados por Apple. Apple tiene la potestad de eliminar una app del catálogo y de revocar al instante los certificados del desarrollador.

La **Protección de la Integridad del Sistema (SIP)** protege archivos clave del sistema operativo que podrían ser el objetivo de accesos malintencionados de usuarios o aplicaciones.

La **zona protegida (sandboxing) de apps** garantiza que las apps no comparten (ni roban) datos del sistema o de otras apps.

XProtect es una utilidad antimalware automática, que Apple se encarga de mantener actualizada. Evita la ejecución en un Mac de software malicioso o plugins desfasados y a menudo vulnerables, como por ejemplo de Java y Flash.

Los **controles de privacidad** son otro recurso a disposición de los usuarios y del equipo de IT, un proceso transparente que permite a los usuarios saber cuándo se usan los servicios de localización, qué apps tienen acceso a contactos o calendarios y qué información se comparte con Apple y/o los desarrolladores de apps.

Gatekeeper permite al equipo de IT definir desde dónde pueden los usuarios descargar sus aplicaciones. El sistema evita la ejecución de apps (o malware) sin firmar y funciona coordinado con XProtect para frenar de inmediato la propagación del malware.

Para ver una lista completa de las funciones de seguridad del Mac, puede visitar la siguiente dirección: **https://www.apple.com/es/macos/security/**

VENTAJAS DE FILEVAULT PARA EL CIFRADO DEL DISCO

FileVault es un sistema de cifrado del disco integrado para macOS, gracias al cual el equipo de IT no tiene que añadir ningún software adicional para cifrar una unidad. El cifrado puede activarse manualmente o bien de forma remota en todos los ordenadores Mac. Las claves de cifrado pueden gestionarse de forma centralizada para que el equipo de IT pueda acceder a los datos necesarios cuando un empleado abandona la organización o si ha perdido la contraseña y necesita ayuda para conectarse. Además, la rotación de las claves de cifrado es muy sencilla, lo que refuerza la seguridad.

CHIP T2 DE APPLE PARA REFORZAR LA SEGURIDAD

Los nuevos ordenadores Mac como el MacBook Air y algunos modelos de MacBook Pro incluyen un chip T2 Security de Apple personalizado, con un Secure Enclave que abre la puerta a nuevas funciones de seguridad y protege la información de huellas dactilares de Touch ID.

El chip T2 Security de Apple también incorpora un controlador de unidad de estado sólido (SSD) con cifrado de datos automático e instantáneo, ofreciendo almacenaje más seguro que cualquier ordenador. Además, garantiza que no se ha manipulado el software cargado, asegurando un proceso de arranque más seguro que con cualquier otro ordenador.

REDUCCIÓN DE LA DEPENDENCIA DE SOFTWARE DE SEGURIDAD DE TERCEROS

A diferencia de Windows, en el Mac es poco habitual emplear una capa adicional de seguridad o herramientas de terceros.

Las empresas de seguridad tradicionales especializadas en Windows no suelen seguir el ritmo de los ciclos de desarrollo del Mac, lo que puede ralentizar la adopción de los nuevos sistemas operativos y funciones de seguridad. De hecho, tratar un Mac como si fuera un ordenador Windows a menudo impide a los empleados rendir al máximo y pone trabas a la experiencia de usuario que tanta fama ha dado a Apple. Además, la adopción de una versión de software para Windows en un Mac es garantía de una mala ejecución del código, lastres en la memoria y problemas derivados de la extensión del núcleo (KEXT). El resultado son interminables quebraderos de cabeza para el equipo de IT.

El cifrado y el antivirus integrados en el Mac permiten a muchas organizaciones prescindir de terceros, aunque algunas siguen buscando soluciones para controlar las filtraciones de datos de la empresa. Sin embargo, este tipo de filtraciones puede controlarse a través de MDM, con protecciones adicionales en la red a través de herramientas como Cisco Security Connector.

Las organizaciones que traten sus ordenadores Mac como si fueran PC con Windows corren el riesgo de gastar dinero innecesariamente en software de protección antimalware. Y además de este coste extra, estas aplicaciones complementarias pueden poner en peligro el rendimiento y la estabilidad del Mac.

Protección antimalware

Mac
(funciones de seguridad integradas)

- Firewall de red
- Gatekeeper
- XProtect
- Protección de la Integridad del Sistema

PC
(complementos de terceros)

- McAfee
- KasperSky
- Symantec
- BitDefender

LOS SERVICIOS EN LA NUBE Y EL MAC

Los servicios en la nube son una tendencia en auge. El hosting en la nube limita el acceso a la base de datos, que ya no está alojada en un servidor de su red. Durante décadas, las organizaciones se han dedicado a construir muros alrededor de su empresa y han utilizado los perímetros de la red como primera línea de defensa.

En la actualidad, con los nuevos patrones de movilidad en el entorno laboral y unos datos que ya no se encuentran confinados a los límites del firewall, las organizaciones deben adoptar un modelo de seguridad más moderno y basado en la identidad. Microsoft, por ejemplo, está trasladando los datos de empresa a la nube con Microsoft Azure Active Directory.

Para garantizar que solo los usuarios autorizados, usando dispositivos autorizados y apps autorizadas, acceden a estos datos de la empresa en la nube, Microsoft y Jamf ofrecen una integración exclusiva, que abre la puerta a un acceso condicional sin necesidad de proxy.

Puede encontrar más información aquí: **https://www.jamf.com/resources/white-papers/conditional-access-going-beyond-perimeter-based-security/**

ADIÓS A LA VINCULACIÓN A ACTIVE DIRECTORY

La vinculación de PC con Windows a Active Directory (AD) es una práctica habitual en los procesos de implantación. Sin embargo, cuando las organizaciones tratan de vincular los Mac a la red, se produce un problema de sincronización de contraseñas y los procesos de Apple Business Manager se ven afectados si los controladores de dominio no están expuestos al exterior. La vinculación también impide enviar nuevos ordenadores Mac ya preparados a empleados que trabajan en remoto.

Si bien la vinculación es posible (a pesar de no estar recomendada), las organizaciones que utilizan soluciones de gestión de Apple específicas, como Jamf Pro y Jamf Connect, pueden gestionar cuentas locales para aplicar los mismos requisitos de complejidad y caducidad de las contraseñas sin preocuparse por las conexiones ni perder la sincronización con AD. El resultado son menos mensajes pidiendo la contraseña a los usuarios finales y menos llamadas al servicio de asistencia de IT.

Para garantizar la máxima seguridad sin necesidad de vinculación, Jamf Connect incorpora la gestión de identidades. Gracias a integraciones con los principales proveedores de identidad en la nube (como Okta, Microsoft Azure Active Directory, Google Cloud Identity, IBM, OneLogin o Ping Identity), Jamf Connect permite un aprovisionamiento de usuarios sencillo desde un servicio de identidad en la nube durante un proceso de aprovisionamiento de Apple, complementado con autenticación multifactor.

Jamf Connect ofrece la flexibilidad de utilizar los mismos usuarios locales, controlados por las mismas políticas y controles de un servicio de directorio o un proveedor de identidad. Además, un usuario puede sacar su Mac de la caja, ponerlo en marcha y acceder de forma segura a cualquier aplicación aprobada en el sistema tras iniciar sesión con unas únicas credenciales de identidad en la nube.

CUMPLIMIENTO DE LOS ESTÁNDARES DE SEGURIDAD DEL SECTOR

Como bien saben los equipos de seguridad informática, el nivel de cumplimiento depende de cuáles sean los estándares de seguridad vigentes. SOC 2 es diferente de HIPAA y PCI es diferente de CIS. Saber a qué debemos atenernos es un primer paso muy importante.

Jamf Pro proporciona una infraestructura flexible que facilita el cumplimiento de los estándares más habituales. El equipo de IT simplemente tiene que definir los estándares aplicables, crear los perfiles y las políticas correspondientes, para finalmente aplicarlos. Estas normas pueden incluir la restricción de funciones como iCloud Drive, la aplicación de Gatekeeper para garantizar la descarga únicamente de apps seguras, la utilización de FileVault para cifrar el Mac o la restricción de apps buscando una app restringida (o incluso un macOS) en toda la flota de dispositivos Apple gestionados para, una vez localizada, eliminarla.

El equipo de IT solo tiene que definir los ajustes y usar esta información para diseñar perfiles y políticas de configuración y aplicarlos a los dispositivos.

Consulte este documento técnico para saber cómo cumplir con las pautas del Center for Internet Security (CIS): **https://www.jamf.com/resources/white-papers/macos-security-checklist/**

UN NIVEL DE SEGURIDAD SIN RIVAL PARA HARDWARE, SOFTWARE, USUARIOS Y REDES

La plataforma más segura requiere la solución de gestión más fiable para que todas las funciones de seguridad se instalen y utilicen correctamente. Ninguna otra empresa de gestión de dispositivos móviles garantiza una mejor integración con Apple y sus servicios que Jamf. Y ningún otro proveedor está mejor preparado para ayudarle a llegar tan lejos con sus Mac.

Si está valorando la opción de ofrecer a sus empleados un programa de elección de Mac o quiere implementar ordenadores Mac en toda su empresa, podemos echarle una mano.

Póngase en contacto con nosotros para empezar a recorrer este camino o realice una prueba gratuita de Jamf y experimente de primera mano con nuestras funciones de seguridad para Mac.

Contactar ahora **Solicitar prueba**

O póngase en contacto con su distribuidor autorizado de dispositivos Apple para realizar una prueba con Jamf.

jamf

www.jamf.com

30 de septiembre de 2019 a las 10.27