jamf

DOCUMENTO TÉCNICO

Superando las brechas de seguridad en macOS

Privacidad y seguridad nativas, pero ningún sistema operativo es perfecto.

La necesidad de seguridad es común a todos los sistemas operativos, y macOS no es una excepción. Apple ha realizado una gran inversión para proporcionar características de seguridad y privacidad nativas, pero a medida que aumenta la presencia de Mac en el mundo empresarial también lo hacen las oportunidades para el malware, las vulnerabilidades y las infracciones de seguridad. Ahora más que nunca las empresas permiten a sus empleados utilizar macOS a través de programas de elección personal. Es por eso que, como sucedería con cualquier otra plataforma, se necesitan seguridad y visibilidad adicionales.

Varios proveedores de seguridad ofrecen soluciones de protección para Mac adicionales, pero muchas parten de modelos de seguridad específicos para ese proveedor y sus productos para Windows, y no están concebidos para los entornos más modernos ofrecidos por macOS. Así, es más difícil estar al día de todas las novedades de un sistema operativo en constante evolución. En vez, las prácticas recomendadas consisten en ampliar el modelo de seguridad macOS existente, superar las brechas y sumar el valor específico de macOS que los equipos de seguridad necesitan para operar de manera eficiente y mantener su organización a salvo de amenazas.

Y si bien los sistemas operativos de Apple garantizan la protección y seguridad del usuario, la facilidad de uso y la productividad siempre han sido aspectos prioritarios. La experiencia Apple está centrada en el usuario y no en su sector empresarial. Y lo mismo podría decirse de muchas de las funciones de seguridad y privacidad de macOS.

En este documento técnico, presentamos una visión general del estado actual de la seguridad macOS y ofrecemos orientación acerca de cómo puede mejorarse el nivel básico de seguridad Apple de manera eficiente, intuitiva y efectiva.

Descubrirá:

- Detalles acerca de las funciones de seguridad Mac integradas disponibles
- Cómo Jamf consigue mejorar estas funciones en la empresa
- Cómo consigue Jamf detectar amenazas más allá de las funciones y especificaciones integradas
- Fórmulas adicionales para ampliar el modelo de seguridad Apple para mejorar la seguridad en la empresa

Confianza en las aplicaciones con macOS

Apple ha realizado un gran esfuerzo para diseñar funciones de seguridad y generar confianza entre el usuario y las aplicaciones de terceros que utiliza. En esta sección presentaremos algunas de estas funciones y hablaremos acerca de las maneras en que pueden mejorarse y ampliarse de forma estratégica. Para obtener más información acerca de las funciones de seguridad Apple, visite la guía completa de seguridad de Apple en **https://support.apple.com/es-es/guide/security/welcome/web** aquí.

Fiabilidad con Gatekeeper

La forma más segura, y la preferida por Apple, de instalar aplicaciones de terceros es desde la App Store. Hacerlo de esta manera permite que Apple revise y filtre los programas que no cumplen con sus estándares de privacidad, seguridad o experiencia de usuario. Sin embargo, Apple también limita las capacidades de las aplicaciones en la App Store, y muchas apps esenciales para la empresa no se ajustan bien a este tipo de distribución.

Cuando la distribución desde la App Store no es viable, Apple permite a los desarrolladores para macOS distribuir sus aplicaciones directamente mediante descargas directas y otros métodos de distribución tradicionales. Para apoyar estas distribuciones ad hoc, Apple ha introducido otros filtros en el sistema operativo que reducen el riesgo de distribución generalizada de software no fiable en dispositivos macOS. Gatekeeper es el nombre de la función central de estos controles de fiabilidad y autenticación de Apple. Lo que comenzó siendo una opción de macOS que permitiera a los programas ejecutarse según su nivel de confianza, ha evolucionado para convertirse en un conjunto extendido y estricto de requisitos y medidas de mitigación. Los niveles de confianza básicos, que permiten que las aplicaciones sean descargadas desde la App Store o desde “los desarrolladores identificados por la App Store” siguen estando disponibles, pero la opción de ejecutar código no fiable no es común.

Tenga en cuenta que estos controles solo afectan a las aplicaciones descargadas desde Internet. Apple rastrea estas aplicaciones mediante la inclusión de metadatos adicionales a los archivos descargados, conocidos como atributos de cuarentena. Cuando se ejecuta un programa, Gatekeeper comprueba los atributos de cuarentena para determinar si la aplicación va a superar una serie de comprobaciones antes de poder ejecutarse. Uno de estos controles fundamentales verifica si la aplicación viene firmada por un desarrollador legítimo o si ha sido distribuida por la App Store, dependiendo de la configuración antes mencionada.

Si la aplicación ha sido firmada por un desarrollador, el certificado se contrasta con la base de datos de firmas denegadas, para garantizar que el firmante no se ha visto asociado con malware en el pasado. De esta manera, Apple puede retirar rápidamente un certificado y detener la distribución generalizada de malware.

Desde la versión Catalina de macOS, superar la verificación de Gatekeeper también exige que las aplicaciones vengan certificadas por Apple. Para que una aplicación supere el control, ha de subirse primero a Apple para su análisis. Una vez superado el análisis con éxito, los datos de verificación se asocian a la aplicación para señalar que ha superado este nivel de inspección adicional.

La confianza definitiva depende del usuario

En nombre de la usabilidad, macOS permite que el usuario final pueda hacer caso omiso de Gatekeeper. Un usuario puede, sencillamente, hacer clic derecho en la aplicación y seleccionar “abrir” o “abrir con”. En lugar de negarse a ejecutar la app, una nueva alerta avisará al usuario de que está a punto de ejecutar una aplicación no fiable, pero Gatekeeper le permitirá hacerlo.

Una vez ejecutada la app por primera vez, el atributo de cuarentena se actualiza de manera que las acciones de Gatekeeper no se repitan la siguiente vez que se abra la aplicación.

Bloquear amenazas con XProtect y MRT

El conjunto de tecnologías Gatekeeper incluye también los mecanismos de detección Apple basados en la firma conocidos como XProtect y la herramienta de eliminación de malware (MRT). Juntos, son capaces de escanear archivos del sistema operativo, buscando atributos en su interior que hayan sido asociados a cualquier malware conocido. XProtect se activa desde el lanzamiento de las aplicaciones, mientras que MRT escanea el sistema de archivos de forma periódica.

XProtect opera con un motor de escaneado de firmas binarias llamado Yara. Yara dispone de definiciones de firma binaria flexibles y potentes, y de un motor de ejecución eficiente. Con el fin de verificar la fiabilidad de una aplicación, XProtect escanea cada descarga ejecutable únicamente en su primera ejecución. Si se detectan firmas concordantes el programa no obtendrá permiso para ejecutarse. Los archivos de firmas denegadas reconocidas se obtienen mediante actualizaciones independientes a macOS desde Apple. Apple define y hace entrega de estas firmas cuando lo considera oportuno, al margen del propio motor de ejecución de Yara. Tal y como pasa con Gatekeeper, esta comprobación solo se realiza cuando una app contiene el atributo de cuarentena ampliado correcto, que se actualiza una vez ha tenido lugar la primera ejecución exitosa de la aplicación.

Por otro lado, MRT se ejecuta de forma programada y no al arrancar el programa; escanea el sistema de archivos en busca de nombres de archivo específicos y de artefactos que el malware haya podido dejar a su paso, y los elimina una vez descubiertos. Esta característica tiene por objeto localizar y remediar amenazas conocidas que puedan estar ya ejecutándose en el entorno macOS.

Ampliar el rango de Gatekeeper a la empresa

Gatekeeper opera de manera eficiente tal y como se pretende. Impide que las aplicaciones no fiables puedan arrancar y notifica al usuario cuando identifica una aplicación como sospechosa o maliciosa. Los profesionales de IT y de seguridad informática necesitan tener constancia de cualquier intento de lanzar software no fiable en un activo corporativo. Más importante aún, necesitan tener conocimiento de cualquier usuario que haya decidido hacer clic derecho para ejecutar una app y sortear así el control de seguridad de la empresa. Con el fin de atender a estas necesidades empresariales, Jamf Protect —una solución de seguridad para endpoints diseñada específicamente para Mac— detecta indicios de acción por parte de Gatekeeper e informa de los resultados a una ubicación centralizada desde la que los equipos de IT y seguridad podrán evaluar de manera precisa los riesgos y tomar decisiones informadas.

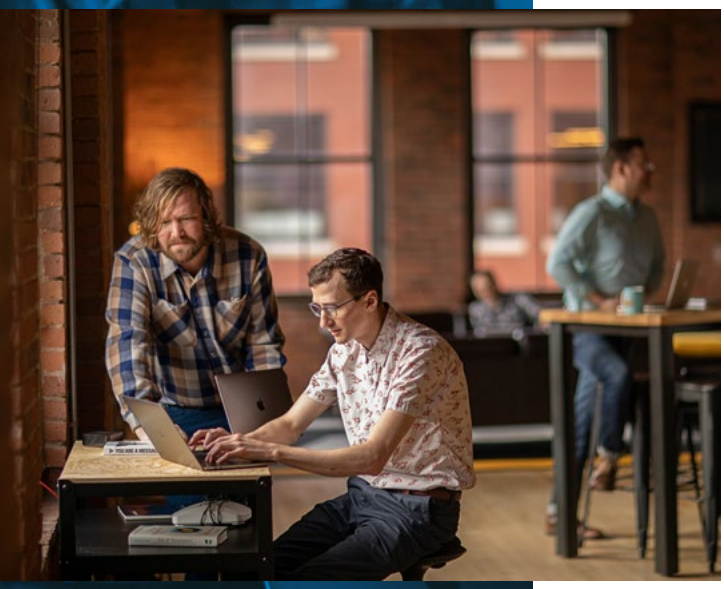
Más allá de ofrecer visibilidad a la actividad de Gatekeeper, Jamf Protect también permite a las empresas hacerse con el modelo de confianza de los desarrolladores identificando cualquier información de acceso adicional como no fiable en el entorno empresarial. Basándose en el más reciente entorno de seguridad para endpoints de Apple, Jamf Protect denegará de forma proactiva la ejecución de cualquier app en la lista de bloqueo específica de la empresa. Esto puede especificarse a nivel de aplicación (ID de aplicación) o a nivel de proveedor (ID de equipo de desarrollo).

Además, macOS tampoco proporciona firmas ni bloqueos para toda una variedad de Grayware (software potencialmente no deseado o no autorizado) que incluye muchas apps de adware y de minería criptográfica que pueden llegar a participar en comportamientos no deseados y potencialmente invasivos. A menudo estos programas cuentan con firmas

legítimas de desarrolladores Apple, y el usuario acepta ceder su información o que se utilicen sus recursos, muchas veces sin darse cuenta. Es por ello que Apple, en muchos casos, no interfiere con el funcionamiento de estas apps.

Sin embargo, la estimación de riesgos es sencillamente distinta en el entorno empresarial y puede que lo deseable sea un enfoque más estricto y específico. De esta manera, Jamf Protect aplica su propio conjunto de reglas Yara, firmas binarias y certificados de desarrolladores no fiables, y los utiliza para escanear procesos en el momento de su ejecución, independientemente de si detecta atributos de cuarentena o no. Esto garantiza que, a medida que se añaden nuevas firmas y la empresa actualiza sus directrices de seguridad, las apps existentes vuelven a escanearse con cada nueva ejecución, y no solo la primera vez.

Jamf elabora este listado de malwares conocidos, específicos para Mac, a partir de sus propias investigaciones intensivas en amenazas dirigidas a macOS, así como de datos obtenidos de terceros sobre amenazas para Mac. Si una organización deseara un control aún más específico sobre el software que se ejecuta en su entorno, la lista de apps puede ampliarse para incluir, además de las aplicaciones bloqueadas por Jamf Protect, su propia lista de hashes binarios, IDs de equipo, etc. Cuando se ejecuta una aplicación cuyo comportamiento o firma se asemeja al de un malware conocido en macOS 10.15 (Catalina) o posterior, Jamf Protect impedirá la ejecución de ese proceso, pondrá en cuarentena el archivo sospechoso y emitirá una alerta señalando su intervención sobre dicho malware. Esta operación no forma parte del rango de acciones de Gatekeeper/XProtect y ha sido diseñada como un conjunto de sus mejores funcionalidades. Jamf Protect es capaz de identificar el malware conocido sin necesidad del atributo de cuarentena que se utiliza normalmente para identificar binarios potencialmente peligrosos, y gestiona su propia base, mucho más amplia, de conocimientos de malware.



Ampliar el modelo de confianza de App Store con Self Service

En ciertas situaciones, puede resultar conveniente determinar qué programas pueden instalar los usuarios mediante un autoservicio de apps con recursos previamente aprobados por IT.

Self Service de Jamf permite el acceso seguro e instantáneo a estos recursos al permitir que IT elabore su propio catálogo de apps de empresa donde los usuarios pueden instalar apps, actualizar configuraciones y solucionar problemas habituales por sí mismos, sin necesidad de mandar un ticket a asistencia de IT.

Controlar y supervisar el comportamiento de las apps

Controles de privacidad para limitar y reconocer el comportamiento de las apps

Los controles de privacidad de sistema se introdujeron con macOS Mojave. Estos controles exigen que los usuarios (o empresas) discriminen las carpetas o acciones a las cuales tienen acceso según qué aplicaciones. Una vez estas aplicaciones hayan recibido el permiso para realizar acciones específicas no se les volverá a preguntar cuando, en el futuro, la misma acción se ejecute desde la misma aplicación. Esta función garantiza que las apps reciben permisos específicos para acceder a las partes potencialmente sensibles del sistema operativo (webcam, micro, combinaciones de teclado o descargas) e invita a los usuarios a considerar el hecho de que están concediendo el acceso de las aplicaciones a datos privados.

Vaya más allá de los controles para auditar y analizar el comportamiento de las apps

Aunque los controles de privacidad limitan lo que las apps tienen autorizado hacer, los usuarios siempre cometerán errores y se abusará de las autorizaciones. Ya hemos explicado el modo en que Jamf Protect permite visibilizar la actividad de las funciones de seguridad integradas de Apple y las capacidades tradicionales de prevención de malware y adware para mantener informadas y protegidas a las empresas. Pero en Jamf creemos que una solución de protección de endpoints no debería limitarse a eso. Jamf Protect ofrece, además, funciones de auditoría y seguimiento tradicionalmente reservadas a productos de detección y respuesta para endpoints (EDR), pero centradas en Apple y con la vista puesta en los estándares de privacidad y seguridad que los usuarios de macOS esperan.

Ingeniería de detección con Jamf Protect

En lo más profundo del cliente Jamf Protect hay un liviano sensor de modo de usuario (sin kext adjunto) que se sirve de uno de los motores de ejecución lógica de Apple, el GameplayKit. Aunque utilizar un motor de juegos para analizar eventos de seguridad no es lo más ortodoxo, esto es lo que le permite a Jamf estar perfectamente integrado en el ecosistema Apple y analizar los datos disponibles del dispositivo, mientras sea necesario, para recopilarlos e informar acerca de ellos. Los motores de juegos también están diseñados para gestionar un gran número de eventos en tiempo real, lo que los hace perfectos a la hora de analizar actividades a medida que tienen lugar en el dispositivo. Compare este diseño con las numerosas soluciones de seguridad centradas en la plataforma Windows y luego migradas a macOS como remedio de última hora, o con aquellas que requieren la recopilación y el análisis de todos los datos en la nube.

Una ventaja adicional de GameplayKit es que, al igual que Yara, mantiene el motor de ejecución y las definiciones de detección separados, lo cual permite la actualización y ampliación de detecciones sin necesidad de actualizar el cliente principal. Las definiciones de detección son también nativas de Apple, y utilizan NSPredicate, un potente lenguaje lógico compatible con la sintaxis de búsqueda típica y las expresiones de uso común. El modelo de datos de Jamf Protect ha sido desarrollado específicamente para sacar partido de las complejas funciones de NSPredicate, incluida su capacidad para invocar funciones nativas y encadenar modelos de datos. Esto desbloquea funcionalidades de difícil o costosa implementación informática de una forma distinta, más tradicional. Por ejemplo, al utilizar el modelo de datos de Jamf Protect y el lenguaje NSPredicate, podemos:

- Dar el aviso si un archivo se borra a sí mismo, una técnica habitual de eliminación del propio rastro. Este caso de uso aparentemente sencillo exige analizar tanto el archivo eliminado como el proceso encargado de su eliminación, sin costosas operaciones conjuntas ni detecciones prefijadas.
- Dar el aviso cuando binarios sin firma, o con firmas sospechosas, persisten como demonios de lanzamiento. Esto implica cotejar un archivo de configuración, extraer una ruta binaria integrada de su contenido y utilizar los metadatos acerca de ese archivo binario en el análisis.
- Dar el aviso cuando una aplicación de Microsoft Office da luz a “hijos inesperados” con los que identificar vulnerabilidades en macros de Office. Este ejemplo pone de relieve la capacidad para comprender las relaciones entre “padres” e “hijos” a fin de descubrir vulnerabilidades en las funciones de las aplicaciones.

- Dar el aviso sobre cualquier otra actividad “de subsistencia” que pueda estar siendo utilizada y sea sintomática de posibles ataques. Este tipo de actividades requieren de acceso a las relaciones “paternofiliales” y de los grupos de procesos, a los parámetros de línea de comandos, etc., para descubrir infracciones en actividades que suelen ser inocuas (curl, ssh, python, etc.).
- Rastrear el uso de USB en toda la empresa y reportar metadatos acerca de los archivos que están siendo copiados a medios extraíbles.

Para hacer más sencilla la comprensión del impacto de este tipo de detecciones, Jamf Protect genera, cuando procede, un plano de los ataques para el entorno Mitre Att&ck. Su cobertura actual incluye casos de uso provenientes de cualquier parte del entorno, e incluye la detección de técnicas en las siguientes categorías:

- Persistencia
- Acceso inicial
- Comandos y control
- Evasión de defensas
- Descubrimiento
- Escalada de privilegios
- Acceso mediante credenciales

Recolección y notificación sencilla de registros unificados

El registro de endpoints es una costumbre arraigada entre la mayoría de analistas de seguridad y administradores de IT, como parte de una auditoría de cumplimiento o cuando buscan eliminar brechas en otros controles de seguridad. En el momento en que macOS pasó de los mensajes de registro syslog a Unified Logging, recopilar, contabilizar e inspeccionar esa información por toda la empresa se volvió mucho más difícil. La app Consola de macOS ofrece una buena visión y acceso a la infraestructura de registro unificado en Mac locales, pero no permite a las organizaciones centralizar esos datos con facilidad.

Con Jamf Protect, los registros de clientes se pueden transmitir a un sistema de registro tan pronto hayan sido inscritos en el registro unificado. Para garantizar que tan solo se recopilan datos específicos, los administradores de Jamf Protect utilizan el mismo lenguaje de filtrado de predicados (NSPredicate) desde la función integrada de “flujo de registros” de línea de comandos. De esta manera, construir sistemas de archivo de datos de registro Mac se convierte en una sencilla configuración en lugar de una engorrosa recolección máquina tras máquina. Entre los ejemplos se incluyen: inicios de sesión y cierre, ssh, AirDrop y los eventos de autorización. Si los datos han sido registrados al acceder al registro unificado, Jamf Protect puede recopilarlos.

En línea con los estándares de Apple

Asistencia durante el día de lanzamiento

Jamf Protect utiliza tecnologías nativas Apple para interconectar con macOS y recopilar los datos necesarios que le permitirán tomar decisiones de seguridad. Estas tecnologías incluyen entornos emergentes como Entreprise Security Framework (ESF) en Catalina+ y OpenBSM Audit en versiones anteriores. Mediante el uso de estos mecanismos, Jamf Protect minimiza el impacto que pueda tener su dispositivo y no arriesga perderse los cambios introducidos en macOS a través de parches o actualizaciones importantes del sistema operativo. Actualizar de forma temprana y frecuente es el protocolo de seguridad más comúnmente recomendado. Las herramientas de seguridad comprometidas con la asistencia durante el día de lanzamiento son fundamentales para cumplir con ese protocolo.

La experiencia de usuario como rasgo característico

Aunque Jamf Protect supervisa, de forma continua, la actividad de apps y usuarios ante posibles amenazas, omite deliberadamente el escaneo de malware inactivo o propio de Microsoft Windows. El escaneado de ficheros que se limitan a formar parte del sistema de archivos, en busca de indicios de malware es, con frecuencia, una de las mejores maneras de ofrecer una mala experiencia al usuario. Este enfoque se asemeja al de Gatekeeper/XProtect en que las amenazas se identifican en el momento de su potencial ejecución, de modo que la experiencia de usuario y la productividad se vean mínimamente perjudicadas.

Privacidad

Jamf Protect analiza los datos del dispositivo y solo recoge la información pertinente cuando se configura a tal efecto; habitualmente cuando detecta alguna actividad potencialmente maliciosa o de interés, en tiempo real. Esta solución equilibra las necesidades de la empresa con la privacidad de los usuarios, ya que no es necesario extraer tantos datos de usuario del dispositivo para guardarlos en la nube. Cuando se identifica alguna actividad maliciosa, dicha actividad y los datos asociados a ella son transmitidos a la consola Jamf Protect en la nube, o a los sistemas de seguridad de la información y gestión de incidentes (SIEM) configurados. En caso de solicitarlo, cualquier otro dato específico también será trasladado a Jamf Protect o SIEM. Al filtrar los datos innecesarios, el analista de seguridad encargado de supervisar e investigar los incidentes recibirá datos aplicables concretos y de gran calidad.

Más mejoras sobre el modelo de seguridad de Apple

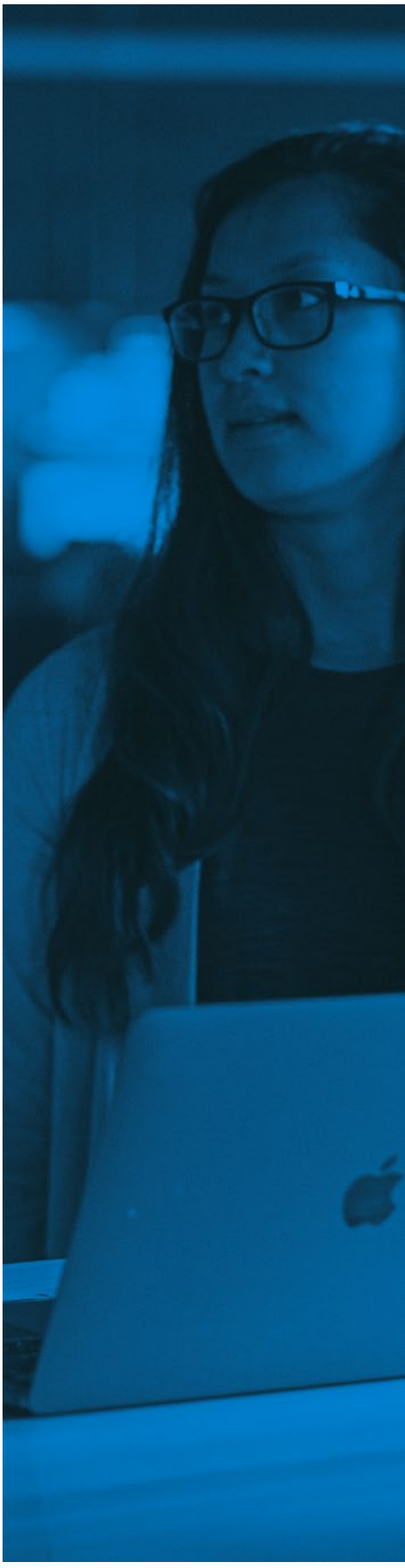
Práctica recomendada: fortalecer macOS

Aunque Apple ofrece y mantiene algunos de los sistemas operativos más seguros y fiables disponibles, es costumbre preguntarse qué medidas adicionales se pueden adoptar para conseguir que macOS se adapte aún mejor al entorno corporativo.

El primer paso recomendado es comenzar a beneficiarse del entorno de gestión de dispositivos móviles de Apple (MDM) y garantizar así una gestión automática a escala. MDM no solo le ayudará a proteger mejor su organización, sino que se hará cargo de gran parte del trabajo de gestión y protección de su flota.

El entorno MDM, introducido con OS X 10.7 (“Lion”), permite una cantidad increíble de flujos de trabajo con los cuales personalizar la funcionalidad del dispositivo y ajustarlo a las necesidades específicas de la organización. Los perfiles de configuración y los comandos de gestión son las dos formas más habituales de sacar partido a MDM para garantizar la seguridad de los equipos al margen de su ubicación.

Lleve la seguridad a otro nivel con MDM al combinarlo con el potencial de Apple Business Manager, una solución gratuita de Apple para empresas que permite automatizar la provisión de hardware, su gestión y mucho más.



Empiece con Apple

A lo largo de los años, Apple se ha labrado una reputación como empresa que prioriza la seguridad, y macOS es un ejemplo de ello. Funcionalidades nativas como el cifrado FileVault 2, la autenticación en dos pasos, los bloqueos y borrados remotos, y la posibilidad de imponer estándares de código de acceso, vienen de serie con cada nuevo Mac que se suma al entorno de una organización.

Las modernas plataformas de gestión –como Jamf Pro– se sirven de MDM para llevar estas características un paso más allá, y ayudan a personalizar la implementación, la aplicación y la redacción de informes acerca de herramientas de seguridad como el cifrado.

Crezca con Jamf

Aunque MDM es un buen pilar para cualquier organización, muchos se preguntan qué más pueden hacer para mejorar aún más sus directrices de seguridad y blindar la privacidad de sus empleados. Aquí es donde entra Jamf.

No es ningún secreto que, en cierta medida, la gestión de dispositivos acaba siendo en un derroche de recursos para el equipo. Más gente significa más hardware y más hardware un mayor gasto en IT.

Al menos, así era antes de las plataformas de gestión de flotas como Jamf Pro.

Apoyados en tecnologías propietarias como los grupos inteligentes, que ayudan a organizar los dispositivos corporativos y ejecutan funciones de gestión de forma automática, los equipos de IT pueden pasar menos tiempo con la cabeza enterrada en la gestión de dispositivos y disfrutar de más tiempo libre para dedicarse a otras tareas de cada día. Los grupos inteligentes supervisarán, ojo avizor, los inventarios de dispositivos, añadiendo y eliminando dispositivos de grupos predefinidos, en tiempo real, a medida que cambien los estados de un dispositivo.

Gestión de identidad moderna en macOS

El pilar de la seguridad más moderna es la identidad, el acceso seguro y personalizado para usuarios finales. Los modelos antiguos de IT se apoyan en servicios de directorio locales que actúan a modo de registro centralizado de datos acerca de los empleados, como nombre y departamento. A medida que evolucionan las necesidades de seguridad e implementación, las empresas deben adoptar un nuevo enfoque sobre la identidad como parte de su estrategia empresarial. Con un modelo de identidad integral basado en la nube, las empresas pueden unificar la gestión de identidad en todo su hardware y software para aprovechar nuevas prestaciones y flujos de trabajo avanzados y para, en última instancia, transformar su forma de trabajar.

A partir de información de servicios de directorio, el SSO en la nube garantiza que los usuarios finales introducen credenciales seguras a la hora de acceder a los recursos de la empresa.

Jamf Connect lleva estas formas comunes de gestión de identidad más allá.

Jamf Connect unifica la identidad en todas las apps de la empresa y el Mac del usuario, sin comprometer la confianza. Los usuarios finales utilizan una única identidad en la nube para acceder de forma rápida y sencilla a los recursos que necesitan para trabajar.

Gracias a Jamf Connect, las organizaciones han logrado:

- Simplificar el aprovisionamiento y la autenticación desde el principio, para ofrecer asistencia integral a sus empleados tanto remotos como in situ
- Automatizar la sincronización de identidades de usuario y credenciales de dispositivo
- Dotar a IT de funciones de gestión de identidad completas en todos sus servicios y dispositivos

Responder y remediar las amenazas para Mac

Jamf Pro, el estándar de gestión de Apple, proporciona tableros de control que ayudan a mantener a las organizaciones al tanto del estado de sus dispositivos Mac y detectar el hardware que necesita atención. Gracias a las funcionalidades patentadas de Smart Group, los administradores de IT podrán localizar los dispositivos que necesitan parches o ser actualizados para mejorar su situación de seguridad. Todo esto puede hacerse de forma remota y automática, para que IT nunca necesite entrar en contacto físico con el dispositivo.

Cuando Jamf Protect se combina con Jamf Pro, la resolución de amenazas va un paso más allá. Al servirse de esta tecnología de grupos inteligentes, todos los comandos de MDM y Jamf Pro pueden orquestarse en respuesta a las alertas derivadas de actividades detectadas por Jamf Protect. Esto incluye el aislamiento automatizado de la red, la restauración de imágenes, el acceso condicional fallido, las notificaciones de usuarios o cualquier otro método específico de solución y respuesta. Con Jamf Pro y Jamf Connect unidos, los ataques contra un usuario o dispositivo pueden dar lugar a una suspensión de credenciales, cambios en la forma de acceso y otros tipos de intervención relacionados con la identidad.

A más Apple más beneficios sin precedentes

Apple no va a dejar de ganar terreno en la empresa si cada vez más usuarios exigen Mac. Una vez implementadas las herramientas adecuadas, los equipos de IT y de seguridad de la información pueden sacar adelante iniciativas Mac con absoluta confianza, y dotar a los usuarios de los recursos y el acceso que necesitan, todo ello sin olvidar ningún aspecto de la seguridad y la privacidad.

Aproveche hoy las soluciones Jamf para empresas y disfrute de la visión y las soluciones que su moderna organización necesita.

Empezar O póngase en contacto con su distribuidor de Apple para realizar una prueba gratuita de Jamf.