jamf

DOCUMENTO TÉCNICO

Rellenando los huecos: la seguridad en macOS

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

La necesidad de seguridad se extiende a todos los sistemas operativos y macOS no es una excepción. Apple ha realizado grandes inversiones para proporcionar funciones nativas de privacidad y seguridad, pero el valor de atacar la plataforma Mac aumenta a medida que se incrementa su cuota de mercado empresarial, lo que la convierte en un objetivo más apetecible para el malware, las brechas y el descubrimiento de vulnerabilidades. Más que nunca, las empresas permiten a sus empleados utilizar macOS a través de programas de elección del empleado. Es por eso que, como sucedería con cualquier otra plataforma, se necesitan seguridad y visibilidad adicionales.

Muchos proveedores de seguridad ofrecen soluciones adicionales de protección para Mac, pero muchas de estas soluciones usan un modelo de seguridad específico para ese proveedor y sus productos para Windows, en lugar de trabajar con los modernos mecanismos que ofrece macOS. Esto dificulta estar al día con todas las novedades de un sistema operativo en constante evolución. En vez de ello, las prácticas recomendadas consisten en ampliar el modelo de seguridad macOS existente, rellenar los huecos 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 protegen tanto al usuario como su privacidad, la facilidad de uso y la productividad siempre han sido aspectos prioritarios. La experiencia Apple está fuertemente enfocada al usuario más que en el negocio en el que opera. Y lo mismo podría decirse de muchas de las funciones de seguridad y privacidad de macOS.

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

Usted conocerá:

- Detalles de las características de seguridad disponibles integradas en Mac
- Cómo Jamf consigue mejorar estas funciones en la empresa
- La manera en que Jamf amplía la detección de amenazas más allá de las firmas y las funciones integradas
- Formas adicionales para extender el modelo de seguridad de Apple para lograr una seguridad empresarial avanzada

Aplicaciones en macOS

Apple ha realizado un gran esfuerzo para diseñar funciones de seguridad para proteger al 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 las plataformas de Apple en: **support.apple.com/guide/security/**.

Verifique la confianza con Gatekeeper.

La ruta más segura y preferida por Apple para instalar aplicaciones de terceros es desde la App Store. Hacerlo de esta manera permite que Apple revise y filtre los programas que no cumplan 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 aplicaciones 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 que los desarrolladores de macOS distribuyan sus aplicaciones directamente mediante descargas directas y otros métodos de distribución tradicionales. Para apoyar estas distribuciones “a la medida”, Apple ha introducido otros controles en el sistema operativo para reducir el riesgo de distribución generalizada de software a través de dispositivos macOS. Gatekeeper es el nombre de la función que se encuentra en el centro de los controles de verificación de Apple. Lo que comenzó como una opción de macOS que permitiera a los programas ejecutarse según su nivel de riesgo, ha evolucionado en un amplio y estricto conjunto de requisitos y medidas de mitigación. Siguen existiendo los niveles básicos de aceptación para permitir apps descargadas de la "App Store" o de la "App Store y desarrolladores identificados", pero la opción de ejecutar código problemático o riesgoso continúa marginada.

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 realiza una serie de controles como verificar el atributo de cuarentena para determinar si puede ejecutarse.
Una de estas comprobaciones más básicas es si la app está firmada por un desarrollador legítimo o si ha sido distribuida por la App Store, en función de la configuración comentada anteriormente.

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, debe subirse primero a Apple para su análisis. Una vez superado el análisis con éxito, los datos de certificación se asocian a la aplicación para señalar que ha superado este nivel de inspección adicional.

La confianza definitiva depende del usuario.

En beneficio de la usabilidad, macOS permite en muchas situaciones que el usuario final "ignore" Gatekeeper. El usuario puede simplemente hacer clic con el botón derecho en la aplicación y seleccionar "abrir" o "abrir con". En lugar de negarse rotundamente a iniciar la aplicación, un nuevo aviso advertirá simplemente al usuario que está ejecutando una aplicación desconocida o potencialmente maliciosa, pero Gatekeeper le permitirá hacerlo. Es importante señalar que el malware que XProtect tiene identificado definitivamente no puede ser autorizado para ejecutarse por un usuario.

Una vez ejecutada la aplicación por primera vez, se actualiza el atributo de cuarentena 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 (Marlware Removal Tool, MRT). Juntos son capaces de escanear archivos del sistema operativo, buscando atributos en su interior que se hayan asociado a algún malware conocido. XProtect se activa desde el lanzamiento de la aplicación, 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. Para verificar una aplicación, XProtect escanea cada ejecutable descargado en la ejecución inicial y tras las actualizaciones posteriores. Si se detecta alguna firma coincidente, no se permitirá la ejecución del programa. Los archivos de firmas denegadas reconocidas se obtienen mediante actualizaciones independientes a macOS desde Apple. Apple define y entrega estas firmas cuando considera que se ajustan, al margen del propio motor de ejecución de Yara. Tal y como sucede con Gatekeeper, esta comprobación solo se realiza cuando una aplicación contiene el atributo de cuarentena ampliado correcto, que se actualiza una vez que haya tenido lugar la primera ejecución exitosa de la aplicación.

Por otro lado, MRT se ejecuta de forma programada en vez de cuando arranca el programa y escanea el sistema de archivos en busca de nombres de archivo específicos y de artefactos asociados con malware que haya podido dejar a su paso, y los elimina una vez descubiertos. Esta característica en gran medida tiene por objeto localizar y remediar amenazas conocidas que puedan estar ejecutándose ya en el entorno macOS.

Ampliación del rango de Gatekeeper a la empresa.

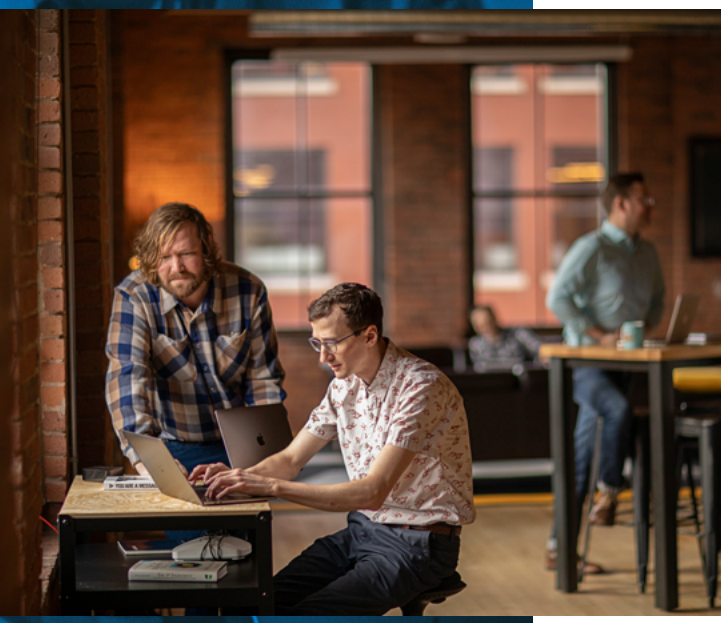
Gatekeeper opera de manera eficiente tal para lo que se creó. Impide que se ejecuten aplicaciones no confiables y notifica al usuario cuando identifica una aplicación como sospechosa o maliciosa. Los administradores de IT y de seguridad necesitan tener visibilidad de los intentos de ejecutar software no confiable en un activo corporativo. Más importante aún, necesitan tener conocimiento de cualquier usuario que haya decidido hacer clic derecho para ejecutar una aplicación y eludir así el control de seguridad de la empresa. Con objeto de atender a estas necesidades empresariales, Jamf Protect —una solución de seguridad para terminales diseñada específicamente para Mac— monitorea en busca de indicios de acciones de Gatekeeper e informa de los resultados a una ubicación centralizada para que los equipos de IT y seguridad puedan evaluar de manera precisa sus riesgos y tomar decisiones informadas.

Más allá de ofrecer visibilidad a la actividad de Gatekeeper, Jamf Protect también permite a las empresas tomar posesión del modelo de confianza de los desarrolladores al registrar información de acceso adicional como no confiable en el entorno empresarial. Basándose en el más reciente entorno de seguridad para terminales de Apple, Jamf Protect denegará de forma proactiva la ejecución de cualquier aplicación de la lista de bloqueo específica de la empresa. Esto puede definirse a nivel por aplicación (ID de aplicación) o a nivel por 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 aplicaciones de adware y de minería criptográfica que pueden llegar a participar en comportamientos no deseados y potencialmente invasivos. A menudo, estos programas están firmados

legítimamente por un desarrollador de Apple y el usuario acepta, en el momento de la instalación, que se recopile su información o se utilicen sus recursos, normalmente sin darse cuenta. Por lo tanto, en muchos casos, Apple no interfiere en el funcionamiento de estas aplicaciones.

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 confiables que utiliza para escanear procesos en el momento de su ejecución, sin importar 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 aplicaciones existentes vuelven a escanearse con cada nueva ejecución, y no solo la primera vez.



Jamf elabora este feed de malware conocido dirigido a Mac basándose en la amplia investigación de Jamf sobre amenazas dirigidas a macOS, así como en datos de terceros sobre amenazas para Mac. Para las organizaciones que deseen un control aún más exhaustivo del software que se ejecuta en su entorno, pueden ampliar la lista de aplicaciones bloqueadas por Jamf Protect con su propia lista de hashes binarios, TeamIDs, 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 administra su propia base, mucho más amplia, de conocimientos de malware.

Ampliación del modelo de confianza de App Store con Self Service.

En ciertas situaciones, puede resultar conveniente imponer 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 facultar 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 tícket de asistencia a IT.

Controle y supervise el comportamiento de las aplicaciones.

Limite y reconozca el comportamiento de las aplicaciones con controles de privacidad.

Los controles de privacidad de sistema se introdujeron en macOS Mojave. Estos controles exigen que los usuarios (o las empresas) permitan el acceso por aplicación a acciones y carpetas específicas. 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 aplicaciones reciban permisos explícitos para acceder a las partes potencialmente sensibles del sistema operativo (cámara web, micrófono, 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 aplicaciones.

Aunque los controles de privacidad limitan lo que las aplicaciones 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 pensamos que una solución de protección de terminales no debería limitarse a eso. Jamf Protect ofrece, además, funciones de auditoría y monitoreo tradicionalmente reservadas a productos de detección y respuesta para terminales (EDR), pero con un primer enfoque 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 agente Jamf Protect hay un sensor de modo de usuario ligero (sin texto 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 o reportarlos. Los motores de juegos también están diseñados para manejar un gran número de eventos mientras suceden en tiempo real, lo que los hace perfectos para analizar actividades a medida que tienen lugar en el dispositivo. Compare este diseño con las numerosas soluciones de seguridad enfocadas primero en la plataforma Windows y migradas después 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 agente principal. Las definiciones de detección también son nativas de Apple y utilizan NSPredicate, un potente mecanismo de consulta lógica que soporta la sintaxis de consulta típica junto con expresiones regulares. El modelo de datos de Jamf Protect ha sido desarrollado específicamente para sacar partido de las complejas funciones de NSPredicate, incluyendo su capacidad para invocar funciones nativas y encadenar modelos de datos conjuntamente. Esto desbloquea funcionalidades de difícil o costosa implementación informática de una forma distinta, más tradicional. Por ejemplo, utilizando el modelo de datos de Jamf Protect y NSPredicate podemos:

- Emitir una alerta 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 de difícil codificación.

- Alertar si un binario sin firma, o con firmas sospechosas, persiste como launch daemon. Esto implica analizar un archivo de configuración, extraer una ruta binaria integrada de su contenido y utilizar los metadatos acerca de ese archivo binario en el análisis.

- Alertar cuando una aplicación de Microsoft Office da luz a hijos inesperados para identificar la vulnerabilidad de 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.

- Alertar de cualquier otra actividad subrepticia que pueda estar siendo utilizada y sea sintomática de posibles ataques. Este tipo de actividades requieren de acceso a relaciones de hijos/padres y de grupos de procesos, parámetros de línea de comandos, etc., para descubrir infracciones en actividades que de otra forma son 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 mapea los ataques identificados al marco ATT&CK™ de MITRE, cuando procede. Su cobertura actual incluye casos de uso provenientes de cualquier parte del marco, e incluye la detección de técnicas en las siguientes categorías:

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

Recolección y notificación simple de registros unificados

La mayoría de los analistas de seguridad y administradores de IT tienen grandes necesidades de los registros de terminales como parte de una auditoría de observancia o cuando buscan cerrar brechas en otros controles de seguridad. En el momento en que macOS pasó de los mensajes de registro syslog al registro unificado, se volvió mucho más difícil recopilar, contabilizar e inspeccionar esa información por toda la empresa. La app Consola.app 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 recopilen 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 la línea de comandos. De esta manera, construir sistemas de registros para los datos de registro de Mac se convierte en una simple 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.

Soporte en el día de lanzamiento

Jamf Protect aprovecha las tecnologías nativas Apple para interconectarse con macOS y recopilar los datos necesarios que le permitirán tomar decisiones de seguridad. Estas tecnologías incluyen los marcos emergentes como la API de seguridad de las terminales de Apple y el marco de auditoría OpenBSM anterior. 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 que se adhieren firmemente al soporte del día de lanzamiento son fundamentales para cumplir con ese protocolo y un componente crítico en una estrategia de seguridad integral de defensa en profundidad.

La experiencia de usuario como rasgo característico

Aunque Jamf Protect monitorea de forma continua la actividad de aplicaciones y usuarios ante posibles amenazas, omite deliberadamente el escaneo de malware inactivo o propio de Microsoft Windows. El escaneado de archivos 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 para tal efecto, habitualmente cuando detecta alguna actividad potencialmente maliciosa o de alto 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 administración de incidentes (SIEM) configurados. Cualquier dato específicamente solicitado más allá de eso también se envía a Jamf Protect o a 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.

Otras ampliaciones al modelo de seguridad de Apple

Práctica recomendada: fortalecer el macOS

Aunque Apple ofrece y mantiene algunos de los sistemas operativos más seguros y confiables 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 administración de dispositivos móviles de Apple (MDM) y garantizar así una administración automática a escala. MDM no solo le ayudará a proteger mejor su organización, sino que le quitará a IT gran parte del trabajo de administración 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 que se puede personalizar la funcionalidad del dispositivo y ajustarlo a las necesidades específicas de la organización. Los perfiles de configuración y los comandos de administración son las dos formas más habituales de sacar partido a la MDM para garantizar la seguridad de los equipos independientemente 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 administración 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 manera estándar con cada nueva Mac que se suma al entorno de una organización.

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

...Mejore con Jamf.

Aunque la MDM es un buen pilar para cualquier organización, muchos se preguntan qué más pueden hacer para mejorar todavía 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 administración 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 administración de flotas como Jamf Pro.

Apoyados en tecnologías propietarias como Smart Groups (grupos inteligentes), que ayudan a organizar los dispositivos corporativos y ejecutan funciones de administración de forma automática, los equipos de IT pueden pasar menos tiempo con la cabeza enterrada en la administración de dispositivos y disfrutar de más tiempo libre para dedicarse a otras tareas de cada día. Smart Groups supervisará con 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.

Administración de la identidad moderna en macOS

El pilar de la seguridad más moderna es la identidad, el acceso seguro y personalizado para usuarios finales. Los modelos heredados 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 administración de la identidad y el acceso como parte de su estrategia empresarial. Con un modelo de identidad integral basado en la nube, las empresas unifican la identidad en el hardware y el software para desbloquear la funcionalidad, los flujos de trabajo avanzados y, en última instancia, transformar el negocio.

A partir de información de servicios de directorio, el inicio de sesión único (SSO) en la nube garantiza que los usuarios finales introduzcan unas credenciales seguras para acceder a los recursos de la empresa.

Jamf Connect lleva estas formas comunes de administración de la identidad más allá.

Jamf Connect unifica la identidad en todas las apps de la empresa y en la Mac del usuario, con flujos de trabajo de autenticación fluidos. 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:

- Aprovisionamiento y autenticación agilizados al sacar de la caja el equipo para que los empleados a distancia y en la empresa tengan todo lo que necesiten.
- Automatizar la sincronización de identidades de usuario y credenciales de dispositivo
- Dotar a IT de funciones de administración de identidad completas en todos sus servicios y dispositivos
- Una solución de acceso a la red de confianza cero (ZTNA) que sustituye a las redes privadas virtuales (VPN) heredadas y satisface las necesidades de la empresa moderna e híbrida

Respuesta y resolución de amenazas para Mac

Jamf Pro proporciona tableros que ayudan a mantener a las organizaciones al tanto del estado de sus dispositivos Mac y señala 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 Smart Group, 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, 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 resoluciones relacionadas con la identidad.

Seguridad más allá de la administración de dispositivos

Lea nuestro informe sobre el estado de la seguridad de Apple en la empresa, en el que se encuestó a 1,500 profesionales de IT e InfoSec. Incluye el uso y los enfoques actuales de los dispositivos, los retos para la seguridad de los dispositivos y el estado futuro de la seguridad de las terminales.

Trusted Access

es la solución de Jamf para la seguridad más allá de la administración. Trusted Access es un flujo de trabajo único que conjunta la administración de dispositivos, la identidad de los usuarios y la seguridad de las terminales para ayudar a las organizaciones a crear una experiencia de trabajo que aprecien los usuarios y un lugar de trabajo seguro en el que las organizaciones confíen.

Utilizando Jamf Protect con Jamf Pro y aprovechando Jamf Connect, los administradores pueden asegurarse de que solo los usuarios de confianza accedan a las aplicaciones corporativas en dispositivos de confianza y en cumplimiento. Si hay un problema con un dispositivo infectado, puede ser solucionado rápidamente y puesto de nuevo en servicio con Jamf Pro.

Trusted Access con Jamf aumenta drásticamente la seguridad de su moderno lugar de trabajo a la vez que agiliza el trabajo de sus usuarios, sin importar en dónde se realice el trabajo.

Administre y asegure Apple para obtener beneficios sin precedentes.

Una vez implementadas las herramientas adecuadas, los equipos de IT y de seguridad de la información pueden poner en marcha iniciativas Mac con absoluta confianza, verificar y autentificar identidades y accesos, y dotar a los usuarios de los recursos y el acceso que necesiten, todo ello sin pasar por alto ningún aspecto de la seguridad y la privacidad.

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

Empiece ahora

O póngase en contacto con su distribuidor preferido para probar Jamf de forma gratuita.

jamf

www.jamf.com/es/