PARA MAC, IPAD, IPHONE Y APPLE TV

La seguridad en los dispositivos Apple

PARA PRINCIPIANTES

Un ciberataque bien organizado o una descarga accidental de malware pueden marcar la diferencia entre un día productivo y un paro total en la actividad. A medida que los hackers van sofisticando sus técnicas, si las organizaciones quieren proteger su cuenta de resultados y también los datos de sus clientes, empleados o estudiantes, la seguridad debe convertirse en una prioridad ineludible.

Las preocupaciones de seguridad de Apple, como todas las preocupaciones de seguridad del sector, son reales.

Aunque Apple ha invertido importantes recursos en el desarrollo de sus funciones de seguridad, hasta situarse en una posición de liderazgo en privacidad y seguridad de datos y dispositivos, ningún sistema operativo es inmune a los desafíos en este terreno.

Por tanto, los administradores no solo deben dar respuesta rápidamente a los problemas de seguridad, sino también adoptar medidas para protegerse.

Esta guía está pensada para administradores y supervisores que quieran tomarse en serio la seguridad de los dispositivos Apple en su organización y contiene información básica que le ayudará a iniciarse en la administración de dispositivos Apple o a refrescar sus conocimientos.

Introducción a la seguridad de Apple

Eliminar palabra pilares sólidos

A la hora de garantizar la seguridad del hardware y los datos de su organización intervienen diferentes factores, que pueden dividirse en seis áreas diferentes:

Seguridad nativa de Apple

Sistemas de seguridad integrados en macOS, iOS y tvOS

Página 4

Protección de dispositivos

Seguridad de sus dispositivos físicos y protección de sus usuarios

Página 6

Encriptación de datos

Conceptos básicos de la encriptación de datos estáticos y datos en tránsito

Página 8

Control del cumplimiento

Supervisión de dispositivos para identificar qué actualizaciones son necesarias

Página 11

Seguridad de aplicaciones y parches

Actualización de software

Página 12

Implantaciones seguras

Implantación con el máximo nivel de seguridad disponible

Página 14

Pilar número uno: Seguridad nativa de Apple

Consejos para sacarle todo el partido con la gestión de dispositivos

Las funciones de seguridad integradas en macOS (sistema operativo del Mac), iOS (sistema operativo del iPad y el iPhone) y tvOS (sistema operativo del Apple TV) son numerosas y aportan interesantes ventajas:

- Los sistemas operativos de Apple están basados en una arquitectura UNIX, conocida por su fiabilidad y su gran estabilidad.
- Potente entorno de seguridad del SO
- Protección de los equipos a través de bloqueos y localizadores de dispositivos
- Posibilidad de aplicar y configurar controles de seguridad a través de opciones de seguridad mediante gestión de dispositivos móviles (MDM)

Una solución de MDM puede partir de estas configuraciones de seguridad existentes y desplegarlas (e imponerlas) en un volumen importante de dispositivos. Así, no solo podrá configurar un Mac de forma segura, sino miles.

También tiene a su alcance controles de seguridad más estrictos, con una herramienta de MDM capaz de bloquear y borrar dispositivos perdidos o sustraídos de la empresa.

Funciones de seguridad al detalle

Funciones de seguridad nativas para macOS, iOS y tvOS

Funciones de seguridad de macOS

- Actualizaciones de software
- Protección de la Integridad del Sistema (SIP)
- Gatekeeper
- App Store
- Cifrado de FileVault
- XProtect
- Zona protegida (sandboxing) de app
- Ajustes de privacidad

Funciones de seguridad de iOS

- Actualizaciones de software
- Sistema seguro
- App Store
- Touch ID
- Cifrado por hardware
- Zona protegida (sandboxing) de app
- Privacidad
- Supervisión
- Localizador remoto de dispositivos perdidos

Funciones de seguridad de tvOS

- Actualizaciones de software directas de Apple
- Apps del App Store validadas y seguras
- Supervisión (con MDM)
- Restricciones en apps
- Ajustes y contraseñas de AirPlay
- Banner/pantalla por omisión

Pilar número dos: Protección de dispositivos

Seguimiento, seguridad y protección de dispositivos y usuarios

Una de las formas más fáciles de poner en peligro el entorno de seguridad de una organización o la seguridad de un usuario final es a través del acceso a un solo dispositivo. Tanto si los usuarios de su organización son estudiantes o profesores como si son profesionales del sector sanitario, teletrabajadores, dependientes o viajeros frecuentes, la cuestión es que en un momento dado los dispositivos de su organización pueden estar en veinte sitios diferentes.

Dispositivos perdidos o robados

Un iPad, iPhone o Mac perdido o robado no solo hace daño al bolsillo, sino también a la seguridad. Y los daños pueden ser incalculables, por ejemplo si un delincuente consigue localizar datos confidenciales de un estudiante en un portátil perdido o accede a toda la base de datos de la organización desde ese portátil. O un antiguo empleado que sigue teniendo acceso a su portátil del trabajo y divulga información privada o la ofrece a empresas competidoras. Incluso puede colarse malware de una fuente remota.

Las pérdidas y los robos de dispositivos son habituales. Cualquiera puede tener un accidente o un despiste, por lo que es fundamental asumir que ocurrirá, aunque no sabemos cuándo.

Además, muchos dispositivos, especialmente los que utilizan estudiantes y pacientes o los que comparten varios usuarios, necesitan medidas de protección contra usos incorrectos, acceso accidental a datos ajenos o reproducción de contenidos inadecuados.

Protección o restricción de dispositivos manualmente:

Mac

- Contraseña obligatoria en todos los dispositivos
- Activación de Buscar mi Mac a través de Preferencias del Sistema > iCloud
- Necesidad de que cada usuario individual inicie sesión en iCloud y recuerde la contraseña
- Seguimiento de todos los números de serie de Mac
- Notificación online a Apple en caso de pérdida o robo de un dispositivo
- Activación de controles parentales en el dispositivo para bloquear sitios web (solo aplicable al navegador Safari)

iPad y iPhone

- Contraseña obligatoria en todos los dispositivos
- Activación de Buscar mi iPhone a través de Preferencias del Sistema > iCloud
- Necesidad de que cada usuario individual inicie sesión en iCloud y recuerde la contraseña
- Notificación online a Apple en caso de pérdida o robo de un dispositivo
- Activación de controles parentales en un dispositivo individual y creación de diferentes cuentas para cada dispositivo

Apple TV

- Contraseña obligatoria en todos los Apple TV
- Restricciones de uso:
  - En el menú principal, vaya a Ajustes > General > Restricciones
  - Seleccione Restricciones para activarlas
  - Cuando el sistema se lo solicite, cree un código de cuatro dígitos
  - Introduzca los cuatro dígitos de nuevo para confirmar y seleccione OK
  - Asegúrese de recordar el código
  - Repita el proceso con todos los Apple TV

Protección de dispositivos

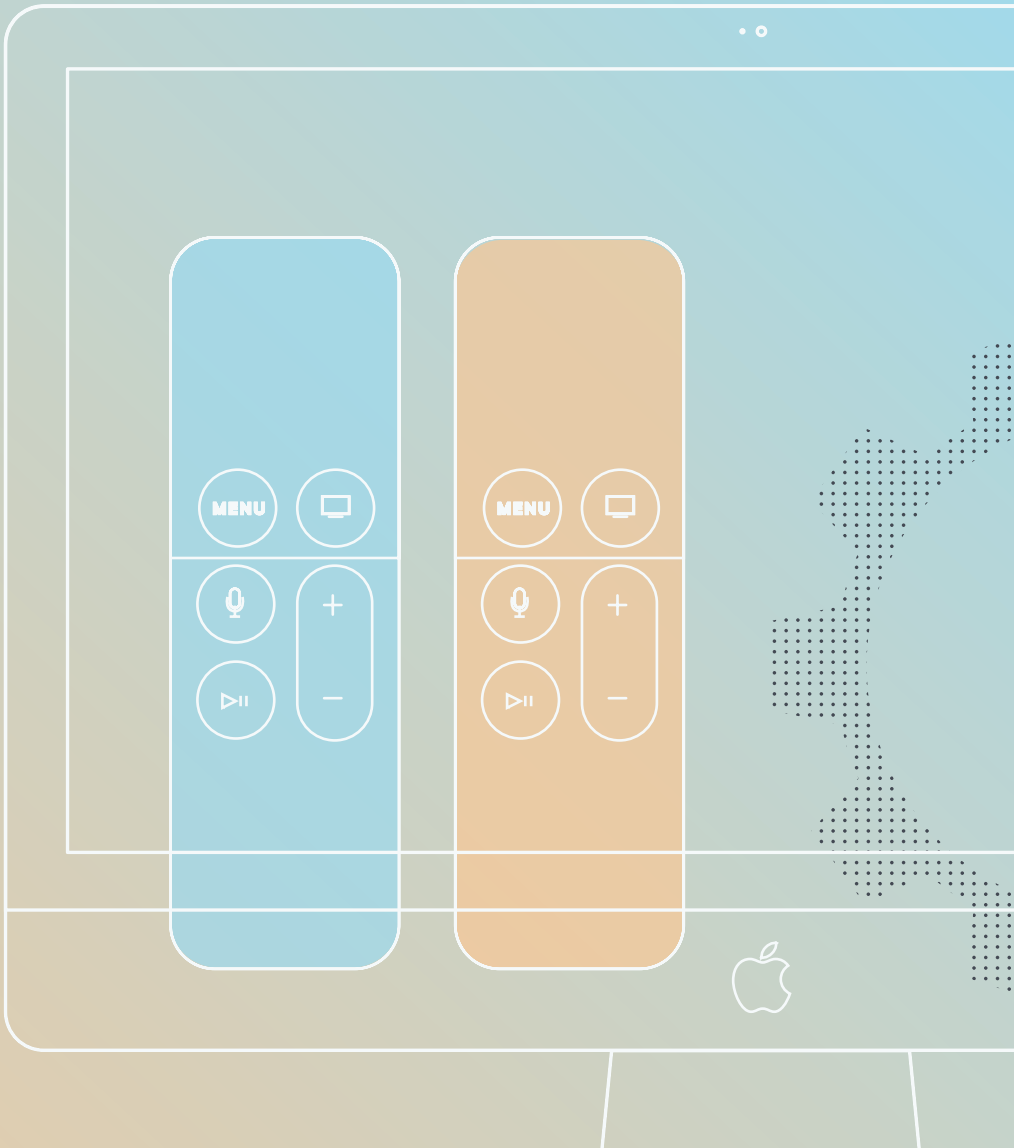
Restricción de AirPlay en Apple TV:

- En el menú principal, vaya a Ajustes > AirPlay
- Active o desactive AirPlay
- Elija entre:
  - Todo el mundo
  - Cualquiera en la misma red
- Repita el proceso con todos los Apple TV

Protección o restricción de dispositivos con una solución de MDM como Jamf:

Mac, iPad, iPhone y Apple TV

- Defina todas las restricciones y funciones de seguridad desde el primer uso o configuración con perfiles de configuración o políticas
- Bloquee de forma centralizada cualquier dispositivo perdido o utilizado incorrectamente
- Borre de forma centralizada cualquier dispositivo perdido o utilizado incorrectamente
- Permita a varios usuarios compartir dispositivos de forma segura, utilizando sus propias credenciales con sus ajustes o borrando el dispositivo al pasar de un usuario a otro, por ejemplo en entornos hospitalarios



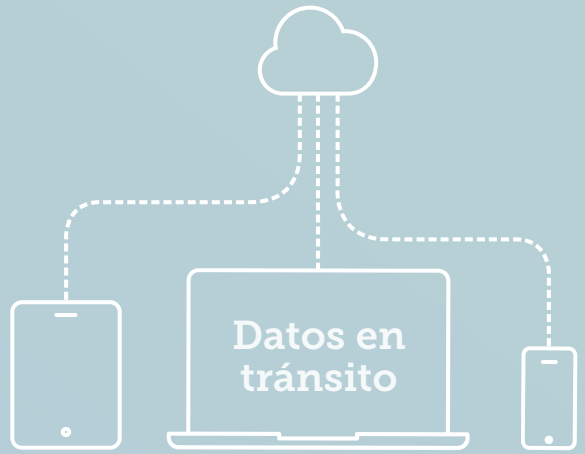
Pilar número tres: Encriptación de los datos

Conceptos básicos sobre datos estáticos y datos en tránsito, y claves para la seguridad de los dos tipos de datos.

Tanto si su organización es un centro educativo que quiere proteger la información de los estudiantes como una institución médica que custodia historiales de pacientes o una empresa que desea proteger la propiedad intelectual, la encriptación ya no es simplemente una opción: es una necesidad. El mejor consejo es encriptar todos los datos de los dispositivos.

Hay dos tipos de datos:

Datos en dispositivos o en bases de datos.



Información que circula de forma inalámbrica de un punto a otro.

Encriptación de los datos

Datos estáticos: Cifrado del disco o el dispositivo.

- macOS ya incorpora una herramienta de encriptación del disco: FileVault. Para encriptar una unidad del Mac no hace falta ningún software adicional.
- FileVault cuenta con la certificación FIPS 140-2. Por tanto, Apple aplica un nivel de encriptación igual de estricto que el sistema del gobierno estadounidense.
- Puede activar FileVault de forma manual o remota: el usuario puede seleccionar la opción en un dispositivo o el departamento de IT puede activar FileVault (con Jamf) en cientos o incluso miles de dispositivos en una sola sesión.
- Jamf garantiza el almacenamiento centralizado de las claves de encriptación por si necesita obtener datos o si alguien se va de la empresa o ha olvidado la contraseña.

Para activar manualmente FileVault:

1. Vaya a Preferencias del Sistema > Seguridad y privacidad > FileVault
2. Seleccione la opción para activar la opción desde allí
3. Repita el proceso con todos los dispositivos

Para activar FileVault en los dispositivos de su organización, puede utilizar una solución de MDM para automatizar, implantar y aplicar la encriptación. Puede implantar un perfil de configuración o una política que active FileVault, y el equipo de IT puede recuperar las claves de encriptación si algún trabajador necesita desencriptar el dispositivo en otro momento.

1. Cree un perfil de configuración simplemente seleccionando una serie de opciones en Jamf
2. Realice la implantación en todos los dispositivos que quiera
3. No hay paso tres

Con Jamf también puede configurar el redireccionamiento de la clave de recuperación, aunque el usuario haya activado FileVault por su cuenta. En este caso, el equipo de IT guardará la clave en su solución de gestión.

¿Y qué hay del iPad o el iPhone?

La encriptación de dispositivos iOS es todavía más sencilla. Los dispositivos iOS cuentan con encriptación integrada nada más definir un código. Puede hacerlo individualmente o bien con Jamf, además de definir parámetros para el código como la longitud y la complejidad.

Encriptación de los datos

Datos en tránsito:
Una VPN (red privada virtual) puede proteger los datos cuando circulan de forma inalámbrica de un dispositivo a otro servicio.

Las personas que viajan o trabajan a distancia deben usar una VPN para conectarse a la red de su organización. Este saludable hábito permite establecer una conexión segura con la red de confianza de su organización, lo que garantiza la encriptación de extremo a extremo de los datos enviados.

Tanto macOS como iOS incluyen clientes VPN integrados para conectar con diferentes proveedores de servicios VPN de referencia.

Qué necesitará para los datos en tránsito

- Una conexión de red segura
- Un servidor VPN

Para establecer la conexión con una VPN manualmente:

Tras configurar un proveedor de VPN:

1. Vaya a Preferencias > Red
2. Escriba la dirección del servidor de VPN en el dispositivo
3. Seleccione el servidor en sus opciones de red
4. Repita el proceso con todos los dispositivos

Para conectar varios dispositivos a una VPN:

Tras configurar un proveedor de VPN:

1. Cree un perfil de configuración en una solución de MDM, como Jamf para iOS y/o Mac
2. Implante las configuraciones en tantos dispositivos como quiera
3. Efectivamente... No hay paso tres

¿Cómo puedo saber que la encriptación funciona?

Una buena forma de garantizar la seguridad y una encriptación fiable es alojando su solución de MDM en la nube. Con un producto de prestigio como Jamf Cloud, tendrá la tranquilidad de saber que su servidor está seguro y sus datos también, y de que podrá acceder al instante a cualquier actualización o parche.

Pilar número cuatro: Control del cumplimiento

La importancia de aplicar protocolos y controles a todos los dispositivos

Un sistema de seguridad no sirve de mucho si tiene puntos débiles. Para tener todos los flancos cubiertos, los administradores deben supervisar los dispositivos de la organización y asegurarse de que todos están actualizados, tienen los últimos parches y funcionan con las opciones de encriptación correctas.

Control manual del cumplimiento:

Para garantizar que todos los dispositivos de su organización están protegidos, deberá mantener una supervisión constante de los dispositivos.

1. Realice un seguimiento físico de cada dispositivo
2. Revise cada opción individualmente para comprobar que:
   - Las actualizaciones de software están al día
   - La encriptación está activada
   - Nadie ha introducido malware ni virus
3. Las actualizaciones solo sirven si tenemos la más reciente instalada, por lo que deberá insistir
4. E insistir otra vez
5. Este proceso requerirá una vigilancia permanente y también la colaboración y la implicación de los usuarios finales

Control del cumplimiento con Jamf:

Para garantizar que todos los dispositivos de su organización están protegidos con la función de inventario de Jamf:

1. Visualice información actualizada y en tiempo real en todos los dispositivos de forma simultánea
2. Implante actualizaciones y configuraciones de seguridad en cualquier dispositivo que no esté correctamente protegido
3. Repita con nosotros: no hay paso tres

La posibilidad de ver los estados de los dispositivos ayuda a los administradores a saber qué actualizaciones enviar y dónde, y qué funciones de seguridad configurar. Los grupos inteligentes basados en departamentos, permisos, dispositivos u otros métodos de categorización ofrecen a los administradores la posibilidad de aplicar las actualizaciones de forma selectiva o global.

Pilar número cinco: Seguridad de las aplicaciones y parches

Parches siempre al día y aplicaciones seguras

Seguridad de las aplicaciones:

Es vital tener la certeza de que sus aplicaciones no contienen malware ni otros códigos hostiles. Si no puede confiar en las fuentes de sus aplicaciones, toda su seguridad estará en riesgo.

Apple ha reforzado al máximo la seguridad en la descarga y la utilización de las apps gracias a las siguientes funciones:

- Adopción de un **modelo de zona protegida (sandbox)**: cada app tiene su propio espacio y no puede interactuar con otras aplicaciones. Para que una app pueda escribir o leer datos compartidos de otra hace falta la aprobación del usuario o el administrador.
- Apps del **App Store** validadas para minimizar su riesgo para la seguridad: no hay otra forma de hacer llegar una app a un dispositivo iOS. Los usuarios de Mac solo pueden instalar apps del App Store, lo que permite a los administradores controlar la seguridad en todos los dispositivos.
- **Gatekeeper para macOS** es una función que los usuarios pueden seleccionar o que, en el caso de una solución de MDM como Jamf, los administradores pueden configurar para todos los dispositivos. Los usuarios o administradores pueden elegir entre tres opciones de Gatekeeper, para permitir apps descargadas de:
  - Mac App Store
  - Mac App Store y desarrolladores identificados
  - Cualquier sitio

Lo más recomendable es permitir apps del Mac App Store y de desarrolladores identificados, especialmente si crea sus propias aplicaciones o reempaqueta apps. Póngales su propia firma para que pasen el filtro de Gatekeeper.

Aunque el Mac permite las descargas desde cualquier sitio, conocer el origen de la app y saber que lleva la firma de un desarrollador de confianza es la única forma de asegurarse de que no se ha modificado en ningún punto antes de instalarse en un equipo.

Configuración manual de opciones de Gatekeeper:

1. Vaya a: Preferencias > Seguridad y privacidad > General
2. Seleccione una de las tres opciones disponibles
3. Repita el procedimiento con todos los dispositivos de su organización

Configuración de opciones de Gatekeeper con Jamf:

Siguiendo el mismo esquema que hasta ahora, puede configurar e implantar un perfil de configuración en todos los dispositivos.

Así de fácil.

Seguridad de las aplicaciones y parches

Parches:
Cualquier software, creado por humanos que cometen errores, puede presentar fallos. No hay forma de evitarlo. Los humanos tenemos este inconveniente: somos humanos.

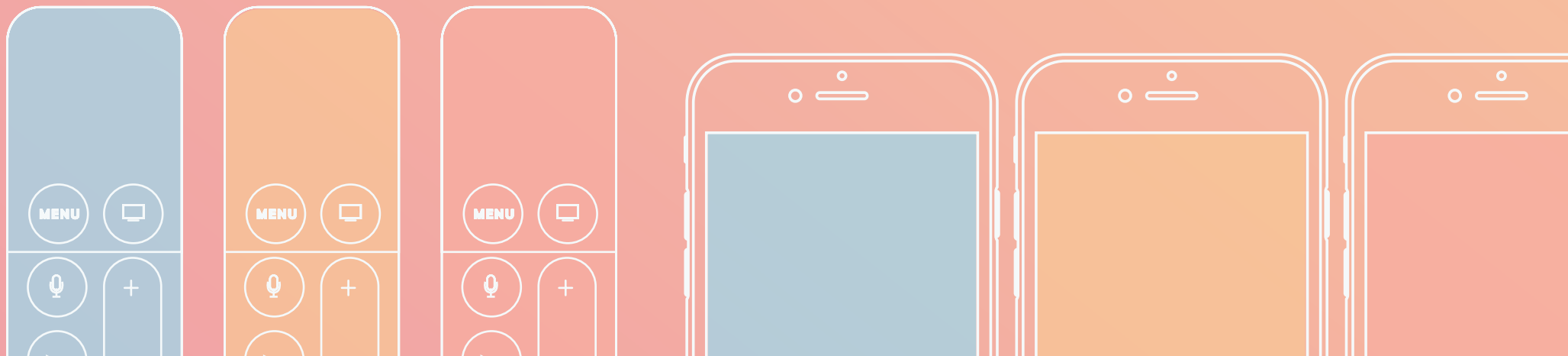
Por eso es tan importante que las organizaciones desplieguen una estrategia para integrar las correcciones de errores lo antes posible, porque los errores pueden traducirse en vulnerabilidades.

Opciones para gestionar manualmente los parches:

- Concienciar a los usuarios sobre la importancia de actualizarse enseguida cuando reciban avisos de actualización en sus dispositivos.
- Juntar todos los dispositivos cuando salga un nuevo parche de una app y realizar la descarga manualmente.
- Aprovechar los controles manuales del cumplimiento para instalar los parches que falten.

Opciones para gestionar los parches con Jamf:

- Jamf recibe notificaciones automáticas de parches y actualizaciones, y cuenta además con herramientas para distribuir los parches a todos los dispositivos de su organización para que nadie se salte nunca ninguno.
- Con el catálogo de apps Self Service de Jamf, los usuarios lo tienen más fácil que nunca, ya que reciben una notificación cuando una actualización es obligatoria para poder continuar usando la app.
- Otra opción es impedir a los usuarios la aplicación de actualizaciones y enviar parches en forma de políticas a todos los dispositivos o solo a algunos, seleccionados mediante Grupos inteligentes dinámicos.



Pilar número seis: Implantaciones seguras

Implantaciones seguras de dispositivos y software con Jamf y la inscripción de dispositivos de Apple

El primer paso para garantizar eliminar palabra implantaciones seguras en todos sus dispositivos es la inscripción gratuita en el Programa de Inscripción de Dispositivos de Apple.

Con la inscripción de dispositivos, puede informar a Apple de todos los dispositivos propiedad de su organización e indicarle que desea gestionarlos todos a través de la solución de MDM que utiliza. Entonces, la primera vez que se ponga en marcha un dispositivo vinculado al programa, se inscribirá automáticamente en la solución de MDM de su organización, lo que permitirá aplicar eliminar palabra controles de seguridad más estrictos e instalar actualizaciones más rápidamente, además de aplicar todos los perfiles de configuración. Así no solo ganará tiempo, sino que también reforzará la seguridad y evitará tener que confiar en el ensayo y error.

jamf

Jamf pone en sus manos:

Inscripción sin intervención

Implantaciones escalables

Configuraciones seguras

Para Mac, iPad, iPhone y Apple TV

Con la seguridad de los datos y dispositivos, mejor no se la juegue.

Las organizaciones pueden anticiparse a posibles ataques o robos aplicando las medidas de seguridad más estrictas previstas por Apple. Y Jamf puede ayudarles a hacerlo de una forma más práctica, rápida y segura que con protocolos de seguridad manuales.

jamf

No se deje sorprender: tome las riendas de la protección de sus datos y dispositivos, y garantice la seguridad de su organización y de las personas que la conforman.

Descubra las mejores opciones de seguridad probando gratis un producto Jamf o poniéndose en contacto con un representante de Jamf.

Probar producto | Contactar

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