Seguridad de dispositivos Apple

PARA PRINCIPIANTES

jamf

Un ciberataque bien planificado o una descarga accidental de malware pueden marcar la diferencia entre un día productivo y la paralización de todo el trabajo. A medida que los piratas informáticos se vuelven más sofisticados, las organizaciones preocupadas por los daños que puedan producir y por la seguridad de los datos de sus usuarios, como clientes, empleados o estudiantes, deben mantenerse al día en materia de seguridad.

Los problemas de seguridad de Apple, como todos los problemas de seguridad informática, son bastante reales y plantean una amenaza crítica para los recursos de la organización y la seguridad de los interesados.

Apple fabrica sistemas operativos increíblemente seguros; no cabe duda de que su atención a las protecciones de seguridad y privacidad incorporadas a su hardware y software han desempeñado un papel importante en su aumento de popularidad y adopción masiva en empresas, instituciones de educación y otras organizaciones de la industria. Y como Apple sigue siendo la plataforma preferida para el hardware personal y profesional, se ha convertido en un objetivo más atractivo para los atacantes. Esto significa que los administradores deben responder rápidamente a los incidentes de seguridad a medida que surgen y no esperar a que se produzca un problema. En su lugar, los administradores de Mac y los equipos de seguridad (y los interesados a los que apoyan) están mejor servidos para protegerse proactivamente contra ellos antes de que las amenazas puedan convertirse en algo mucho peor, sacando el máximo partido de soluciones adaptadas o creadas específicamente para Apple para protegerse eficazmente contra las amenazas centradas en Apple.

Esta guía está dirigida a administradores y directivos que quieran tomarse en serio la seguridad organizativa de sus dispositivos Apple y ofrece información básica para los recién llegados o incluso un simple repaso para los veteranos de la administración de Apple.

Introducción a la seguridad de Apple

Son varios los factores que actúan conjuntamente para garantizar la seguridad del hardware y los datos de su organización:

1. **Seguridad nativa de Apple:** Sistemas de seguridad ya integrados en macOS, iOS, iPadOS y tvOS.
2. **Dispositivos inscritos:** Inscripción e implementación de dispositivos con administración y visibilidad centralizadas y seguras.
3. **Protección de dispositivos:** Protección de sus dispositivos físicos y salvaguarda de sus usuarios de las amenazas.
4. **Cifrado de datos:** Protección de los datos en reposo y en tránsito, en el dispositivo y en red en todo momento.
5. **Control del cumplimiento:** Dispositivos de vigilancia para determinar el estado de salud y observancia de los criterios de referencia.
6. **Seguridad de las aplicaciones y aplicación de parches:** Mantenerse al día de los parches de sistemas operativos, apps y software.

jamf

1

BLOQUE DE CONSTRUCCIÓN UNO:

Seguridad nativa de Apple

Los dispositivos Apple son las opciones de hardware listas para usar más seguras del mercado, y las soluciones de administración y seguridad diseñadas específicamente para ampliar el poder de Apple.

Las características de seguridad ya integradas en macOS (el sistema operativo para Mac), iOS (el sistema operativo para iPad y iPhone) y tvOS (el sistema operativo para Apple TV) son amplias y muestran varias ventajas:

- **Los sistemas operativos Apple se basan en fundamentos de UNIX, lo que crea una rica base informática a partir de una plataforma madura y bien estudiada, con profundas raíces de desarrollo para una estabilidad sólida como una roca.**
- **Marco sólido de seguridad OS:**
  - Notarización
  - Gatekeeper
  - XProtect
  - Herramienta de eliminación de malware (MRT)
  - Transparencia, consentimiento y control (TCC)
  - Respuestas rápidas en materia de seguridad
  - Modo de bloqueo
- **Seguridad de dispositivos físicos en forma de bloqueo y rastreo de dispositivos perdidos con el servicio Find My**
- **Capacidad para implementar y configurar controles de seguridad mediante opciones de configuración a través de la administración de dispositivos móviles (MDM)**
  - Los dispositivos Apple incorporan modos de inscripción seguros, como la inscripción automatizada de dispositivos y la inscripción iniciada por el usuario para dispositivos de propiedad de la empresa y/o personales, para satisfacer todas las necesidades de los modelos de propiedad (como BYOD, CYOD y COPE) sin ninguna URL de inscripción arriesgada ni invitaciones sospechosas por correo electrónico
  - Integración perfecta con Apple Business Manager o Apple School Manager para ayudar en la administración centralizada de todo el hardware institucional, incluida la habilitación de la supervisión de dispositivos por aire y la transferencia segura a su solución MDM para funciones de administración de dispositivos, como la implementación administrada de aplicaciones, el aprovisionamiento seguro de dispositivos y los flujos de trabajo de incorporación sin contacto.

Una solución MDM creada de forma específica puede tomar estas configuraciones de seguridad existentes, alinearlas con sus necesidades organizativas únicas, incluidas las referencias de la industria, e implementarlas (así como hacerlas cumplir) en todo su flota Apple, sin importar su tamaño. Por lo tanto, puede configurar una Mac de forma segura y eficaz con la misma facilidad con la que configuraría miles de estos dispositivos. También obtendrá controles de seguridad más amplios con una herramienta MDM que facilita la realización de tareas administrativas en cualquier dispositivo que seleccione. Por ejemplo, puede agilizar las tareas repetitivas bloqueando y borrando a distancia los dispositivos perdidos, o los que deban eliminarse del inventario de sus instalaciones, por citar algunos ejemplos. Obtenga más información con nuestro ebook de Administración de dispositivos Apple para principiantes.

Detalles de las características de seguridad

Características de seguridad nativas para macOS, iOS, iPadOS y tvOS

macOS	iOS y iPadOS	tvOS
Actualizaciones de software	Actualizaciones de software	Actualizaciones de software
Protección de la Integridad del Sistema (SIP)	Sistema seguro	App Store
Gatekeeper	App Store	Ajustes y contraseñas de AirPlay
App Store	Identificación biométrica	Restricciones de apps
Cifrado de FileVault	Cifrado por hardware	Protector de pantalla
Supervisión	Supervisión	Supervisión
XProtect y la herramienta de eliminación de malware (MRT)	Zona protegida (sandboxing) de app	
Find My	Find My	
Ajustes de privacidad	Ajustes de privacidad	
Notarización y cuarentena de archivos	Secure Enclave e identificación biométrica	
API de seguridad de endpoints	Notarización	
Zona protegida (sandboxing) de app		
Secure Enclave e identificación biométrica		

2

BLOQUE DE CONSTRUCCIÓN DOS:

Dispositivos inscritos e implementados de forma segura

Como ocurre con todos los bloques de construcción, la clave del éxito es una base sólida. Esto informa a cada uno de los siguientes bloques de construcción y establece el tono general para la administración y la seguridad en lo que respecta a los ciclos de vida del hardware y las aplicaciones.

El primer paso para aprovisionar correctamente los dispositivos e implementarlos de forma segura en toda la flota de una manera estandarizada y eficiente, es utilizar la inscripción automatizada de dispositivos, que se incluye como parte de los servicios gratuitos que ofrece Apple a través de Apple Business Manager y Apple School Manager.

Con la inscripción automatizada de dispositivos, puede informar a Apple de todos los dispositivos que posee su organización, así como de otros modelos de propiedad que se comentan a continuación, y asignarlos para que sean administrados por la MDM de su organización. Cuando un dispositivo inscrito en este programa se encienda:

- Se inscribirá de forma automática en su instancia de MDM
- Habilitará la supervisión, que es integral para permitir controles de seguridad más estrictos
- Permitirá que los administradores apliquen perfiles de configuración y endurezcan los ajustes.
- Garantizará que los ajustes de seguridad críticos y las cargas útiles se implementen antes de que el usuario pueda empezar a utilizar un dispositivo.
- Simplificará la administración y la implementación de actualizaciones OS y los parches de seguridad.
- Reducirá la cantidad de flujos de trabajo de aprovisionamiento de los dispositivos centralizando la adquisición, configuración e implementación de apps, lo que también garantiza la seguridad de las apps procedentes de fuentes de confianza y verificadas.
- Reducirá la configuración de dispositivos, facultando a usuarios para mantener sus dispositivos sin necesidad de asistencia de IT.
- Permitirá la administración remota sin importar el dispositivo compatible que se utilice, desde dónde y a través de cualquier conexión de red.

Modelos de propiedad de los dispositivos

Automatizar la administración y la seguridad de su flota de dispositivos es una característica fundamental, especialmente a medida que aumenta el número de dispositivos y se descentraliza la fuerza laboral. El aumento de la adopción y dependencia de la plataforma Apple y los dispositivos móviles en el espacio de trabajo se ha vuelto tan diverso como las industrias y usuarios que dependen de estos dispositivos para seguir siendo productivos.

Algunas organizaciones han adoptado los productos Apple implementando programas de elección del empleado que asignan dispositivos propiedad de la empresa que ejecutan macOS e iOS y iPadOS, mientras que otras organizaciones han adoptado Apple en el trabajo permitiendo
que los empleados utilicen dispositivos de su propiedad para acceder a los recursos de la empresa. Al facultarles para trabajar más cómodamente utilizando el hardware y el software con el que están más familiarizados, las organizaciones compensan el gasto de proporcionar equipos para cada interesado, especialmente cuando los usuarios ya tienen un dispositivo funcional que conocen y adoran.

De este modo, la pregunta pasa de "¿Cómo proporcionamos dispositivos a los usuarios?" a "¿Cómo garantizamos que los recursos de la empresa permanezcan seguros?".

Aquí es donde la MDM de su organización y los modelos flexibles de propiedad de dispositivos se encuentran para conformar la solución de múltiples modelos de propiedad de dispositivos, tales como:

Trae tu propio dispositivo (BYOD)

Podría decirse que es el modelo más común, que permite a los usuarios utilizar sus dispositivos personales para acceder a los recursos de la empresa. Al exigir que los usuarios inscriban manualmente sus dispositivos en la MDM de la empresa antes de obtener acceso a los recursos de trabajo, la doble ventaja es que los usuarios pueden estar seguros de que obtendrán las herramientas necesarias para acceder a los datos y servicios que necesitan para desempeñar sus funciones laborales; las organizaciones están más tranquilas sabiendo que los dispositivos inscritos cuentan con el software de seguridad y los ajustes necesarios para mantener protegidos los datos de la empresa mientras se utilizan, en reposo y en tránsito.

Elija su propio dispositivo (CYOD)

Se trata de una variación del BYOD anterior, con la salvedad de que, a menudo, la organización o institución es la propietaria de los dispositivos utilizados en este modelo y deben utilizarse en el desempeño de funciones relacionadas con el trabajo o en la búsqueda de aprendizaje (en el caso de la educación). Al instituir un programa de elección por parte de los empleados, los interesados pueden elegir el dispositivo Apple que mejor se adapte a sus necesidades. Cada dispositivo se inscribe, se asigna a un interesado y es administrado por la MDM de la organización. Las apps, los perfiles de configuración, los ajustes del dispositivo y el software de seguridad se aprovisionan de acuerdo con una línea base de la postura de seguridad de la organización y teniendo en cuenta los requisitos de trabajo del asignado.

Propiedad de la empresa pero habilitado personalmente (COPE)

El modelo COPE es una tendencia creciente entre las grandes organizaciones, especialmente las que se han vuelto totalmente remotas o con entornos de trabajo híbridos. En este caso, las organizaciones adquieren y son propietarias de los equipos, al tiempo que los inscriben y administran por completo en la MDM de la organización. Al igual que CYOD, se instalan y administran las herramientas necesarias para que los interesados realicen sus tareas en función del dispositivo y de la postura de seguridad de la empresa. Pero al igual que en el BYOD, la organización permite e incluso alienta a los usuarios a utilizar los dispositivos para uso personal junto con el uso profesional. Esto garantiza que los datos de la empresa permanezcan seguros dentro de las apps administradas y los perfiles de configuración. Aunque esto puede plantear el problema que datos personales y privados sean accesibles a las empresas a través de dispositivos COPE, es importante tener en cuenta la privacidad de los datos y proporcionar el grado adecuado de administración y privacidad a estos dispositivos mediante políticas de uso aceptable (PUA) y administración de datos.

Métodos flexibles de inscripción

Para simplificar la administración de múltiples modelos de propiedad de dispositivos dentro del mismo entorno de la MDM, Apple ha desarrollado dos métodos de inscripción diferentes que se utilizan conjuntamente para administrar y aplicar la seguridad de la organización sin comprometer la privacidad del usuario y viceversa.

Inscripción automatizada de dispositivos

Este es el método más común que prefieren elegir la mayoría de las organizaciones con equipos propiedad de la empresa. Este método certifica que cada paso de la cadena de inscripción esté verificado: desde la adquisición a Apple (o a un tercero autorizado), pasando por la preconfiguración en la MDM, hasta la fase de inscripción que comienza cuando se enciende el dispositivo; cada paso sigue un procedimiento automatizado desde Apple a la MDM y al administrador para la administración continua. Dado que esta cadena está verificada, la supervisión se activa en los dispositivos inscritos a través de la inscripción automatizada de dispositivos, que actúa como una base de confianza que permite al departamento de IT obtener un control total sobre el dispositivo durante todo su ciclo de vida. La supervisión es la raíz de la confianza, necesaria cuando se realizan determinadas tareas de administración en dispositivos administrados.

Inscripción de dispositivos iniciada por el usuario

Este método de inscripción es más nuevo y más común cuando los dispositivos inscritos son de propiedad personal como parte de un modelo BYOD. Con la inscripción automatizada de dispositivos, la inscripción depende de que el usuario o propietario del dispositivo lo inscriba manualmente en la app Settings y lo autentique con sus credenciales de empresa. Una vez completado el proceso de inscripción del usuario, la MDM de la organización establece una comunicación bidireccional segura entre el dispositivo del usuario y la solución de administración de la organización.

Una vez inscritos, los dispositivos de propiedad personal pueden administrarse a través de la MDM, y los administradores tienen permitido instalar apps administradas, desplegar perfiles de configuración y modificar determinados ajustes mediante un conjunto de configuraciones que permiten a las organizaciones establecer requisitos específicos para cada dispositivo, así como asociar acciones o requisitos de administración con el usuario, no con todo el dispositivo. Apple diseña la limitación para permitir que las organizaciones tomen las medidas necesarias para proteger la forma en que se accede a sus datos, se interactúa con las apps, se almacenan en el dispositivo y se transmiten a través de las redes sin afectar a las apps personales, los datos y la información privados del dispositivo. Las organizaciones pueden personalizar la visibilidad de los dispositivos administrados asociando un Apple ID personal con los datos personales y un Apple ID administrado con los datos de la empresa.

3

BLOQUE DE CONSTRUCCIÓN TRES:

Protección de los dispositivos

Protección de dispositivos, datos y usuarios frente a amenazas

"Los háckers solo tienen que acertar una vez; nosotros tenemos que acertar siempre".

— Chris Triolo, HP

Si volvemos la vista atrás a algunas de las mayores, más complejas e incluso más mortíferas transgresiones de datos de la historia reciente, encontraremos un hilo conductor común. Ataques como Stuxnet deshabilitaron el programa de enriquecimiento nuclear de Irán al infectar la computadora portátil de un contratista que realizaba actualizaciones en el equipo SCADA. LinkedIn fue el blanco de un desarrollador que vulneró su API para obtener información personal de 700 millones de usuarios y venderla en Internet. Aadhaar —que alberga la mayor base de datos de identificación, incluidos datos personales y financieros, de más de 1,100 millones de ciudadanos indios— fue robada y vendida por agentes de amenazas tras acceder a través de un sitio web desprotegido vinculado a la base de datos. En estos casos y en otros similares, los ataques fueron posibles al atacar y comprometer un solo dispositivo.

Una de las formas más comunes de saltarse el marco de seguridad de una organización y obtener acceso a datos confidenciales, al mismo tiempo que se pone en peligro la seguridad del usuario final, es poner en peligro un único dispositivo. Sin importar la industria que represente su organización o si proporciona datos y/o recursos a trabajadores del conocimiento, estudiantes, profesores, proveedores de atención médica, personal remoto, personal de comercios minoristas o viajeros frecuentes — en cualquier momento, sus dispositivos podrían estar en cualquier parte del mundo y conectarse a través de diversos número de redes no confiables— lo que aumenta exponencialmente la exposición al riesgo de amenazas tanto para el dispositivo como para la red de la empresa.

Dispositivos perdidos o robados

La pérdida o el robo de un iPhone, iPad o Mac no es solo una pérdida económica: también representa un enorme riesgo para la seguridad, cuyas consecuencias pueden ser incalculables. Considere los siguientes ejemplos para subrayar la importancia de mitigar el riesgo de dispositivos perdidos y robados:

SITUACIONES REALES

Un empleado en remoto prepara documentos legales para un caso de responsabilidad civil que se está dirimiendo en los tribunales y trabaja desde una cafetería cercana. Deja desatendida brevemente la Mac portátil propiedad de la empresa mientras rellena su taza el café en el preciso momento en que un ladrón se abalanza sobre ella y la roba. Con el dispositivo desbloqueado, el atacante tiene acceso ilimitado a información sensible y posiblemente confidencial de la empresa que podría afectar negativamente a los procedimientos legales en curso y a la reputación de la empresa.

En un segundo ejemplo, un estudiante que utiliza su iPhone de propiedad personal para acceder a recursos relacionados con la escuela a través del portal educativo extravía su dispositivo mientras cambia de clases. Otro usuario encuentra el teléfono y accede a los detalles de la cuenta del estudiante, obteniendo acceso a información confidencial, como su dirección, número de teléfono o credencial de estudiante. Un usuario no autorizado puede utilizar información de identificación personal de esta clase para robar la identidad o cometer delitos haciéndose pasar por la víctima. El dispositivo puede incluso estar infectado con malware y ser devuelto a la víctima, lo que pone en peligro su seguridad y bienestar por el seguimiento en remoto y el acecho de los actores de la amenaza.

En pocas palabras: los dispositivos se pierden y los roban. También ocurren accidentes y momentos de falta de atención. Sin embargo, la planificación, partiendo de la base de que solo es cuestión de cuándo, y no de si alguien perderá el rastro de un dispositivo, es una clave vital para garantizar que se aplican las estrategias de mitigación adecuadas para minimizar el riesgo antes de que los dispositivos se pierdan o sean robados.

Otros aspectos a tener en cuenta para la seguridad de usuarios y datos son que muchos dispositivos —especialmente los que sirven a estudiantes y pacientes o los entornos de dispositivos compartidos que sirven a múltiples usuarios— requieren salvaguardas contra el uso indebido, el descubrimiento accidental de datos ajenos o el acceso y la visualización de contenidos arriesgados e inapropiados.

Dependiendo de las necesidades específicas de su organización, reforzar los ajustes de seguridad al mismo tiempo que se configuran los dispositivos para que estén alineados con los requisitos de organización y cumplimiento, puede ser una tarea considerable que requiera mucho tiempo y trabajo, especialmente a medida que aumenta el número de dispositivos.

Al proteger o restringir dispositivos manualmente, es necesario:

Mac

- Exigir contraseñas en todos los dispositivos
- Activar Buscar mi Mac a través de Preferencias del Sistema > iCloud
- Depender de cada usuario para poder iniciar sesión en iCloud o recordar su contraseña (requisito previo para activar FindMy)
- Informar a Apple si se perdió un dispositivo o lo robaron mientras se habilita la capacidad de iniciar limpieza/borrado
- Dar seguimiento a todo el inventario por números de serie de las Mac o etiquetas de activos
- Activar el control parental en el dispositivo para bloquear contenidos inapropiados y sitios web maliciosos (utilizando el navegador Safari)
- Mantener las Mac al día con todas las actualizaciones de sistemas y apps para minimizar vulnerabilidades
- Configurar y reforzar los ajustes del dispositivo para minimizar los errores de configuración que podrían dejar los datos sin protección
- Implementar aplicaciones compatibles y mantenerlas actualizadas
- Instalar y configurar la seguridad de endpoints para monitorear dispositivos, identificar y remediar amenazas

Teléfono y iPad

- Exigir contraseñas en todos los dispositivos
- Activar Buscar mi Mac a través de Preferencias del Sistema > iCloud
- Depender de usuarios individuales para poder iniciar sesión en iCloud o recordar su contraseña
- Dar seguimiento a todo el inventario por números de serie de los dispositivos o etiquetas de activos
- Informar a Apple si se perdió un dispositivo o lo robaron mientras se habilita la capacidad de iniciar limpieza/borrado
- Activar el control parental en un dispositivo individual, creando cuentas diferentes para cada dispositivo
- Mantener al día los dispositivos basados en iOS con todas las actualizaciones de sistemas y apps para minimizar vulnerabilidades
- Configurar y reforzar los ajustes del dispositivo para minimizar los errores de configuración que podrían dejar los datos sin protección
- Implementar aplicaciones administradas y mantenerlas actualizadas
- Instalar la seguridad de endpoints para monitorear dispositivos, identificar y remediar amenazas

Apple TV

- Exigir contraseñas en todos los Apple TV
- Configurar restricciones:
  - En el menú principal, vaya a Ajustes > General > Restricciones
  - Seleccione Restricciones para activarlo
  - Cuando se le solicite, introduzca un código de acceso de cuatro dígitos.
  - Vuelva a introducir los cuatro dígitos para confirmar y seleccione OK
  - Recordar el código de acceso
  - Repetir para todos los Apple TV

Para restringir AirPlay para Apple TV:

- En el menú principal, vaya a Ajustes > Seleccionar AirPlay
- Activar o desactivar AirPlay

Elegir entre:

- Todo el mundo
- Cualquiera en la misma red
- Repetir para todos los Apple TV

En una solución MDM óptima, como Jamf Pro, las mismas tareas de administración realizadas anteriormente para proteger o restringir dispositivos son las siguientes:

Mac, iPhone, iPad y Apple TV

- Establezca todas las restricciones y características de seguridad desde el primer uso o actívelas automáticamente con Supervisión y perfiles de configuración y políticas de confianza.
- Bloquee o borre cualquier dispositivo perdido o mal utilizado de forma remota, independientemente de su ubicación física, e sin importar si el dispositivo tiene una cuenta de iCloud iniciada o no (no requiere ID de Apple).
- Permita que varios usuarios compartan dispositivos de forma segura borrando un dispositivo entre usos y permitiendo que los usuarios utilicen sus credenciales y ajustes conectados al usuario, no al dispositivo.
- Configure los ID de Apple administrados que se asignarán al dispositivo para las tareas de la empresa al mismo tiempo que permite al usuario acceder a las apps personales, los datos y los ajustes almacenados en iCloud con su ID de Apple de consumidor.
- Mantenga un inventario de todos los dispositivos, incluyendo la capacidad de agruparlos por cualquier categoría —no solo por número de serie o etiqueta de activo— para recabar todos los datos necesarios, como asignaciones de usuario, versión del sistema operativo o apps instaladas, por nombrar algunos.
- Realice tareas de administración que emitan comandos a un solo dispositivo o en masa, como implementar actualizaciones de seguridad, actualizar a una nueva versión del sistema operativo o borrar administrativamente contraseñas olvidadas en dispositivos bloqueados.
- Implemente controles parentales y bloquee el acceso a apps de riesgo o inapropiadas, aplicando restricciones granulares basadas en determinados criterios o a todos los dispositivos a la vez.
- Implemente las aplicaciones administradas necesarias para que los usuarios sigan siendo productivos en casa, en la oficina, en la escuela o en cualquier otro lugar. Pre-aprobar apps para ser alojadas dentro de la app de Self Service, facultando a usuarios a acceder al software que necesiten exactamente cuando lo necesiten.
- Integre las soluciones de seguridad de endpoints con su MDM para garantizar que los dispositivos sean monitoreados y protegidos constantemente frente a las amenazas a la seguridad, al mismo tiempo que comparte datos de telemetría enriquecidos con la MDM para permitir una administración basada en políticas para automatizar la respuesta ante incidentes.
- Administre cada faceta de las tareas de administración de dispositivos de forma centralizada para garantizar que los dispositivos, los usuarios y los datos permanezcan seguros frente a las ciberamenazas, mientras defiende la privacidad de los usuarios.

Esta experiencia no solo simplifica el trabajo de los administradores de IT y el personal, sino que también ayuda a los usuarios finales. Proporciona la experiencia que la gente adora y espera de Apple sin sacrificar los requisitos de seguridad y cumplimiento de la organización y el sector, ni la privacidad del usuario en favor de controles de seguridad más estrictos.

4

BLOQUE DE CONSTRUCCIÓN CUATRO:

Cifrado de datos

Fundamentos básicos de los datos en reposo y en tránsito, y cómo mantener seguros ambos tipos.

Tanto si su organización es una escuela que protege la información de los estudiantes, un centro de atención médica que custodia los historiales médicos de los pacientes o una empresa que pretende proteger su propiedad intelectual, el cifrado ya no es opcional para su organización: es un requisito fundamental para cualquier empresa que desee mantener a salvo datos sensibles, confidenciales y de misión crítica, o realmente para los datos de cualquier tipo de clasificación, la mejor práctica es cifrar todos la información de los dispositivos.

A continuación se resumen los tres estados de los datos en cualquier momento dado en un dispositivo:

Datos en reposo: almacenados localmente (normalmente) en un dispositivo al que no se accede ni se utiliza en ese momento.

Datos en movimiento: datos transferidos —tanto recibidos como transmitidos— a través de un canal de comunicaciones, como una red cableada o inalámbrica.

Datos en uso: no se conservan en almacenamiento permanente ni se transmiten por redes; se trata de datos con los que trabajan actualmente aplicaciones u otros procesos.

Cada uno tiene riesgos inherentes propios de su estado, lo que significa que, en general, una solución para un estado puede no funcionar totalmente para otro (o no funcionar en absoluto). Aunque esto añade complejidad a su estrategia de seguridad, no se preocupe, porque todas las soluciones eficaces se centran en la función fundamental del cifrado.

SITUACIONES REALES

Una persona recién contratada en el departamento de Recursos Humanos de su organización recibe su nuevo Mac y completa rápidamente el proceso de configuración para empezar a trabajar. Una de sus funciones laborales requiere crear un árbol de contactos de emergencia **utilizando un software de hoja de cálculo**, que incluya el nombre de cada empleado, el cargo, la dirección de correo electrónico de la empresa, la dirección personal, el número de contacto personal y especificar si es un contacto principal o alternativo. Esta información debe **guardarse localmente** en la computadora, incluida la información de contacto personal de los miembros de los equipos de administración y los equipos directivos, y debe ponerse a disposición de los interesados autorizados un duplicado para que puedan **acceder a ella desde un repositorio en la nube de forma segura.**

En la situación anterior, las partes en negritas indican un ejemplo concreto de cada estado de los datos. En primer lugar, "utilizar software de hojas de cálculo" es un ejemplo de datos en uso, lo que indica que los datos deben permanecer seguros mientras se trabaja con ellos dentro de la app. Para ello es necesario comprobar y verificar la integridad del software, a fin de asegurarse de que un agente de amenazas o un código malicioso no hayan puesto en peligro su seguridad interna. En segundo lugar, "copia de seguridad local" es un ejemplo de datos en reposo, lo que indica la importancia de activar el cifrado para evitar que personas no autorizadas accedan a los datos y los lean. En tercer lugar, "acceso seguro desde un repositorio en la nube" es un ejemplo de datos en movimiento, como los que se envían y reciben a través de una conexión de red. Las conexiones de red utilizadas para la comunicación deben estar cifradas de extremo a extremo, garantizando que solo las dos conexiones de cada extremo puedan descifrar con éxito el mensaje y proteger estos datos de la recepción no autorizada o de ataques de escucha a escondidas.

Y aunque este tercer estado de datos puede parecerse mucho a los servicios VPN heredados, el componente que lo separa de la VPN heredada es la redacción "partes interesadas autorizadas", ya que Zero Trust Network Access (ZTNA) proporciona cifrado para los datos en movimiento, ZTNA también se integra con su proveedor de identidad (IdP) asegurando que solo los usuarios y dispositivos que se hayan autenticado correctamente y estén aprovisionados con los permisos de acceso necesarios tengan acceso a los recursos solicitados detrás de capas adicionales de protección, defendiendo el principio del mínimo privilegio. Además, a diferencia de los servicios VPN tradicionales, que suelen conceder accesibilidad a toda la red una vez autenticados, la implementación de ZTNA para proteger las conexiones utiliza microtúneles para establecer un túnel único para cada app o servicio protegido. Esto proporciona mayor seguridad al aplicar el principio del menor privilegio, al tiempo que emplea comprobaciones de salud para garantizar que los dispositivos cumplen los requisitos mínimos —junto con los requisitos de autenticación del usuario— cada vez que se realiza una solicitud y antes de conceder el acceso.

Cómo cifrar los tres estados de los datos

Datos en reposo

Cifrado de volúmenes o dispositivos completos

Cifrar los datos almacenados en un dispositivo móvil o en un volumen de la computadora es una buena práctica por varias razones. Compuesto por medidas proactivas y reactivas, el proceso fácil de configurar para activar el cifrado proporciona la máxima protección y seguridad para los datos en reposo en almacenamiento permanente. Utilizar algoritmos que tomaría a los atacantes cientos, o más probablemente, miles de años de trabajo sin descanso utilizando las computadoras más potentes para derrotarlos, dado el esfuerzo relativamente mínimo necesario para configurar el cifrado, es una "obviedad" cuando se trata de incluir este control de seguridad como parte de una estrategia de defensa en profundidad, como El Álamo, o la proverbial "última batalla" entre un actor de amenazas y los datos confidenciales.

Tomemos como ejemplo algunos incidentes de seguridad comunes que se mitigan eficazmente activando el cifrado completo de dispositivos o volúmenes:

Pérdida o robo de un dispositivo

El extravío de dispositivos, como iPhones, iPads o MacBook portátiles es especialmente frecuente en el caso de los dispositivos móviles. A mayor movilidad, mayor riesgo de pérdida o robo. Dicho esto, una vez que un dispositivo está fuera de sus manos, los actores de amenazas tienen vía libre para intentar obtener los datos almacenados en el dispositivo.

Por supuesto, un código de acceso complejo o una contraseña fuerte deberían proteger tu dispositivo. Sin embargo, dependiendo del dispositivo, todavía podría haber medios alternativos para que los atacantes accedan a algunos o todos los datos contenidos en el dispositivo, excepto cuando está cifrado. El simple hecho de activar el cifrado codifica los datos hasta el punto de que serán ilegibles, a menos que los descifre la clave de descifrado. No importa si el dispositivo arranca en la pantalla de inicio de sesión o si se accede de algún modo a la unidad SSD y se conecta a otro dispositivo como unidad externa. Los datos cifrados permanecen cifrados hasta que se utiliza la clave de descifrado o recuperación para descifrarlos; cualquier otra situación hace que los datos sean ilegibles y, por tanto, inútiles.

Accesibilidad física

Al igual que en el caso de los dispositivos perdidos o robados, para obtener accesibilidad física a un dispositivo no es necesario haberlo extraviado. Piense en un dispositivo compartido en un espacio de trabajo, tal vez la computadora dedicada asignada a usted en su escritorio o cualquier dispositivo informático que un actor de amenazas pueda intentar utilizar cuando nadie está viendo. Cuando finaliza su sesión y la cierra, apaga o incluso bloquea su dispositivo mientras se aleja o no lo utiliza, los datos contenidos en el volumen o dispositivo están y permanecen cifrados. Se necesita una clave de descifrado o recuperación para descifrar los datos y obtener un acceso legible a los datos protegidos.

Cumplimiento regulatorio

Dependiendo de la industria a la que pertenezca su organización, puede estar sujeta a leyes —conocidas como reglamentos— que regulan los requisitos mínimos para salvaguardar los datos y la forma en que se procesan, mientras que imponen limitaciones sobre qué funciones laborales están permitidas para trabajar con tipos de datos protegidos. Hay industrias específicas que están reguladas de manera más agresiva que otras; estas son industrias altamente reguladas, como el sector financiero y del cuidado de la salud, mientras que otras pueden solo centrarse en ciertos aspectos de la seguridad de los datos, como las regulaciones educativas que tienen como objetivo proteger el bienestar de los estudiantes y la información personal identificable (PII) asociada a ellos.

Como ya se ha dicho, los reglamentos se basan en leyes y su incumplimiento puede tener consecuencias nefastas para la organización o institución si no se atiene debidamente a las normas de los órganos de gobierno. A menudo, el cifrado de datos es un control de seguridad esencial que se requiere en diferentes estados de los datos, como en reposo o en movimiento, para minimizar el riesgo de que la información regulada caiga en manos equivocadas por fuga de datos, filtración al exterior o incluso exposición a usuarios no autorizados.

Cifrado de datos y dispositivos Apple

- El macOS ya dispone de cifrado de volúmenes integrado en FileVault. No necesita añadir ningún software adicional para cifrar una carpeta, un disco o un volumen en una Mac.
- Las Mac más recientes, como las que se basan en Apple Silicon, dependen de Secure Enclave. Un componente de hardware dedicado que se encarga de la creación y almacenamiento de claves de cifrado, a la vez que realiza cálculos algorítmicos.
- Las Mac basadas en Intel se basan en un componente de hardware dedicado similar denominado chip de seguridad T2 para realizar funcionalidades similares a las de Secure Enclave.
- FileVault cuenta con la certificación FIPS 140-2. Esto significa que el sistema de cifrado de Apple está certificado y cumple los más altos estándares de cifrado del gobierno federal.
- Usted puede activar FileVault de forma manual o remota: los usuarios personales pueden elegir la opción en un dispositivo, o el departamento de TI puede automatizar y aplicar la activación (mediante Jamf Pro) en cientos o incluso miles de dispositivos con una sola política.
- Conceda acceso a los usuarios a volúmenes cifrados/descifrados simplemente autenticándose en macOS o introduciendo su código de acceso en dispositivos iOS y iPadOS. Los usuarios de dispositivos compatibles pueden aprovechar las tecnologías TouchID o FaceID de Apple para agregar una capa de seguridad a la protección de datos a través de la biometría utilizando sus huellas dactilares o patrones de reconocimiento facial.

Para activar manualmente FileVault en macOS:

- Vaya a Ajustes del sistema > Privacidad y seguridad > FileVault
- Seleccione el botón "Activar..." para activar el cifrado del volumen.
- Repetir para todos los dispositivos

Para habilitar FileVault en todos los dispositivos de su organización, aproveche su solución de MDM para automatizar, implementar y exigir el cifrado. Puede implementar un perfil de configuración o una política que active FileVault. IT puede recuperar las claves de recuperación si el personal necesita descifrar el volumen más adelante.

- Cree un perfil de configuración mediante una sencilla selección de opciones dentro de Jamf Pro
- Implemente de forma granular en todos los dispositivos que desee o en todos los dispositivos basados en macOS.
- **No hay paso tres**

Con Jamf Pro, también puede configurar la redirección de la clave de recuperación, incluso si el propio usuario activa FileVault. A continuación, el departamento de IT tendrá la clave guardada en su solución de administración para poder recuperarla fácilmente por registro de dispositivo.

¿Y qué hay de un iPad o un iPhone?

Cifrar dispositivos iOS y iPadOS es aún más fácil. Los dispositivos basados en iOS tienen cifrado integrado desde el momento en que se establece un código de acceso. Puede hacerlo individualmente o exigirlo a Jamf Pro, así como establecer los parámetros para la seguridad del código de acceso, como la longitud mínima y los requisitos de complejidad.

Datos en tránsito

Cifrado de las conexiones de red de extremo a extremo

Las buenas prácticas convencionales dictaban el uso de una VPN para proteger los datos al trasladarse de un dispositivo a otro servicio. Este método se remonta a décadas atrás, ya que se desarrolló en una época en la que las VPN se utilizaban para unir dos redes dispares de forma segura a través de una red no confiable, como Internet.

Y aunque este control de seguridad sigue siendo utilizado activamente por muchos usuarios personales y empresariales, los cambios en el panorama informático de los últimos años, derivados de la adopción de Apple en el trabajo, el crecimiento explosivo de los dispositivos móviles para uso personal y empresarial y la migración de las organizaciones a entornos de trabajo totalmente remotos e híbridos, han puesto de manifiesto los límites de la tecnología VPN para proteger eficazmente dispositivos, usuarios y datos en el panorama moderno de las amenazas.

Todos estos cambios se han combinado para revolucionar nuestra forma de trabajar —y jugar— con computadoras y dispositivos móviles. Entonces, ¿por qué sigue usted confiando en los procesos heredados para que su estrategia de seguridad mantenga a salvo los datos en movimiento?

La respuesta corta es Zero Trust Network Access, o ZTNA para abreviar. La respuesta larga es que esta solución se desarrolló a partir de la propia necesidad del mundo real de mantener varios tipos de dispositivos, usuarios y equipos locales y distribuidos. Además, se accede a los datos a través de redes no confiables y se confía en servicios basados en la nube para ampliar la infraestructura, al tiempo que se erosiona el perímetro de red de la organización. Todo ello sin dejar de protegerlos frente a las amenazas de seguridad existentes y nuevas empleadas por los actores de amenazas, con un notable aumento de las amenazas dirigidas a macOS y a los dispositivos móviles en general.

En pocas palabras: la seguridad de las conectividades de red ya no es solo cosa de empleados que viajan o de algunos casos especiales para seguir siendo productivos en remoto.

También va más allá del mero cifrado de las comunicaciones entre dos puntos y exige protecciones de seguridad granulares, para salvaguardar a los interesados y evitar el acceso a los recursos de la empresa, minimizando al mismo tiempo la introducción de amenazas. Algunas de las formas en que ZTNA logra esto son:

- Integración con IdP basados en la nube para ampliar las cuentas de usuario administradas de forma centralizada e incluir permisos que sigan al usuario.
- Las comprobaciones frecuentes de los dispositivos garantizan que los endpoints cumplan los requisitos mínimos, como estar actualizados con los parches, garantizar que la integridad de la seguridad permanezca intacta comprobando si hay dispositivos a los que se les haya practicado jailbreak o root y que la seguridad de endpoints esté instalada y configurada correctamente.
- Si los endpoints no superan una verificación de salud o se han considerado comprometidos, la integración de ZTNA con una solución MDM de primera línea, como Jamf Pro, permite una administración basada en políticas al compartir de forma segura los datos de telemetría para suspender el acceso y ejecutar flujos de trabajo de remediación con el fin de realizar las tareas necesarias para que el endpoint cumpla las normativas, verificando que se resuelvan los problemas detectados.
- Se renuncia a la confianza implícita, como las VPN heredadas, en vez de operar bajo el mantra de "nunca confíes, verifica siempre" cada vez que se accede a cualquier recurso de la empresa solicitado. Solo después de que la verificación se haya realizado con éxito se concede el acceso al recurso solicitado.

Qué necesitará para los datos en tránsito

Una conexión de red segura a un servidor VPN.

Para conectarse a una VPN manualmente:

iOS y iPadOS	macOS
▸ Vaya a Ajustes del sistema > VPN	▸ Vaya a Ajustes del sistema > Red > VPN y filtros
▸ Seleccione "Añadir configuraciones de VPN"	▸ Seleccione "Añadir configuraciones de VPN"
▸ Escriba la dirección del servidor VPN en el dispositivo	▸ Escriba la dirección del servidor VPN en el dispositivo
▸ Selecciónela de sus opciones de red	▸ Selecciónela de sus opciones de red
▸ Repita para cada dispositivo	▸ Repita para cada dispositivo

Para conectar varios dispositivos a una VPN:

Después de configurar un proveedor de VPN

- ▸ Crear un perfil de configuración en una MDM como Jamf para iOS y/o macOS
- ▸ Implemente configuraciones en todos los dispositivos que desee
- ▸ Lo adivinó: no hay paso tres

"¿Cómo puedo estar seguro de que mi cifrado se realiza sin contratiempos?"

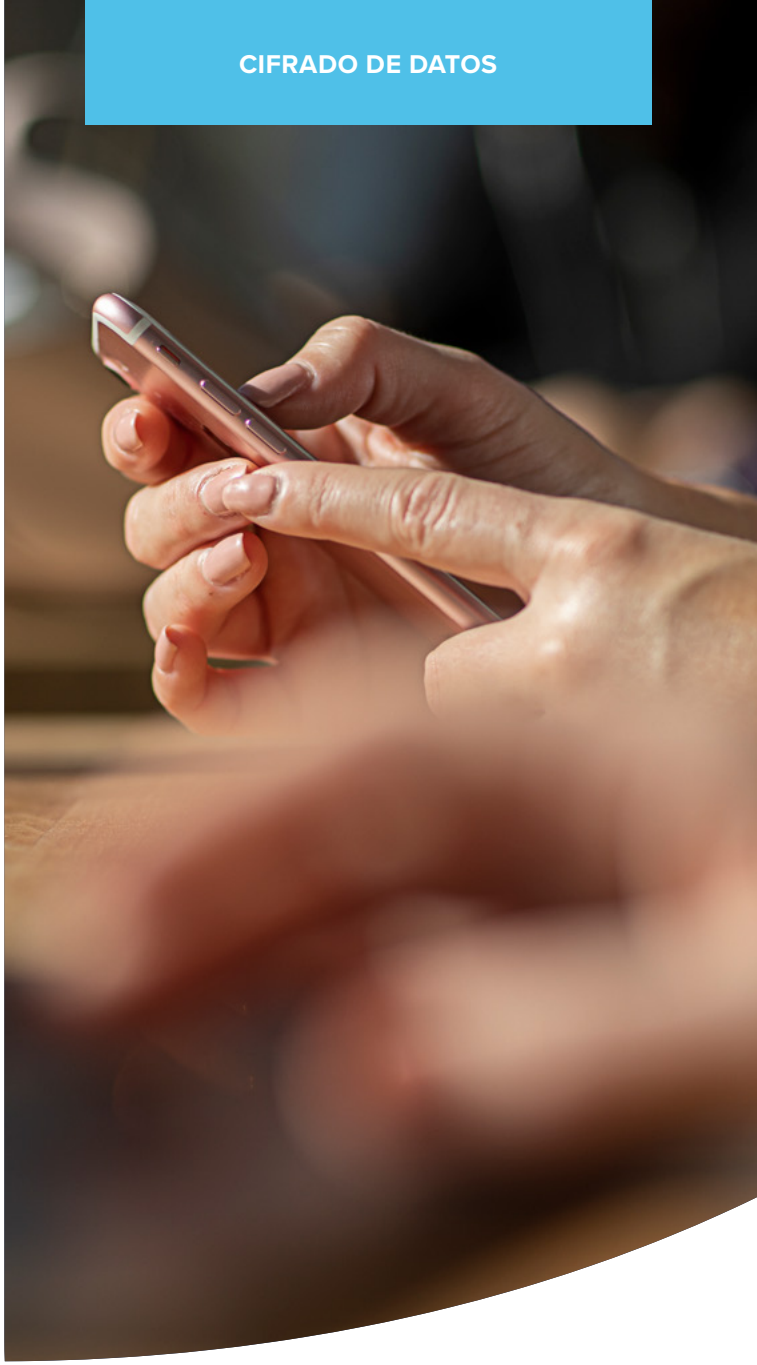
Una forma importante de garantizar la seguridad y un cifrado coherente es alojar su MDM en la nube. Con un producto de confianza como Jamf Cloud, puede estar tranquilo sabiendo que su servidor está seguro y sus datos a salvo, y que cualquier actualización o parche está disponible de inmediato.

Ventajas de ZTNA frente a VPN heredadas:

- La seguridad mejora al pasar de la confianza implícita al modelo explícito de Zero Trust, que exige verificar usuarios y dispositivos antes de conceder acceso a los recursos solicitados.
- La división en túneles protege el tráfico de la empresa, mientras que el tráfico personal se dirige directamente a Internet, no a una red central, lo que reduce la sobrecarga y ahorra ancho de banda, lo que equivale a un mayor rendimiento y una mejor protección de la privacidad de los usuarios finales.
- La protección siempre activa significa que los recursos están protegidos —incluso si el servicio está deshabilitado— al solicitar acceso, se habilitará automáticamente para garantizar que el tráfico permanezca protegido en todo momento.
- Una huella mínima y el alojamiento en la nube significan que no hay costosos contratos de asistencia, configuraciones complejas ni hardware que administrar.
- También es compatible con macOS, iOS, iPadOS, Android y Windows, lo que reduce el TCO y alivia la carga administrativa de los equipos de IT que dan soporte a múltiples tipos de hardware y software.

En esta sección, hemos tratado los fundamentos del cifrado de datos, los tipos de soluciones nativas de los dispositivos Apple e incluso hemos explicado los pasos para activar este control de seguridad en macOS, iOS y iPadOS. También hemos hablado de cómo la moderna tecnología ZTNA va más allá de la protección VPN heredada al seguir protegiendo las conexiones de red remotas al tiempo que incluye capas adicionales de seguridad para verificar a los usuarios y dispositivos antes de conceder las solicitudes de acceso y garantizar que los datos permanezcan seguros en reposo (primero) y en movimiento (después). Pero, ¿qué ocurre cuando los datos son utilizados o procesados por apps?

Desbloquear los otros dos estados de los datos; los datos en uso no tienen un control de seguridad específico para mitigar este riesgo. En su lugar, la solución se encuentra en conjunción con los flujos de trabajo de administración y seguridad en curso.



CIFRADO DE DATOS

Cuando las apps acceden a los datos y los procesan, los datos pasan de la memoria (RAM) a la app para ser procesados y luego vuelven a la memoria antes de guardarse permanentemente en el almacenamiento del dispositivo. Todas las apps desarrolladas por desarrolladores conocidos y de confianza contienen mecanismos de seguridad que garantizan que la seguridad interna de la app permanece intacta. Entre las muchas razones para ello, una de ellas es garantizar que los datos procesados dentro de una app no se compartan o filtren con otras apps, servicios o procesos que se ejecuten en el dispositivo. Esto está diseñado para mantener la integridad de los datos mientras se mantiene la integridad de la aplicación .

Sin embargo, las apps que se han visto comprometidas por el aprovechamiento de una vulnerabilidad tienen modificaciones no autorizadas a su seguridad interna o son apps fraudulentas, comercializadas para simular la realización de una tarea cuando en realidad llevan a cabo otras tareas clandestinas, y ponen en peligro la seguridad de los datos mientras se utilizan.

Entonces, ¿cuál es la mejor solución, se preguntará? Las respuestas que se ofrecen a continuación incluyen una combinación de buenas prácticas, una estrategia de defensa en profundidad y procesos y flujos de trabajo que aprovecha Jamf Pro para mantener los datos en uso lo más seguros posible:

- Una política continua de administración de parches que adquiere aplicaciones de fuentes legítimas, como el App Store de Apple, el sitio web de los desarrolladores o un proveedor de administración de confianza, como App Installers con Jamf.
- Implementar apps administradas a través de su solución MDM preferida e implementando una administración basada en políticas para mantener las apps actualizadas.
- Verificar los ajustes de dispositivos seguros mediante la instalación de perfiles de configuración para minimizar la posibilidad de amenazas derivadas de configuraciones erróneas.
- Reforzar los ajustes del dispositivo para restringir comportamientos de riesgo que podrían introducir amenazas, como el jailbreaking de iOS o iPadOS, o la carga lateral de aplicaciones desde fuentes no autorizadas o inseguras.
- Implementar un programa de capacitación continua de usuarios para mantener a los interesados informados de las amenazas comunes y de cómo determinadas acciones, como las IT en la sombra, introducen riesgos.
- Elaborar una Política de Uso Aceptable (PUA) que firmen todos los interesados para que conozcan las expectativas de comportamiento y las consecuencias de infringir la política de la empresa.

5

BLOQUE DE CONSTRUCCIÓN CINCO:

Monitoreo del cumplimiento

Conozca el estado de los protocolos y controles implementados en todos los dispositivos

Un sistema de seguridad es tan bueno como lo sea su punto más débil. Para obtener la mejor cobertura, los administradores deben monitorear los dispositivos de la organización para comprobar que todos están actualizados, que han recibido los parches más recientes y que cuentan con las opciones de configuración correctas.

"La conciencia de la ignorancia es el principio de la sabiduría".

—Sócrates

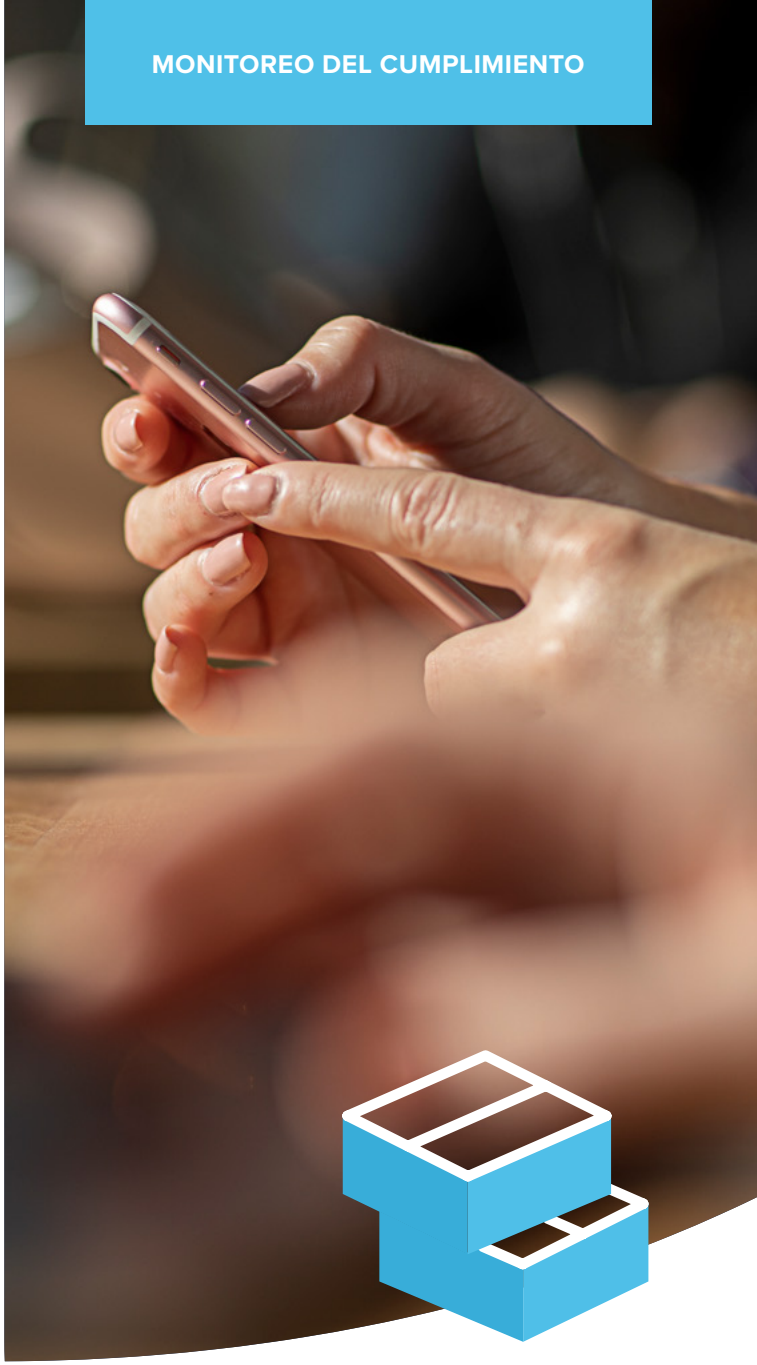
Mediante la recopilación continua de datos de telemetría enriquecidos, los detalles de cada dispositivo que proporciona información sobre los controles de seguridad, la configuración y el estado de salud, el departamento de IT puede proteger mejor a los dispositivos, los usuarios y los datos, al mismo tiempo que se asegura de que los endpoints que estén fuera del alcance se corrijan rápidamente y vuelvan a cumplir las normas antes de que las amenazas puedan provocar resultados mucho peores, como transgresiones de datos.

Como ocurre con la mayoría de los componentes básicos de este ebook, existen múltiples vías para supervisar el cumplimiento de endpoints: métodos manuales y automatizados. Dependiendo de los requisitos de su organización, la eficacia de la supervisión del cumplimiento puede verse afectada por factores contribuyentes, como la base de conocimientos, las soluciones de administración de dispositivos y seguridad utilizadas y las consideraciones presupuestarias, por nombrar algunos de los más críticos.

Monitorear y administrar manualmente el inventario y el cumplimiento de la normativa significa:

- Garantizar la protección de todos los dispositivos de su organización auditándolos constantemente.
- Rastreo físico de cada dispositivo para las necesidades de administración del inventario.
- Actualizar individualmente las aplicaciones de software en cada dispositivo para garantizar que están al día.
- Verificar que los ajustes de seguridad, como el cifrado, están configurados de forma congruente en todos los dispositivos.
- Monitorear y confirmar que nadie ha introducido riesgos, como malware o apps sospechosas.
- Realizar actualizaciones de seguridad críticas y del sistema operativo tan pronto como estén disponibles para parchar vulnerabilidades conocidas y corregir errores en el software
- Desplegar el personal adecuado para clasificar los problemas detectados, poner en cuarentena los dispositivos comprometidos y realizar tareas de remediación para que los endpoints afectados vuelvan a cumplir las normas.

Este método requiere una vigilancia constante y grandes ventanas de tiempo para la sobrecarga administrativa relacionada con la realización de tareas de administración. Se necesita una gran aceptación y cooperación entre las partes interesadas y los equipos de administración para tener éxito. También es importante tener en cuenta que este método es en gran medida de naturaleza reactiva, lo que significa que las situaciones sensibles al tiempo, como los tiempos de respuesta a incidentes, probablemente se alargarán, produciéndose después de que se detecten los problemas, aunque rara vez antes.



Como última consideración, también aumentará exponencialmente el número y los tipos de dispositivos compatibles, un aumento en el tamaño, el tiempo para que IT y Seguridad respondan a los problemas manualmente. Esto les da a los actores de amenazas más tiempo para ampliar las amenazas en su cadena de ataques contra las organizaciones, aumentando simultáneamente el riesgo de una transgresión de datos.

Controlar el monitoreo con Jamf significa:

- Visualizar información actualizada y en tiempo real de todos los dispositivos simultáneamente.
- Implementar actualizaciones y configuraciones de seguridad para todos los dispositivos que no estén protegidos correctamente.
- Ahora, dígalo con nosotros: **no hay paso tres**

La capacidad de ver el estado del inventario de dispositivos ayuda a los administradores a mantener el pulso de todos los dispositivos Apple de su flota. Al conocer el estado actual de un dispositivo, los administradores pueden gestionar eficazmente los dispositivos y la seguridad sabiendo qué actualizaciones enviar y dónde, y qué funciones de seguridad configurar respectivamente. La creación de Grupos inteligentes, basada en criterios dinámicos, permite a los administradores ser tan específicos o abarcar todas las actualizaciones como deseen. Ya sea que se base en permisos granulares, tipos de dispositivos específicos o prácticamente cualquier otro método de categorización, Jamf Pro proporciona herramientas poderosas para reducir el trabajo de las tareas relacionadas con el cumplimiento mientras mantiene cero flexibilidad para concentrarse (o enviar tareas a todos los dispositivos de su flota) a través de criterios personalizables. Obtenga más información con nuestro ebook Administración del inventario para principiantes.

Administración del cumplimiento con medios de Jamf:

- Auditoría de endpoints basada en referencias del Centro de Seguridad de Internet (CIS).
- Transmisión de todos sus datos de cumplimiento a la nube para una administración centralizada.
- Acceso a los registros unificados de macOS y a la telemetría integral de endpoints para identificar amenazas de forma rápida y eficaz.
- Exigir el cumplimiento mediante políticas para automatizar las tareas de remediación y mantener los endpoints dentro del ámbito de aplicación.
- Monitoreo de las vulnerabilidades y exposiciones comunes (CVE) para comprender las vulnerabilidades que existen en su entorno.
- Prevenir las amenazas a la seguridad mediante el uso de analíticas exhaustivas basadas en el marco MITRE &TTACK.
- Compartir de forma segura los datos de telemetría entre soluciones de administración (Jamf Pro) y seguridad (Jamf Protect) a través de una API para desarrollar flujos de trabajo avanzados que minimicen automáticamente los tiempos de respuesta ante incidentes y resuelvan sin demora los problemas identificados.

No es suficiente proteger los dispositivos; muchas normativas exigen que las organizaciones puedan demostrar que los dispositivos siguen siendo seguros y cumplen los requisitos de seguridad. Esto significa que las organizaciones deben proporcionar documentación para corroborar los niveles de cumplimiento durante varios puntos en su línea de tiempo. Después de todo, si usted no puede proporcionar evidencia de que el dispositivo cumplía con los requisitos en un momento dado, entonces, para todos los efectos, no los cumplía.

Sin embargo, los datos y reportes de Jamf proporcionan las herramientas necesarias a las organizaciones para obtener datos de telemetría de cada endpoint y organizar estos datos utilizando categorizaciones críticas, como niveles de parches, vulnerabilidades detectadas y marcas de tiempo que identifican las acciones realizadas durante el ciclo de vida del dispositivo. Además, la integración permite compartir de forma segura los datos de telemetría con herramientas propias y de terceros para ampliar aún más los datos a través de tableros centralizados que incluyan visualizaciones de datos y exportación a otros formatos para compartir informes de cumplimiento con los investigadores normativos.

6

BLOQUE DE CONSTRUCCIÓN SEIS:

Seguridad y administración de aplicaciones

Reporte de parches, políticas e instaladores de apps para mantener las apps actualizadas al mismo tiempo que se exige la seguridad fácilmente.

Seguridad de las aplicaciones

Saber que las vulnerabilidades identificadas están parchadas es vital para la postura de seguridad del dispositivo. Pero, ¿sabe de dónde proceden sus aplicaciones? Y, ¿está seguro de que no contienen malware u otro código malicioso? La respuesta a estas preguntas es fundamental para su organización, ya que si no puede confiar en las fuentes de sus aplicaciones, corre el riesgo de poner en peligro la seguridad de sus dispositivos, así como la privacidad de los usuarios finales y la exposición de datos confidenciales.

Para Apple, preservar la seguridad y la privacidad es una prioridad absoluta. En lo que respecta a la seguridad de las apps, propician que sean lo más seguras posible de descargar y utilizar.

Características de la seguridad y la administración de aplicaciones:

1 **Las apps se ejecutan en una sandbox, o entorno aislado:** cada app se ejecuta en su propio espacio y no puede interactuar con otras aplicaciones. Antes de permitir que las apps lean/escriban en/desde los datos compartidos de otros, se requiere la aprobación explícita de un usuario autenticado.

2 **Adquisición centralizada y segura de apps:** Las apps de la App Store de Apple se examinan para reducir los riesgos de seguridad. Parte de esto se consigue mediante la notarización, mientras que la otra parte proporciona un repositorio seguro basado en la nube y administrado por Apple para alojar apps que han superado rigurosas evaluaciones de seguridad. También ofrece un medio a los desarrolladores para poner en manos de los usuarios la última versión de sus apps alojadas directamente, eliminando la posibilidad de introducir riesgos derivados de descargas de software ilegítimo de fuentes riesgosas.

3 **La notarización garantiza la integridad de la seguridad:** Notarizar apps brinda a los usuarios más confianza en que el software firmado por el ID único de un desarrollador —y descargado a su Mac— ha sido revisado por Apple en busca de componentes maliciosos y problemas de firma de código. Cuando una app está notarizada, puede confiar en que no ha sido manipulada ni puesta en peligro.

4 **Gatekeeper bloquea la ejecución de apps sospechosas:** Antes de permitir la ejecución de cualquier aplicación de macOS por primera vez (y tras cada actualización posterior), los tickets de notarización asignados se comprueban con Gatekeeper para determinar si el ticket es válido o está revocado. En el primer caso, la app queda permitida sin problema. En el último caso, se restringe la ejecución de la app, informando al usuario de que puede haber sido modificada por un tercero no autorizado, lo que afecta a la integridad de su seguridad interna.

5 **Restricciones en el uso de apps:** En los dispositivos que ejecutan iOS, la única forma segura de obtener apps es a través de la App Store. Dicho esto, aplicar jailbreake a dispositivos iOS y iPadOS introduce la posibilidad de acceder a tiendas de apps de terceros que a menudo se utilizan para distribuir apps que han sido "crackeadas", o a las que se les ha eliminado la seguridad interna, como las apps de pago que se ponen a disposición de forma gratuita pero que a menudo han sido inyectadas con código malicioso por actores de amenazas para robar datos o espiar a los usuarios. Con una MDM, como Jamf Pro, los administradores pueden configurar alertas que les avisen cuando se identifiquen dispositivos con jailbreak, lo que les permite realizar flujos de trabajo de remediación para corregir el problema de seguridad.

En macOS, los usuarios (o administradores con una MDM) pueden elegir entre dos opciones de Gatekeeper:

- App Store de Mac
- App Store de Mac y desarrolladores identificados

Confinar a los usuarios de macOS a la App Store de Mac para descargar sus apps permite a los administradores controlar la seguridad de apps en todo el dispositivo, al tiempo que se minimiza el riesgo de introducir amenazas —maliciosas o de otro tipo— de apps sospechosas, riesgosas y/o comprometedoras. Sin embargo, si se necesitan apps de terceros que solo estén disponibles en el sitio web del desarrollador, la segunda opción permite obtener apps tanto de la App Store como de desarrolladores identificados que hayan sido examinadas por Apple y creen paquetes de software firmados con su respectivo ID de desarrollador para mayor seguridad.

Prácticas recomendadas

Para macOS, configure permitiendo la selección de la App Store de Mac y desarrolladores identificados, especialmente si crea sus propias aplicaciones o reempaqueta apps para implementarlas. Además, solicite un ID de desarrollador a Apple y firme las aplicaciones desarrolladas internamente por la organización para que Gatekeeper confíe en ellas. Por último, al utilizar Jamf Pro como solución de MDM, el catálogo de apps de autoservicio puede desplegarse en todos los dispositivos, con lo que IT aprueba previamente apps, ajustes, configuraciones y mucho más para los usuarios finales, permitiéndoles acceder e instalar las herramientas y servicios que necesiten, cuando los necesiten, sin necesidad de un ticket del servicio de asistencia, modificación de permisos o un ID de Apple.

Configuración manual de las opciones de Gatekeeper:

- Vaya a: Ajustes del sistema > Privacidad y seguridad > Seguridad.
- Seleccione una de las dos opciones disponibles
- Repita el proceso para todos los dispositivos de su organización.

Configuración de las opciones de Gatekeeper con Jamf Pro:

- Configure e implemente un perfil de configuración con sus ajustes de Gatekeeper en todos sus dispositivos.
- **¡Así de fácil!**

Aplicación y seguridad de parches y actualizaciones

Actualizaciones de OS, control de versiones con comandos MDM, respuesta rápida en materia de seguridad y mucho más

Las organizaciones deben implementar una estrategia de administración de parches para probar e incorporar correcciones de errores lo antes posible, con el fin de mantener protegidos su hardware, sus datos y sus usuarios. Las pruebas son una necesidad que a menudo se pasa por alto a la hora de implementar parches, sobre todo cuando los bugs se presentan en forma de vulnerabilidades de seguridad que hay que solucionar lo antes posible. Al realizar ambas tareas lo antes posible, IT reduce al mínimo el impacto de las amenazas a la seguridad que se propagan, al tiempo que introducen problemas mayores, derivados de parches que arreglan una cosa pero sin querer rompen otras funcionalidades más críticas.

A lo largo de este ebook, la tendencia de cuánto tardarán en efectuarse las tareas de administración realizadas por IT está directamente correlacionada con el número de dispositivos gestionados. A la hora de aplicar parches, esta regla sigue siendo la misma salvo por una variable: el número de parches que hay que implementar puede ir de pocos a muchos, lo que aumenta exponencialmente las tareas administrativas en una cantidad desconocida por dispositivo.

Repasemos algunas de las opciones disponibles para los administradores que aplican los parches manualmente y a través de la MDM:

Opciones para la administración de parches de forma manual:

- Educar a los usuarios para que realicen ellos mismos las actualizaciones en cuanto reciban notificaciones de actualización en sus dispositivos.
- Recopilar todos los dispositivos cuando se publica un nuevo parche e implementarlos manualmente.
- Remediar los dispositivos que carecen de parches como parte de sus procesos continuos de monitoreo del cumplimiento.

Opciones para la aplicación de parches a través de la MDM (es decir, Jamf Pro):

- Jamf recibe automáticamente actualizaciones y notificaciones de parches, junto con las herramientas para implementar los parches en todos los dispositivos de su organización, para que pueda actualizar según su cronograma, no el de otros.
- El catálogo de apps de Self Service de Jamf facilita facultar a usuarios para que actualicen en cualquier momento un nuevo parche disponible, notificando a los usuarios que deben actualizarlo antes de seguir utilizando una app afectada.
- Elimina la dependencia de los usuarios finales al tiempo que alivia la carga de IT automatizando la distribución de parches. Envíe los parches en forma de políticas a todos los dispositivos, o selecciónelos con grupos inteligentes dinámicos para garantizar que los dispositivos estén actualizados.

Para obtener más información sobre el ciclo de vida de las aplicaciones y la automatización e implementación de apps, consulte nuestro documento de investigación.

Aumente su nivel de seguridad

Por si aún no lo ha adivinado, la seguridad no es una solución que se ajuste a todos los contextos. Hay capas para una estrategia integral que protegerá de manera holística sus dispositivos, usuarios y datos, al tiempo que proporciona protecciones granulares que se entrelazan para formar una red de seguridad digital. Esto se conoce como defensa en profundidad, lo que significa que si una capa no detecta una amenaza, la siguiente por encima o por debajo estará ahí para contenerla.

Es probable que ya esté familiarizado con el enfoque de seguridad por capas y que ni siquiera lo conozca. Utilicemos como ejemplo algo con lo que está muy familiarizado: su casa.

Con la mezcla de protecciones heredadas y las nuevas disponibles para la seguridad en el hogar, no cabe duda de que tiene algunas (o quizá todas) para proteger a sus seres queridos y a usted mismo en casa:

- Cerraduras con pestillo en las puertas
- Sistema de alarma doméstico
- Vigilancia por videocámara
- Guardias de seguridad que patrullan los alrededores
- Detectores de humo y monóxido de carbono
- Extintor de incendios
- Seguro de hogar o de alquiler

En teoría, cada una de las soluciones anteriores puede funcionar como una solución independiente para proporcionar seguridad en el hogar. Pero, por sí sola, solo aporta una pieza de la seguridad global necesaria, ¿no? Sin embargo, cuando se combinan, las múltiples piezas encajan como un rompecabezas para ilustrar la imagen completa y abordar exhaustivamente toda la gama de problemas. La ciberseguridad y la administración y seguridad de su flota de dispositivos Apple se basan en principios similares, que constituyen el quid del asunto a la hora de facultar e informar a usuarios para que tengan y sigan buenas prácticas de seguridad para minimizar riesgos y mitigar amenazas.

Uno de estos niveles de seguridad de endpoints es recibir alertas sobre los riesgos que corren los dispositivos. Por ejemplo, algunos usuarios pueden ser capaces de detectar un ataque de phishing y, por lo tanto, no hagan clic en un enlace malicioso todavía; otros usuarios pueden ser demasiado confiados y llevar a cabo las instrucciones del enlace malicioso, introduciendo así un riesgo potencial para el dispositivo, el usuario y los datos. ¿Cómo sabría este usuario afectado que ha hecho clic en un enlace malicioso o que ha realizado una acción que ha puesto en peligro su dispositivo o sus credenciales?

¡Hay una app para eso! Jamf Trust protege contra los riesgos iniciados por el usuario, como el ejemplo de ataque de phishing anterior, notificando a los usuarios en forma de notificaciones push de Apple cuando Jamf detecta una amenaza en su dispositivo, como si ese enlace malicioso al que se hizo clic anteriormente introdujera código malicioso en forma de malware que actualmente registrara la pulsación de las teclas en el dispositivo.

La solución ha determinado que existe una amenaza y ha informado al usuario (y también al administrador). Ayudar al usuario a ser consciente del peligro y a estar atento a los que vengan en el futuro, mientras el departamento de IT puede responder al incidente y remediarlo rápidamente, utilizando una combinación de Jamf Pro y Jamf Protect para poner en cuarentena el dispositivo de la red, limpiar la infección, parchar cualquier vulnerabilidad presente y restaurar el dispositivo a su estado inicial. Por último, aproveche las lecciones aprendidas para la futura capacitación de los interesados en materia de seguridad.

La seguridad de dispositivos y datos no es un asunto de risa.

Las organizaciones tienen la opción de adelantarse a muchos posibles ataques o robos de datos implementando las protecciones de seguridad más sólidas posibles a través de Apple, y Jamf puede hacer que esto sea más fácil, rápido y mucho más seguro y eficaz que los protocolos de seguridad manuales.

Cuando se trata de ciberseguridad, a nadie le gustan las sorpresas y, desde luego, no quiere encontrarse en un aprieto en respuesta a un ataque si puede evitarlo. Obtenga las mejores opciones de seguridad para su organización probando de forma gratuita las soluciones de productos Jamf, o póngase en contacto con un representante de Jamf hoy mismo para hablar de la apariencia de una solución de administración y seguridad de Apple personalizada y completa para las necesidades exclusivas de su organización.

Ya ha probado el resto... ¡ahora vaya con lo mejor!

Pruebe Jamf

O comuníquese con su distribuidor preferido de dispositivos Apple para obtener una prueba gratuita.

© 2023 Jamf, LLC. Todos los derechos reservados.