jamf

Mac e iOS sin concesiones

en empresas con predominio de PC

Introducción

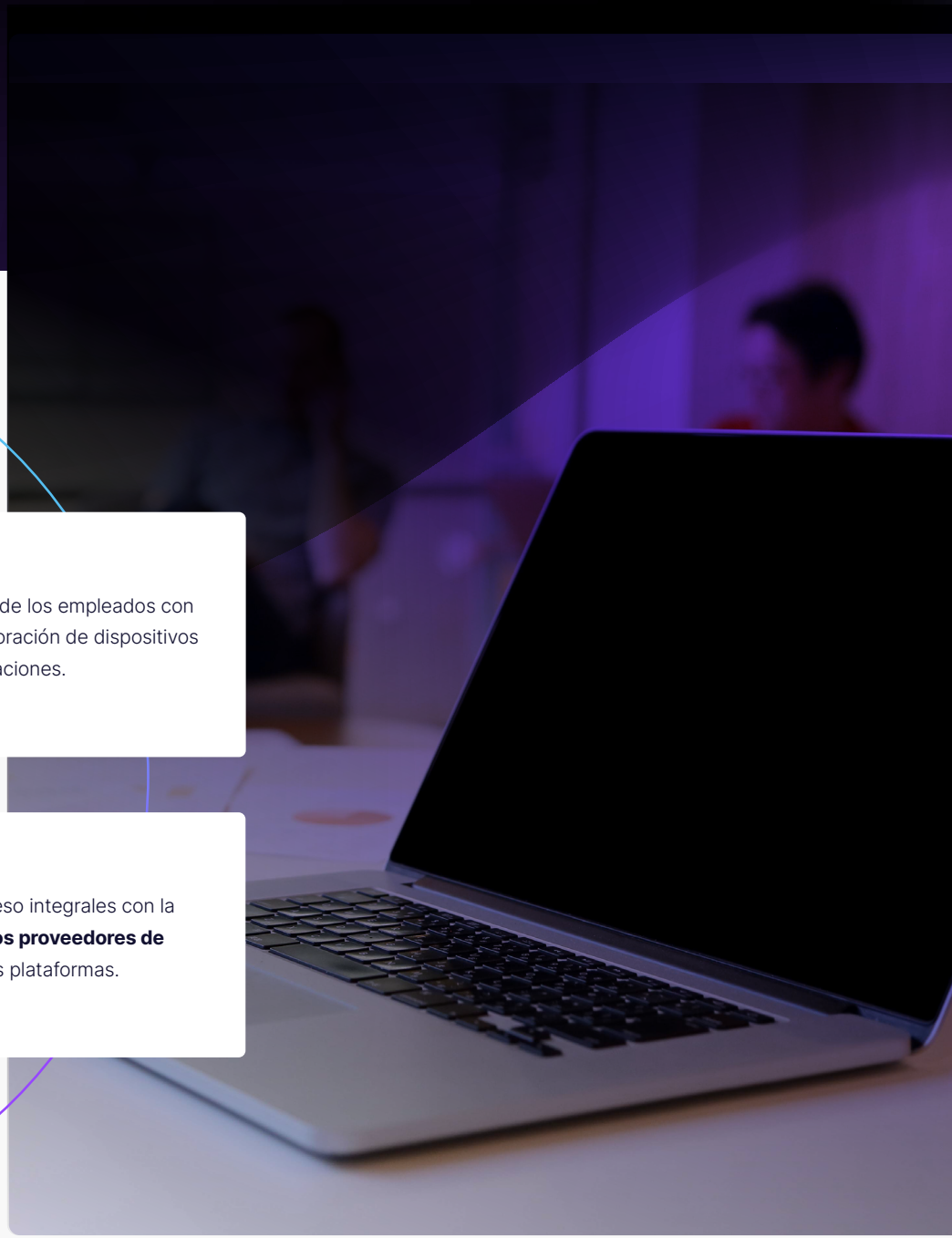
Cuando los dispositivos Apple se incorporan a empresas que suelen operar con Windows, es la eficiencia —y no el personal adicional— lo que determina si el departamento de TI sigue funcionando sin problemas o se ve abrumado por el trabajo extra.

Esta guía constituye la primera parte de la serie *"Por qué Jamf"* y proporciona a los ejecutivos y administradores de TI de todos los niveles la información necesaria para garantizar que las inversiones existentes en identidad, seguridad, automatización y observabilidad ofrezcan resultados conformes con la normativa, mientras se reduce el trabajo manual. En última instancia, se trata establecer una experiencia Apple coherente sin añadir gastos operativos adicionales.

Resumen ejecutivo

A medida que crece la adopción de Apple en las empresas enfocadas en Windows, la eficiencia operativa determina el éxito. Este libro digital describe cómo las organizaciones pueden realizar la integración de Apple sin aumentar el personal, el costo de propiedad o la complejidad, abordando los principales puntos débiles que afectan los procesos y flujos de trabajo. El resultado es una implementación más rápida, una mayor visibilidad y una experiencia Apple coherente y segura que se adapta al crecimiento de la empresa.

Problemas de integración que resuelve Jamf



Elimina la fragmentación de datos y las ineficiencias en los flujos de trabajo mediante **la integración de la identidad**, **la seguridad** y **las soluciones de TI existentes** para lograr una estrategia holística.

Automatiza todo el ciclo de vida de los dispositivos Apple mediante **integraciones en el ecosistema**, desde la adquisición hasta la aplicación de parches y el desmantelamiento seguro.

Acelera la **respuesta ante incidentes** mediante la evaluación constante de datos de telemetría detallados para estandarizar y mantener las posturas básicas.

Optimiza la productividad de los empleados con flujos de trabajo de incorporación de dispositivos sin contacto y sin complicaciones.

Unifica las políticas de acceso integrales con la arquitectura **Zero Trust** y **los proveedores de identidad** (IdP) en todas las plataformas.

Integración profunda con su pila tecnológica existente

La falta de conectividad entre la administración de dispositivos y las herramientas de seguridad e identidad existentes provoca fragmentación de datos, ineficiencias en los flujos de trabajo y deficiencias en la conformidad

Un mito común en torno a los dispositivos Apple y las redes tradicionales basadas en Windows es que las dos plataformas no son compatibles. Aunque esta creencia se remonta a varias décadas atrás, la realidad de la tecnología moderna en la empresa es que la compatibilidad entre plataformas no solo es necesaria para la continuidad de los negocios globales, sino que es algo que se da por hecho. Esto es especialmente importante, ya que las organizaciones dependen cada vez más de la arquitectura, las aplicaciones y los servicios basados en la nube para generar valor y mantener la productividad de los empleados que utilizan diferentes tipos de dispositivos, múltiples plataformas y versiones, en tanto garantizan la paridad integral entre las fuerzas de trabajo distribuidas.

Junto con la compatibilidad entre plataformas, la integración profunda desempeña un papel fundamental en lo que respecta a la compatibilidad entre su infraestructura tecnológica existente y los dispositivos Apple que se integran a gran escala.

¿Qué es lo que hace Jamf para que la integración de Apple sea un proceso sencillo para las empresas?

Un solo concepto: **Interfaz de Programación de Aplicaciones de la Plataforma** (API de plataforma).

La clave para tener una comunicación fluida entre las terminales de Apple y la infraestructura tecnológica que usted posea reside en enlaces seguros y basados en estándares entre soluciones que se vinculan con los flujos de trabajo de administración, identidad y seguridad.

¿Qué significa esto para la conformidad de las empresas ante el panorama actual de amenazas? Soluciones más sencillas y menor complejidad.

Al integrar Apple a la perfección con su infraestructura tecnológica actual, se habilitan las siguientes funciones multiplataforma:

La automatización impulsa flujos de trabajo consistentes, garantizando la paridad

La **seguridad enfocada en la identidad** ofrece protección unificada contra amenazas

Se mantiene la conformidad utilizando **las soluciones que ya posee**

Se optimizan los tiempos de respuesta al reducir la fragmentación de los equipos de TI

¿Por qué elegir Jamf?

Jamf Marketplace ofrece más de 300 integraciones preconfiguradas (y siguen creciendo) para eliminar la complejidad de adoptar Apple en su empresa actual.

Reduzca el tiempo de inactividad de los empleados con implementaciones de dispositivos optimizadas

Cada hora que un empleado espera por un dispositivo aprovisionado es una hora de productividad perdida y, en entornos de PC, esa espera es de un promedio de 2 a 4 horas por máquina.

Al integrar dispositivos Apple en un entorno predominantemente de PC, la tarea más crítica del proyecto, justo después de la planificación, es la fase de implementación. Durante esta fase, los empleados suelen esperar mientras el departamento de TI les proporciona sus dispositivos nuevos o actualizados. Dependiendo de los ajustes que se apliquen, el número de aplicaciones y las configuraciones específicas necesarias para que los empleados puedan realizar su trabajo, el tiempo que transcurre entre el momento en que los empleados reciben sus dispositivos y el momento en que estos están listos para su uso representa una interrupción de la productividad.

¿Y si le dijera que estos retrasos podrían reducirse a unos 15 minutos por computadora Apple (y a solo 5-7 minutos por cada iPad y iPhone)?

El secreto de esta velocidad de implementación es el aprovisionamiento sin intervención. Al conectar Apple Business Manager (ABM) a una solución de administración de Apple diseñada específicamente para este fin, el departamento de TI accede a un marco de automatización que los entornos Windows simplemente no pueden igualar. Piense en ABM como el equivalente de Apple a Windows Autopilot, pero con una integración de hardware más profunda, ya que Apple controla tanto el chip (Silicon) como el servicio de inscripción. El departamento de TI integra ABM con Jamf y define cómo debe ser la preparación de los dispositivos dentro de la consola de administración: aplicaciones, configuraciones, políticas de seguridad y ajustes de identidad. A partir de ahí, a medida que se adquieren los dispositivos de Apple, ABM sincroniza la información de cada dispositivo con Jamf y los añade a un grupo de preinscripción.

Desde aquí, el trabajo de TI está prácticamente terminado.

Los dispositivos propiedad de la empresa se envían al usuario —a la oficina o a su domicilio— donde los desempacan, los encienden y... ¡listo! El dispositivo se inscribe automáticamente en Jamf y se ejecuta el flujo de trabajo de prerregistro, lo que permite aprovisionar el dispositivo sin ningún problema. Gracias a la naturaleza automatizada de la tecnología sin intervención, el usuario final no necesita realizar ninguna función ni enviar tíckets al servicio de asistencia técnica.

¿Por qué elegir Jamf?

Con los proyectos Jamf, los dispositivos aplican políticas de forma autónoma mediante la Administración Declarativa de Dispositivos, lo que reduce la configuración a unos 15 minutos para Mac y a menos de 7 minutos para dispositivos móviles. La Certificación de Dispositivos Administrados añade una prueba de conformidad basada en el hardware, de modo que el departamento de TI sabe que todos los dispositivos son auténticos antes de que accedan a los recursos corporativos.

Apple integra la certificación, la identidad y la administración en un marco unificado: desde el chip de silicio hasta el software.

La **Administración Declarativa de Dispositivos (DDM)** permite a los dispositivos aplicar configuraciones de forma asíncrona e informar del estado al servicio de la administración de dispositivos sin necesidad de realizar sondeos constantes a soporte técnico de Apple. Esto significa que los dispositivos se configuran más rápido y siguen cumpliendo con las normas incluso sin conectividad a Internet.

La **certificación de dispositivos administrados** proporciona pruebas sólidas sobre las propiedades de los dispositivos como parte de una evaluación de confianza, utilizando declaraciones criptográficas basadas en Secure Enclave y los servidores de certificación de Apple para demostrar que el dispositivo es auténtico antes de que acceda a los recursos corporativos.

La **plataforma SSO** permite a los usuarios prescindir de contraseñas gracias a Touch ID, con credenciales resistentes al phishing basadas en claves vinculadas al hardware en el Secure Enclave, de modo que los empleados realizan la autenticación una sola vez al iniciar sesión para obtener un acceso fluido a las aplicaciones corporativas sin tener que manejar contraseñas.

Automatice las tareas y los procesos de TI a escala empresarial

Según Forrester, el costo típico de restablecer una sola contraseña es de 70 dólares; **la empresa promedio destina más de un millón de dólares al año** a sufragar los costos manuales relacionados con las contraseñas.

La automatización es un concepto amplio, que actúa como un gran saco capaz de contener prácticamente todo lo que se le introduzca en él. Es fundamental comprender la relación entre la automatización y el tiempo. No solo cómo automatizar tareas ahorra tiempo al departamento de TI, sino también el tiempo que le lleva al departamento de TI aprender una habilidad hasta alcanzar el nivel necesario para desarrollar la automatización.

Con esa analogía en mente, el gran volumen de dispositivos, tecnologías y soluciones que operan a nivel empresarial realmente hace que el tiempo sea un recurso sumamente valioso para los equipos de TI. La recompensa de automatizar va más allá de la eficiencia, ya que libera al departamento de TI para que se enfoque en tareas estratégicas en lugar de apagar incendios. Permite:

Ejecución constante

Las políticas se aplican de manera uniforme en Mac, iPhone e iPad, sin que ningún dispositivo quede fuera.

Reducción de errores humanos

Los flujos de trabajo estandarizados eliminan los riesgos que introducen los flujos de trabajo manuales.

Escalabilidad sin aumento de personal

Satisface las crecientes exigencias de administración y seguridad a medida que la empresa se expande.

El marco de automatización adecuado se encarga de las tareas repetitivas: implementación de dispositivos, aplicación de políticas, instalación de parches de software y restablecimiento de contraseñas. Pero Apple va más allá. Con la Administración Declarativa de Dispositivos, estos no esperan las instrucciones del servidor, sino que aplican las políticas de forma autónoma e informan de los cambios de estado en tiempo real. Esto se traduce en menos solicitudes de asistencia, una conformidad más rápida y menos intervención manual a medida que crece su flota de dispositivos Apple.

¿Por qué elegir Jamf?

Los flujos de trabajo de automatización inteligente de Jamf eliminan las configuraciones manuales mediante una administración basada en políticas, grupos inteligentes y procesos impulsados por API que están diseñados para garantizar una implementación coherente y sin errores, así como un control de la conformidad a gran escala.

Fortalezca las políticas de acceso mediante la implementación de Zero Trust

El panorama actual de amenazas está en constante evolución. Los delincuentes aprovechan tecnologías avanzadas como la inteligencia artificial para aumentar la sofisticación de las amenazas, maximizar su capacidad de daño y ocultar su rastreo mediante medidas de camuflaje.

No se equivoque, los actores de amenazas atacan todas las plataformas —ningún sistema operativo es invulnerable— por lo que mantener las terminales actualizadas y garantizar la implementación de una estrategia de defensa en profundidad es la piedra angular de la administración moderna de dispositivos. La clave es tratar cada dispositivo, cada usuario y cada solicitud como no confiables hasta que se demuestre lo contrario. Zero Trust no es un producto, es un marco de trabajo.
Y la arquitectura de Apple está diseñada para ello.

La Certificación de Dispositivos Administrados comprueba criptográficamente que un dispositivo sea auténtico antes de que acceda a los recursos corporativos. El SSO de la plataforma vincula la identidad del usuario a claves vinculadas al hardware en el Secure Enclave, lo que dificulta considerablemente el robo de credenciales. La Administración Declarativa de Dispositivos garantiza que dichos dispositivos apliquen las políticas de seguridad de forma autónoma, incluso cuando están desconectados. Juntos, crean una base en la que se verifica la confianza de forma continua, en lugar de darse por sentada.

Las empresas ganan agilidad y aceleran la respuesta ante incidentes **al unificar la administración, la identidad y la seguridad en toda su flota de dispositivos de las siguientes formas clave:**

¿Por qué elegir Jamf?

La IA generativa está potenciando la ingeniería social: ahora son mucho más difíciles de detectar los mensajes de phishing, los medios sintéticos y el malware generado por IA.

Secure Enclave y Managed Device Attestation de Apple verifican la identidad del dispositivo a nivel de hardware, mientras que Jamf aplica controles de red de confianza cero con políticas de acceso basadas en el riesgo, verificación de la conformidad de los dispositivos e integración de acceso condicional que protege los datos confidenciales en la terminal.

Implementar el acceso a la red de confianza cero (ZTNA)

- Aplique políticas de acceso sensibles al contexto que validen la postura del dispositivo y el estado de las credenciales en cada solicitud.
- Aísle las sesiones mediante microtúneles para reducir los ataques habituales tanto en los dispositivos como en la red.
- Amplíe la protección a macOS, iOS, iPadOS, Android y Windows.

Aplique conformidad de líneas de base y de indicadores

- **Realice automáticamente la implementación de configuraciones de seguridad básicas** alineadas con las normativas o los requisitos de conformidad personalizados.
- **Audite el estado de seguridad en todos los dispositivos** y en la empresa mediante el uso de comparativas para validar la conformidad.
- **Utilice la IA/ML para la búsqueda de amenazas, la respuesta a incidentes y el soporte informático**
- Detecte de forma proactiva las amenazas conocidas y mejore al mismo tiempo la capacidad de **identificar y detener las amenazas** desconocidas de forma temprana.
- **Reduzca los tiempos de respuesta y acelere la solución de errores** mientras cierra las brechas de seguridad.
- Utilice **Jamf AI Assistant** para ayudar a los equipos a explorar tecnologías, validar recomendaciones de configuración y desarrollar soluciones más rápidas.

Obtenga visibilidad y mejore las respuestas a lo largo de todo el ciclo de vida de un dispositivo

La mayoría de las conversaciones sobre seguridad se enfocan en las amenazas activas. Pero algunos de los mayores riesgos —y costos— se esconden en las deficiencias: inventarios obsoletos, licencias de software sin usar y dispositivos que se dan de baja de la organización sin un borrado adecuado de datos.

Los equipos de TI y seguridad suelen concentrarse tanto en los problemas relacionados con los actores maliciosos, que la visibilidad de otros aspectos de un dispositivo pasa a un segundo plano.

La visibilidad no consiste solo en saber qué hay en su red. Se trata de saber qué está instalado, qué tiene licencia, qué cumple con las normas y qué está listo para darse de baja. Los datos contextuales de las terminales, como los inventarios actualizados de dispositivos o la proliferación de software, ofrecen una visión completa del estado de dichas terminales a lo largo de su ciclo de vida. Con la Administración Declarativa de Dispositivos, los dispositivos Apple informan de los cambios de estado de forma proactiva (versión del sistema operativo, estado de seguridad, aplicaciones instaladas) sin esperar a que el departamento de TI los consulte. Esto significa que el inventario se mantiene actualizado, no obsoleto.

A continuación, desglosamos cómo la falta de visibilidad afecta a las organizaciones:

Licencias de software no usadas

La falta de un seguimiento preciso de las licencias de software se traduce en un 50 % de licencias sin utilizar, lo que representa un gasto innecesario de aproximadamente **$45 millones de dólares** al mes.

Problemas al dar de baja equipos

Entre el 10 % y el 20 % de las violaciones de datos de los últimos años están relacionadas con los residuos electrónicos (e-waste) y con los dispositivos que no se dan de baja de forma adecuada. Representan un punto ciego para las empresas en comparación con las terminales que se utilizan actualmente

Brechas de conformidad

Las organizaciones que renuevan y redistribuyen dispositivos son susceptibles de que los datos caigan en manos equivocadas (como las amenazas internas) desde dispositivos que no se administran correctamente. Por ejemplo, en el caso de que la laptop anterior de un ejecutivo de recursos humanos se entregue a un nuevo empleado de ventas. La Información de Identificación Personal (PII) contenida en ese dispositivo podría seguir existiendo y ser visible para el nuevo usuario y —dependiendo de las normativas que rijan su industria— esto podría constituir una violación de las leyes de privacidad, como el RGPD.

El enfoque de Apple en materia de administración facilita esta tarea. Los dispositivos se autoinforman, mientras que las políticas se aplican por sí mismas. Y cuando llega el momento de borrarla y volver a implementarla, la integración entre Apple Business Manager y su solución de administración de dispositivos garantiza que el dispositivo se vuelva a inscribir automáticamente, sin intervención manual y sin brechas de seguridad.

¿Por qué elegir Jamf?

Jamf permite que el departamento de TI verifique que las Mac con Apple Silicon funcionen en modo de seguridad total antes de darlas de baja, lo que garantiza que los datos cifrados con FileVault permanezcan protegidos incluso si se pierde un dispositivo o se da de baja de forma inadecuada. Dado que entre el 10 % y el 20 % de las violaciones de datos están relacionadas con los residuos electrónicos, la visibilidad respaldada por hardware del estado de Secure Boot cierra una brecha que la mayoría de las organizaciones no ven hasta que es demasiado tarde.

Flujos de trabajo industriales que ofrecen resultados

La verdadera medida de la administración de dispositivos no es la infraestructura interna (back-end) de TI; es si los empleados y clientes notan una mejora en la forma en que realizan su trabajo. Estos ejemplos reales muestran cómo los dispositivos pueden aumentar la eficiencia de los flujos de trabajo:

Atención médica

Cuando el estado del historial médico de un paciente pasa a "dado de alta", un iPad situado junto a la cama borra automáticamente todos los datos del paciente y se prepara para el siguiente paciente, sin que ningún miembro del personal tenga que tocar el dispositivo. Los médicos comparten iPhones entre turnos, con apps personalizadas activadas en función de sus funciones y credenciales.

Aviación

Los pilotos sustituyen las pesadas listas de verificación, cartas y manuales por una única bolsa de vuelo electrónica alojada en un iPad. Los mecánicos, los agentes de puerta y los auxiliares de vuelo obtienen automáticamente las aplicaciones adecuadas, independientemente del dispositivo que utilicen.

Minoristas

Los iPad bloqueados en modo de aplicación única sirven como quioscos de autoservicio. Esto significa que no hay que solucionar problemas, no hay contenido inapropiado y no es necesario restablecer nada al final del día. Los asociados se desplazan sin problemas entre el punto de venta, el inventario y la información de los clientes en dispositivos compartidos configurados en función de quién inicia sesión.

Fabricación

Los trabajadores de la planta de producción a menudo no tienen credenciales de red ni experiencia con tecnología móvil. Los casilleros de carga seguros ofrecen soporte de nivel cero. Si un iPad no funciona, los empleados lo vuelven a conectar y el dispositivo se reinicia automáticamente y completa la configuración mientras se repara por sí solo. Simplemente, toman otro iPad y vuelven al trabajo, sin necesidad de enviar un tícket al departamento de TI ni de recibir asistencia técnica.

Servicios financieros

Los ajustadores de siniestros, los agentes de crédito y los asesores de campo necesitan acceso instantáneo a datos confidenciales en dispositivos compartidos, a menudo en ubicaciones impredecibles con estrictos requisitos de conformidad. Un ajustador saca un iPad de un inventario compartido, introduce sus credenciales una vez y accede inmediatamente a las apps de reclamaciones, herramientas fotográficas y registros de clientes. Cuando terminan, retiran sus credenciales en cuestión de segundos y el dispositivo queda listo para el siguiente usuario, con un registro de auditoría completo para garantizar la conformidad.

Conclusión

La integración de Apple en empresas centradas en Windows no requiere una transformación a gran escala ni representa una carga operativa adicional. En su lugar, requiere un cambio hacia flujos de trabajo eficientes, automatizados y estandarizados. Al unificar la administración del ciclo de vida de los dispositivos, la identidad y la seguridad en una base nativa de Apple que ofrece integración con las herramientas existentes, los equipos de TI avanzan gradualmente en la madurez operativa. Este enfoque reduce el esfuerzo manual, mejora la coherencia y permite operaciones proactivas, lo que permite a las organizaciones modernizarse a su propio ritmo mientras mantienen la disponibilidad multiplataforma, la conformidad normativa y el control de su flota de dispositivos de escritorio y móviles.

Puntos clave

- La integración de Apple es un reto de eficiencia, no un problema de personal.
- La implementación sin intervención reduce las horas de configuración a minutos, lo que disminuye el tiempo de inactividad.
- La administración, la identidad y la seguridad unificadas eliminan la fragmentación operativa.
- La automatización estandariza la aplicación y reduce los errores humanos a gran escala.
- El acceso a la red de confianza cero (Zero Trust Network Access) refuerza la seguridad sin añadir complejidad.
- La visibilidad del ciclo de vida protege el tiempo de actividad, la conformidad y el gasto en software.
- La Administración Declarativa de Dispositivos mantiene los dispositivos en conformidad, incluso sin conexión.

¿Listo para verlo en acción?

Prueba Jamf hoy mismo