jamf

Proporcionamos excepcionales experiencias al usuario final a dispositivos Apple en empresas donde predominan las PC

Introducción

La experiencia es sinónimo de productividad.

Al ampliar el enfoque de Apple en la experiencia del usuario a los procesos de TI, las empresas reducen las fricciones, lo que les permite maximizar tanto la productividad como el retorno de la inversión (ROI).

Esta guía constituye la segunda parte de la serie "¿Por qué Jamf?" y ofrece 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 permitan a los empleados mantener su productividad, mientras superan los retos y reducen los obstáculos habituales.

Resumen ejecutivo

La productividad disminuye cuando la configuración de dispositivos, la administración de accesos, las actualizaciones de software y la defensa contra amenazas dependen de procesos manuales. Esta guía explica cómo la integración de la administración de dispositivos, la identidad y la seguridad agiliza las operaciones de TI, al mismo tiempo que mejora la experiencia del usuario. Gracias a la implementación sin intervención, los controles de acceso basados en roles y la administración automatizada del ciclo de vida de las apps, Jamf agiliza la incorporación de nuevos usuarios y garantiza la seguridad y el cumplimiento normativo de los dispositivos. Self Service+ permite a los empleados instalar apps autorizadas y resolver necesidades comunes en cualquier momento, lo que reduce el número de tíckets de soporte técnico sin dejar de garantizar el cumplimiento de las políticas. El resultado es un flujo de trabajo escalable que refuerza la seguridad, simplifica la administración y permite a los empleados mantener su productividad desde el primer día.

Problemas de productividad que resuelve Jamf

Realiza la incorporación de los empleados sin complicaciones con dispositivos que están "listos para trabajar" justo al sacarlos de la caja.

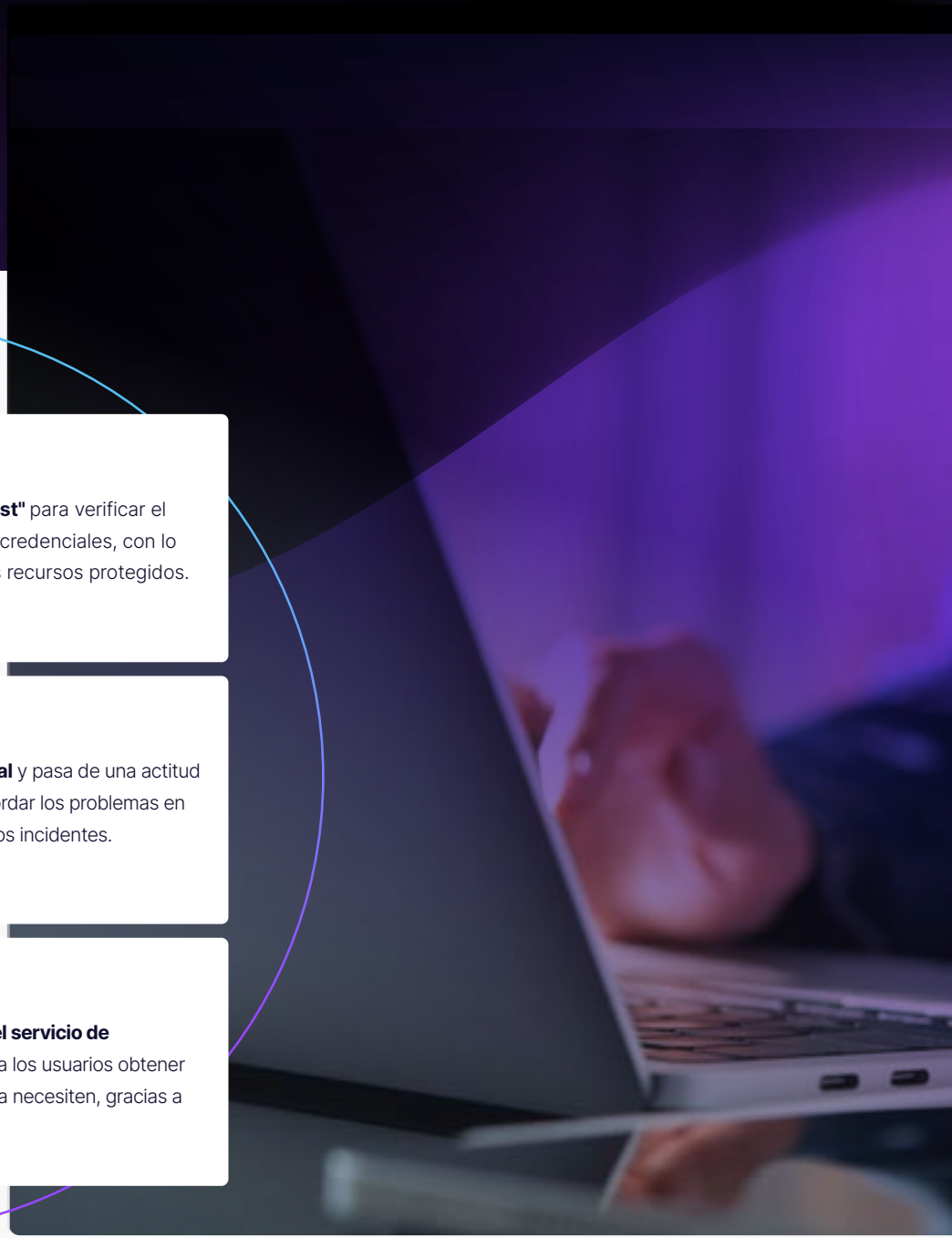
Implementa el modelo **"zero trust"** para verificar el estado de los dispositivos y las credenciales, con lo que se reduce el riesgo para los recursos protegidos.

Proporciona configuraciones básicas seguras junto con optimizaciones específicas para cada rol desde el primer inicio de sesión.

Obtiene **visibilidad en tiempo real** y pasa de una actitud reactiva a una proactiva para abordar los problemas en lugar de limitarse a responder a los incidentes.

Mantiene el **software actualizado** automáticamente: minimiza el tiempo de inactividad y maximiza la conformidad.

Reduce los gastos generales del servicio de asistencia técnica, permitiendo a los usuarios obtener la ayuda que necesiten, cuando la necesiten, gracias a Self-Service.



Incorporación fluida, productividad desde el primer día

En el ámbito de las tecnologías de la información, un proceso de aprovisionamiento manual típico suele ser algo como esto:

1. **Adquirir el hardware**
2. **Desempacar cada dispositivo.**
3. **Colocarlo en el centro de la escena.**
4. **Recorrer las pantallas de configuración inicial.**
5. **Instalar:**
   - Actualizaciones del sistema operativo
   - Aplicaciones
   - Seguridad de terminales
6. **Configurar:**
   - Ajustes de hardware
   - Ajustes de software
   - Puntos de referencia seguros
7. **Comprobar que las terminales se monitorean.**
8. **Asignar al usuario final.**
9. **Verificar que el usuario final pueda realizar la autenticación.**
10. **Comprobar que el usuario final tenga acceso a las herramientas necesarias.**

En teoría, 10 pasos tal vez podrían parecer mucho trabajo para preparar un dispositivo para un nuevo empleado. Sin embargo, en la práctica, las empresas que administran más de 1,000 dispositivos se mostrarán comprensiblemente reacias ante la perspectiva de tener que procesar manualmente incluso solo 10 dispositivos de esta manera, debido al impacto que ello tendría en el tiempo, la productividad y el presupuesto.

Dependiendo de sus necesidades específicas, solo los pasos 5 y 6 pueden tardar varias horas en completarse por dispositivo. Esto significa que algo tan sencillo como aplicar parches al sistema operativo y al software, instalar una suite de productividad y configurar los ajustes del software para cumplir con la conformidad puede ocupar fácilmente medio día de trabajo, entre las interrupciones para reiniciar el sistema y el tiempo dedicado a esperar a que los procesos se completen con éxito.

¿Cuál es la solución para mitigar el impacto sobre los recursos?

Una estrategia de incorporación que integre la administración, la identidad y la seguridad como pilar fundamental para automatizar el aprovisionamiento en función del rol del usuario final mediante una implementación sin intervención. Esto no solo reduce el tiempo que los nuevos empleados pasan esperando a que el equipo esté "listo para trabajar" de horas a minutos, sino que también acorta considerablemente el plazo en el que pueden empezar a ser productivos.

Esto significa:

- **Que no haya retrasos en la incorporación** por tener que esperar a que el departamento de TI brinde asistencia.
- Los empleados no están obligados a recoger su dispositivo en una oficina.
- Se eliminan los errores humanos y la fatiga por tareas repetitivas.
- Los empleados son productivos y contribuyen activamente desde su primer día.
- Los flujos de trabajo eficientes ahorran tiempo y dinero a las empresas, en lugar de desperdiciarlos.

¿Por qué Jamf?

Jamf cuenta con un flujo de trabajo flexible y potente que reduce el tiempo que TI tarda en resolver los tíckets de soporte relacionados con la incorporación de nuevos usuarios. Al trasladar las tareas habituales de configuración a un modelo de implementación automatizado, el departamento de TI crea flujos de trabajo más eficaces y que ofrecen mayor apoyo a los usuarios finales, para que puedan inscribir sus propios dispositivos y acceder al software, las herramientas y las configuraciones que necesiten, cuando las necesiten, de forma segura, a través de Self Service.

Políticas de acceso que protegen los datos sin ralentizar el trabajo de los usuarios

Un pilar fundamental de la seguridad de los datos son las listas de control de acceso (ACL), es decir, los permisos que se han concedido (o no) a una cuenta de usuario para acceder a un recurso protegido. Aunque suele tenerse en cuenta el número de dispositivos a la hora de determinar la proporción de personal de soporte de TI, cuando hablamos de identidad, el debate se enfoca en el número de usuarios a los que presta soporte el departamento de TI para diseñar las estrategias de seguridad de datos.

El factor más importante a tener en cuenta al realizar una configuración manual es el número de permisos necesarios multiplicado por el número total de usuarios finales. A medida que aumenta el personal, también aumenta el número de permisos que el departamento de TI debe manejar manualmente. Esto representa un duro golpe para el rendimiento, lo que provoca considerables retrasos y aumenta la probabilidad de que surjan riesgos derivados de errores humanos y de la fatiga por la repetitividad de los procesos. Además, dado que realizar el proceso manual de los cambios a medida que se detectan depende de los equipos de TI, cualquier factor que dé lugar a una modificación —como el ascenso de un empleado o un cambio en la tolerancia al riesgo— requiere ajustes en cada cuenta y, a menudo, en cada dispositivo, lo que hace que este método sea notoriamente difícil de escalar.

¿Cuál es la solución óptima y escalable?

La integración de la administración de identidades y accesos (IAM) con la administración de dispositivos y la seguridad de terminales ofrece la mayor flexibilidad para adaptarse a las necesidades de las empresas. Además, reduce el trabajo manual que implican los cambios por cuenta o por dispositivo al adoptar un modelo de seguridad centralizado, utilizando el control de acceso basado en roles (RBAC) para definir el acceso de los usuarios a los recursos protegidos en función de su rol, en lugar de su identidad individual o del dispositivo en particular que utilicen para trabajar.

Esto significa:

- **La asignación de permisos** se ha simplificado y se basa en los roles y la pertenencia a grupos de un repositorio central.
- Se aplica el principio del privilegio mínimo, **lo que limita el acceso** únicamente a lo necesario, nada más.
- Los derechos de acceso se aplican durante **la autenticación del usuario**, se mantienen en cualquier dispositivo y durante los cambios de rol.
- **Menor carga administrativa**, incluso a mayor escala, ya que el departamento de TI solo tiene que procesar el cambio una vez.
- La auditoría de los controles se **simplifica**, lo que proporciona una visibilidad centralizada y un registro de la aplicación de las normas de conformidad.

¿Por qué Jamf?

La compatibilidad nativa para proveedores de identidad (IdP) en la nube significa que los mismos controles de seguridad centralizados basados en la identidad que regulan las credenciales de los usuarios y las terminales también se extienden a su instancia de Jamf. Jamf se basa en la integración de identidades para ofrecer una experiencia de usuario fluida, pero aplica estrategias de administración de identidades y accesos (IAM) a los recursos de la empresa, con compatibilidad total con dispositivos Mac y móviles, además de las PC con Windows, lo que da como resultado un paradigma de identidades verdaderamente unificado que es personalizable y escalable a la vez.

Administración del ciclo de vida de las apps sin complicaciones

Uno de los factores que más influyen en la experiencia del usuario son las soluciones de software que se utilizan para realizar el trabajo. Manejo de múltiples procesos:

- **Necesidades de la empresa**
- **Múltiples plataformas**
- **Preferencias del usuario**
- **Diferentes tipos de dispositivos**

Esto significa que el camino hacia la conformidad no es sencillo. Además, el hecho de tener que dar soporte a apps nativas, código propio y/o software alojado en la nube complica aún más las cosas.

La administración de parches para múltiples sistemas operativos, que comprende las actualizaciones de seguridad y las actualizaciones de apps, puede pasar fácilmente de ser una tarea de unos pocos minutos a convertirse en un proyecto de horas o días, a medida que el alcance y la escala se escapan del control de los equipos de TI.

La actualización manual de apps o la realización de actualizaciones del sistema operativo en toda la flota de dispositivos —incluso cuando la proporción de personal de TI por dispositivo sea baja— impide que los usuarios finales puedan trabajar y expone a las organizaciones a riesgos derivados de diversos vectores, tales como:

- **Vulnerabilidades sin parchar** debido a la falta de actualizaciones
- **Problemas de software** debidos a actualizaciones incompletas o parciales
- **Posturas de seguridad debilitadas** debido a implementaciones de parches no coordinadas
- **Uso de apps** no autorizadas o no aprobadas (TI en la sombra)
- **Integridad de las aplicaciones afectada** o instalaciones de apps **inseguras**

¿Qué solución permite armonizar la administración del ciclo de vida de las apps?

Una estrategia que centraliza e implementa aplicaciones de forma nativa, al mismo tiempo que realiza la integración de la visibilidad de terminales, la aplicación de la conformidad basada en políticas y la automatización de las actualizaciones de software a medida que están disponibles, garantiza que los dispositivos se mantengan actualizados —sin que el usuario lo note— y que las vulnerabilidades conocidas que puedan poner en riesgo los datos de la empresa se mitiguen de manera uniforme en toda la infraestructura, sin importar el sistema operativo o el tipo de dispositivo que se trate.

Esto significa:

La información sobre el inventario **se actualiza en tiempo real**, lo que permite saber qué apps y versiones de las mismas están instaladas en los dispositivos administrados.

Las aplicaciones **proceden de desarrolladores legítimos**, y su autenticidad e integridad se verifican mediante firmas digitales.

El software se instala de forma nativa y **se actualiza automáticamente**, lo que reduce los gastos de TI al optimizar los ciclos de vida de las apps administradas.

Se garantiza la **conformidad** mediante políticas, lo que asegura que las apps administradas estén disponibles y configuradas de la misma manera en todos los dispositivos compatibles.

Se **simplifican** los registros de auditoría. Gracias al registro unificado, queda demostrada la conformidad y es fácil de compartir con los auditores.

¿Por qué elegir Jamf?

Para tener éxito, las estrategias de administración de parches deben ser seguras, eficaces, escalables y coherentes. Con los Jamf App Installers se cumplen todos estos requisitos y se combinan con la automatización para garantizar la conformidad y lograr parámetros de seguridad básicos en los dispositivos finales al realizar la implementación de software de terceros. Esto se combina con políticas potentes y flexibles que utilicen indicadores para mantener actualizados los parches de seguridad del sistema operativo y del sistema, lo que permite mantener un estado de seguridad robusto en los dispositivos, en consonancia con el estado de seguridad general de la empresa.

Prevención de amenazas antes de que lleguen al usuario

Nada frena la productividad tan rápidamente como una amenaza maliciosa que impide el acceso a los datos, ralentiza la conectividad a Internet hasta niveles inservibles o pone en peligro la integridad de los datos de la empresa, o las tres cosas a la vez.

Las tres secciones anteriores tratan sobre la implementación de dispositivos, los derechos de acceso y la administración del ciclo de vida de las aplicaciones. En esta sección se destaca que la defensa y la prevención frente a las amenazas son fundamentales para mantener la productividad de los empleados ante las amenazas actuales. En particular, ante las amenazas sofisticadas que combinan dispositivos móviles, diversas plataformas y la dependencia actual de las empresas de los servicios en la nube para atacar a los usuarios finales, tanto a los que trabajan en la oficina como a los que lo hacen de forma remota.

Si bien una respuesta eficaz a incidentes es fundamental para mitigar las amenazas existentes y evitar que se conviertan en algo mucho peor, la realidad es que, para cuando una terminal vulnerable se ve comprometida, el usuario final ya sintió su impacto. Además, corregir el problema requerirá una mayor interrupción, lo que aumentará el impacto al prolongar los retrasos.**Esto da como resultado:**

- Una **pérdida** de **productividad**,
- Lo que provoca **un tiempo de inactividad** prolongado,
- Lo cual **agrava el impacto** en los equipos,
- Lo que afecta **negativamente** las operaciones de la empresa,
- Lo que da lugar a una **pérdida** de **ingresos**,
- **Menoscabando** la confianza de los clientes,
- Lo que genera mayores **costos** de reparación.

¿Qué solución ayuda al departamento de TI a adelantarse a las amenazas?

Para detener una amenaza de manera eficaz, el departamento de TI debe, en primer lugar, ser capaz de identificarla. Ya sea que se trate de una app no compatible o de una configuración desactivada por el usuario, la clave para evitar riesgos para los datos de la empresa es prevenir la amenaza desde el principio.

Esto significa:

- **Monitoreo activo** de datos de telemetría con gran cantidad de información contextual, incluido el estado de los dispositivos finales.
- Obtener un conocimiento profundo de las matrices de riesgo de los dispositivos finales para **evaluar y priorizar la gravedad de las amenazas.**
- **Tener visibilidad sobre los dispositivos** que acceden a recursos protegidos es fundamental, tanto si se trata de dispositivos administrados como de no administrados.
- **Soluciones de integración** para crear una estrategia cohesionada que abarque la administración de dispositivos, la identidad y la seguridad de terminales.
- **Aprovechar las tecnologías de aprendizaje automático (ML)** para reforzar y ampliar de manera eficiente la identificación y resolución de amenazas desconocidas.

¿Por qué elegir Jamf?

Jamf verifica la conformidad de terminales mediante múltiples capas de protección. El monitoreo en tiempo real permite controlar el estado de los dispositivos. Los hallazgos se registran y se comunican al departamento de TI para evitar que los recursos de la empresa se pongan en riesgo. Estos datos se utilizan para corregir riesgos al hacer que el dispositivo cumpla con las normas de manera automática, lo que resuelve el problema de forma invisible para el usuario final y sin la intervención del departamento de TI.

Cero inactividad: conservar a los empleados (y los ingresos) en marcha

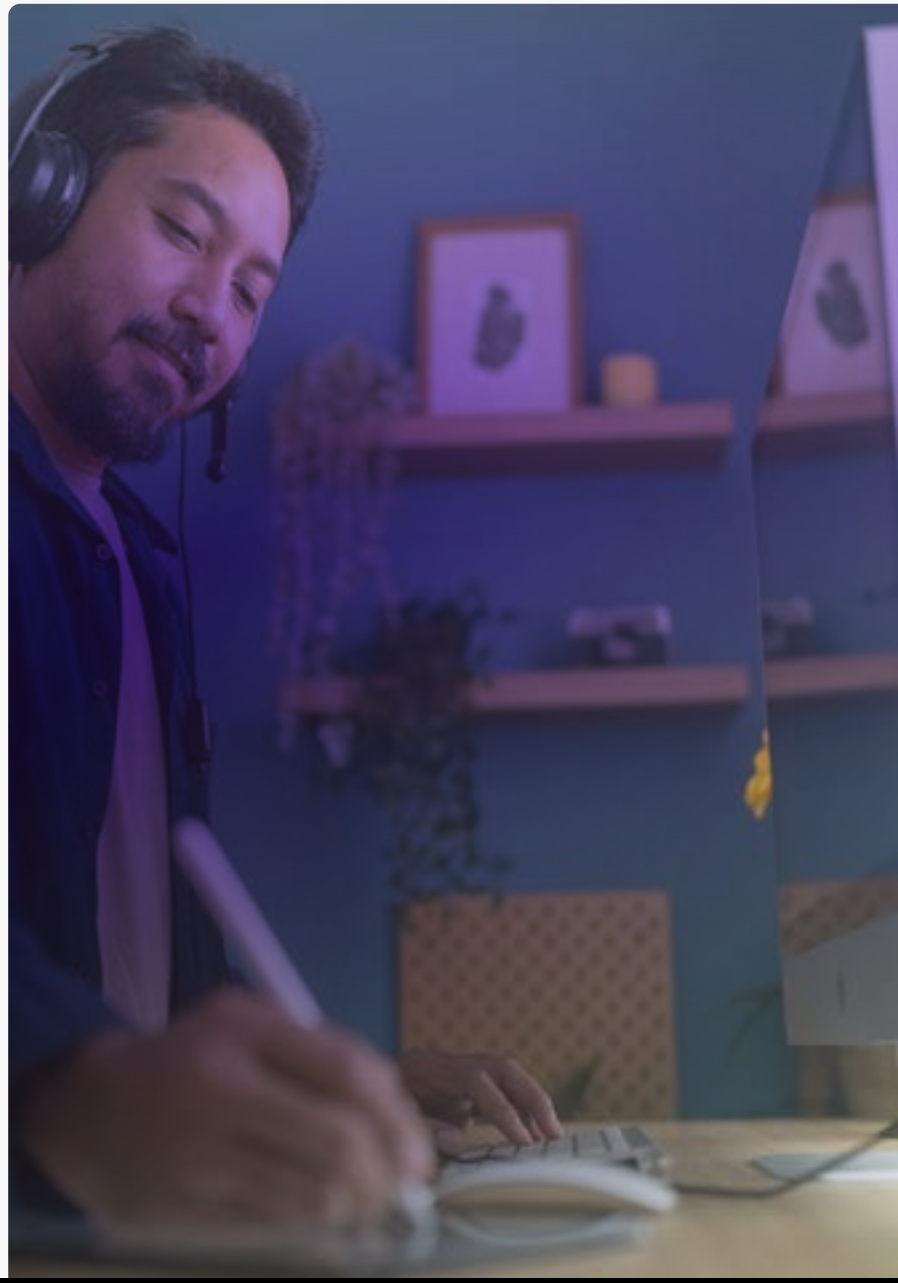
Factores como:

- **Compatibilidad con varias plataformas**
- **Dispositivos de escritorio y móviles**
- **Tecnologías de nube híbrida**
- **Flotillas distribuidas**
- **Modelos de propiedad de los dispositivos**

plantean retos para las estrategias de administración integral. Desde mantener la productividad de los equipos híbridos hasta realizar la integración perfecta de soluciones de distintos proveedores, pasando por ampliar la seguridad de manera integral en toda la infraestructura, el departamento de TI de las empresas debe hacer frente a numerosos retos complejos para que las operaciones comerciales sigan avanzando con éxito.

Las empresas modernas que operan a nivel mundial son multifacéticas, como un pulpo. Cada área representa una iniciativa estratégica que forma parte del conjunto conocido como transformación digital.

Ya han quedado atrás los días en que bastaban un firewall, un antivirus, un dominio local y una conexión VPN para mantener el tráfico seguro dentro de los límites de la red perimetral. Hoy en día, cada una de las "ramas" o áreas específicas requiere soluciones dinámicas y flexibles que permitan una administración y protección de manera eficaz, desde cualquier dispositivo, con cualquier sistema operativo y desde cualquier parte del mundo, sin dejar de ofrecer al usuario toda la comodidad, el acceso y la protección que espera y necesita para mantener a salvo sus dispositivos informáticos, los recursos de la empresa y su privacidad.



¿Qué solución de seguridad protege dinámicamente los recursos protegidos en todas las plataformas?

Las soluciones heredadas dejan brechas de seguridad que conducen a un riesgo de filtraciones de datos. Las empresas actuales necesitan tecnologías adaptativas, basadas en arquitecturas de confianza cero, para aprovechar la administración de identidades y accesos (IAM), la administración de dispositivos y la seguridad de terminales, con el fin de ofrecer una solución integral que vaya más allá de la mitigación de las amenazas y los ataques modernos y garantice la conformidad.

Esto significa:

- Cambiar de un modelo de confianza implícita a uno en el que **se rechace el acceso de manera predeterminada:** nunca confiar, siempre verificar.
- **Validar el estado de las credenciales** y **del dispositivo** en cada ocasión de forma explícita, antes de autorizar una solicitud de acceso.
- Añadir una capa de **conocimiento contextual** para combatir amenazas sofisticadas mediante el análisis de comportamientos.
- Implementación de **defensas dentro de la red** que aíslen el tráfico en microtúneles independientes, para impedir el espionaje y el movimiento lateral.
- **Acelerar** la respuesta ante incidentes y ejecutar flujos de trabajo de solución mediante la automatización para reducir el tiempo de inactividad.

¿Por qué elegir Jamf?

Con el acceso a la red de confianza cero (ZTNA) de Jamf, la protección contra amenazas modernas se extiende a todos los tipos de dispositivos compatibles, lo que ofrece un soporte multiplataforma con paridad para optimizar las estrategias de seguridad en todos los parques de dispositivos, independientemente de su ubicación y del tipo de conexión de red. Al incorporar defensas en capas desde el diseño, los usuarios finales obtienen acceso nativo a los recursos de la empresa, mientras que los equipos de TI se benefician de una mayor alineación entre las operaciones comerciales y los requisitos de conformidad.

Reducción al mínimo de las solicitudes de asistencia técnica para maximizar la productividad de los usuarios

Una de las principales responsabilidades del departamento de TI es satisfacer las necesidades de los usuarios. En la mayoría de las organizaciones, el número de empleados supera con creces el de profesionales de TI que forman parte del personal. Por ello, la capacidad del departamento de TI para responder, clasificar y resolver los problemas de manera oportuna y eficiente, con un alto grado de éxito, se ve significativamente afectada por factores como:

- **Capacidad promedio de procesamiento de tíckets**
- **Eficiencia de los flujos de trabajo**
- **Tamaño del equipo de TI**
- **Cultura empresarial**
- **Competencias de los miembros del equipo**

Cualquier posible deficiencia en uno o varios de estos factores se ve agravada por la falta de coordinación entre ellos. Esto da lugar a una disminución de la eficiencia en las operaciones comerciales, lo que provoca una falta de continuidad con respecto a los objetivos empresariales.

Si bien esos son efectos a largo plazo, las partes interesadas perciben repercusiones más inmediatas en forma de retrasos en la finalización de las tareas laborales debido a:

- Software **no instalado**
- Configuraciones **sin definir**
- Permisos **incorrectos**
- Mensajes de **error** del sistema
- **Incompatibilidades** de hardware

¿Qué solución convierte a las TI en un motor de productividad?

La opinión generalizada es que ampliar los derechos de acceso de los usuarios no resuelve los problemas relacionados con la experiencia del usuario. Al intentar "resolver" un problema, el departamento de TI abre la puerta a un mayor riesgo, lo que aumenta la probabilidad de que se vea comprometida la integridad de los datos y de que se produzcan incidentes de seguridad con mayor frecuencia.

Sin embargo, la creación de un repositorio centralizado que permita a las partes interesadas resolver por sí mismas los problemas —los que no requieren conocimientos técnicos— no solo ofrece a los usuarios las soluciones puntuales que necesitan, sino que libera al equipo de TI para que pueda enfocar sus esfuerzos en desarrollar mejores flujos de trabajo que maximicen la productividad de los usuarios, alineándose así más estrechamente con los objetivos de la empresa.

Esto significa:

- Incluir **a las partes interesadas como parte de la solución,** y no como un problema del que hay que defenderse.
- Los usuarios finales pueden **instalar apps autorizadas** y **configurar ajustes permitidos** sin modificar las normas de permisos.
- La automatización de las **actualizaciones de aplicaciones** mediante una tienda virtual fácil de usar que permita la actualización con un solo clic.
- Enlazar el portal corporativo con **proveedores de identidad (IdP) basados en la nube** para acercarnos más a los usuarios allí donde se encuentren.
- Ofrecer una **tienda nativa** que se adapte a la experiencia del usuario, además de enviar notificaciones sobre las actualizaciones de las apps.

¿Por qué elegir Jamf?

Self-Service+ para Mac, iPhone e iPad suministra una tienda nativa de Apple administrada por la empresa, diseñada para que las aplicaciones, herramientas, scripts, recursos consumibles (como impresoras) y actualizaciones estén a solo un clic de distancia, sin necesidad de permisos administrativos. Al realizar la integración con el proveedor de identidades (IdP), el departamento de TI puede aprobar solicitudes de forma fluida y temporal sin afectar de manera permanente la conformidad, con un completo registro de auditoría.

Conclusión

Las organizaciones productivas eliminan los obstáculos tanto en las operaciones de TI como en la experiencia de los empleados. Al unificar la administración de dispositivos, la seguridad de identidades y la seguridad de terminales, las empresas pueden automatizar la incorporación de usuarios, aplicar controles de acceso coherentes, mantener el buen funcionamiento de las aplicaciones y prevenir las amenazas antes de que afecten al trabajo. Jamf ofrece estas funciones a través de flujos de trabajo diseñados para adaptarse a flotas de dispositivos de todo tipo, al mismo tiempo que garantiza la productividad y la seguridad de los usuarios. Gracias a la implementación sin intervención, la protección proactiva y el autoservicio, que permite a los empleados resolver necesidades comunes en cualquier momento, el departamento de TI reduce los gastos operativos al tiempo que refuerza la conformidad y la resiliencia.
El resultado es un entorno seguro y optimizado en el que los empleados puedan enfocarse en tareas significativas desde el primer día.

Puntos clave

- **Acelerar la incorporación en grandes flotas de dispositivos:** la implementación sin intervención humana proporciona dispositivos listos para el trabajo sin necesidad de un tedioso proceso de configuración manual.
- **Ampliar el acceso sin ralentizar a los usuarios**: el acceso basado en roles adapta automáticamente los permisos a la identidad a medida que crecen las organizaciones.
- **Mantener el buen funcionamiento de las apps en miles de dispositivos:** la automatización de las actualizaciones y los parches garantiza la seguridad del software sin afectar la productividad.
- **Detener las amenazas antes de que interrumpan las operaciones**: el continuo monitoreo y la aplicación de la conformidad reducen el tiempo de inactividad en las plantillas de trabajo distribuidas.
- **Empoderar a los usuarios y reducir la carga de trabajo del departamento de TI**: Self Service permite a los empleados instalar apps aprobadas y resolver problemas comunes sin necesidad de crear nuevos tíckets.
- **Ofrecer experiencias uniformes en todas las plataformas y ubicaciones**: los flujos de trabajo unificados garantizan la seguridad y la productividad de los dispositivos, tanto si los empleados trabajan en la oficina como de forma remota.

¿Listo para verlo en acción?

Pruebe Jamf hoy mismo.