

 jamf

Protección de terminales Mac

para principiantes

La seguridad nativa no se encuentra en la terminal

No cabe duda de que los dispositivos Mac son los más seguros del mercado. Lo que durante décadas ha sido toda una certeza continúa siéndolo hoy en día. A medida que las organizaciones se plantean la composición de su flota, las soluciones de seguridad para proteger los datos, los dispositivos y los usuarios son decisivas.

El exceso de confianza puede provocar intrusiones perjudiciales o de alto costo. Si se dispone de una solución de protección de terminales diseñada para Mac, los equipos de IT y de seguridad no solo pueden protegerse contra las amenazas conocidas, sino también seguir adaptándose y anticiparse a las futuras necesidades de seguridad de su organización.

Tanto si se trata de una empresa con una flota de Apple como de una pequeña empresa que administra un pequeño número de dispositivos Mac, Jamf amplía la protección de las terminales yendo más allá de lo que Apple proporciona como funcionalidad nativa a fin de colaborar en la protección de sus dispositivos macOS, los datos de la organización y los usuarios finales.



EN ESTA GUÍA, HABLAREMOS DE LO SIGUIENTE:

- La protección de terminales de las Mac implica
- Por qué la protección de terminales diseñada para varios sistemas operativos es insuficiente para Mac



PROTECCIÓN DE TERMINALES EN MAC:

Amplíe la ventaja de la seguridad nativa de Apple y prepárese para lo desconocido.

A medida que el uso del Mac sigue incrementándose en empresas, pequeños negocios, escuelas y organizaciones de atención a la salud, es cada vez más importante garantizar que los dispositivos y los datos se utilicen con fines legítimos, de forma correcta y por parte de usuarios autorizados: [incorpore la protección de las terminales Mac](#).

Para lograrlo, muchas áreas operativas —[administración de la identidad](#), [aplicación de parches](#), [antivirus \(AV\)](#), [configuración](#), [detección de terminales y respuesta](#)— actúan de manera conjunta para satisfacer las necesidades de su equipo de IT y de seguridad.



Obtenga más información sobre la administración de recursos, datos y usuarios corporativos con nuestro libro electrónico [Gestión de identidades para principiantes](#).

ADMINISTRACIÓN DE LA IDENTIDAD Y EL ACCESO

Las medidas de seguridad implementadas a través de la administración de la identidad afectan tanto a los usuarios finales como al departamento de IT a lo largo del ciclo de vida de los empleados, sin importar los estados de trabajo presencial o remotos. Las soluciones Zero Trust Network Access (acceso a redes de confianza cero, ZTNA), las redes privadas virtuales (VPN) y las aplicaciones SaaS que conectan a los empleados con los recursos de la empresa ofrecen oportunidades para reforzar la protección de los puntos finales.

Con una fuerza laboral que usa cada vez más dispositivos móviles, con empleados que trabajan desde distintas ubicaciones y con distintos dispositivos, las organizaciones deben ser capaces de administrar y proteger la seguridad de estos dispositivos y la información de la empresa sin el reto de vincularse con el directorio activo de las instalaciones. Jamf Connect ayuda a los usuarios desde su [primer día de trabajo hasta el último](#). Con Jamf Connect, el usuario puede abrir la caja del dispositivo Mac, encenderlo y acceder a todas las aplicaciones corporativas tras iniciar sesión con un único conjunto de credenciales, basado en la nube. Con Jamf Connect, las organizaciones pueden supervisar la identidad y el acceso con un impacto mínimo en la experiencia del usuario final y disfrutar de una priorización constante de la seguridad de dispositivos y datos.

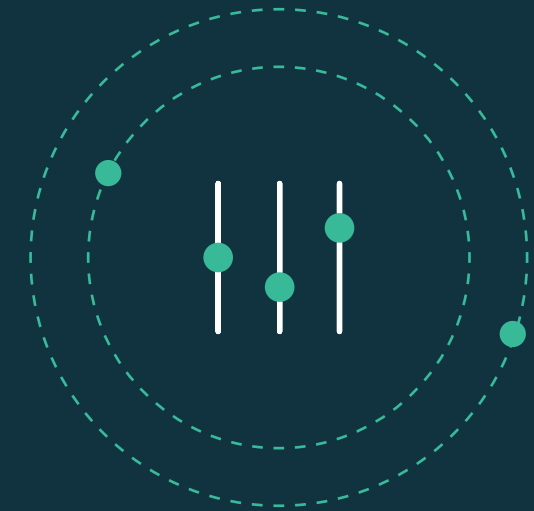
ADMINISTRACIÓN DE APPS

La administración automatizada de las aplicaciones simplifica el trabajo y favorece la eficacia y la seguridad de los usuarios.

Al garantizar que los usuarios obtienen las aplicaciones adecuadas a través de medios seguros, como Jamf Self Service o Mac App Store:

- Las apps pueden implementarse para el servicio de los usuarios y dispositivos correctos
- Los títulos y aplicaciones personalizados están disponibles para que los usuarios los obtengan cuando los necesiten
- El departamento de IT puede impulsar actualizaciones y establecer requisitos que protejan a la organización y a los usuarios

Integre Jamf Pro con Apple Business Manager para asignar y administrar las licencias de las aplicaciones y el software de su organización. Además, Jamf Pro puede ayudarle con los parches y las actualizaciones de software. Esto también garantiza la actualización y administración de cualquier posible versión de software vulnerable y la visibilidad del estado de toda su flota de Mac. Debe realizarse con frecuencia y facilidad la aplicación de parches de seguridad para garantizar la mitigación de vulnerabilidades conocidas. Jamf le permite agilizar el trabajo necesario para mantener o actualizar las aplicaciones en macOS y le proporciona visibilidad adicional en materia de conformidad y compatibilidad, a la vez que ofrece una experiencia de calidad al usuario final. Esto también implica ejecutar la última versión de macOS en cuanto se publique para evitar intrusiones en la seguridad como consecuencia de retrasos en las actualizaciones.



Las herramientas de seguridad y de administración no deberían ser motivo para posponer las actualizaciones del sistema operativo. Con Jamf, la solución no le frena, sino que es compatible con las nuevas versiones de macOS el mismo día en que se publican y sin demoras. Actualice sus dispositivos conforme a su programa, no al nuestro.



ANTIVIRUS (AV)

El antivirus puede parecer una nueva necesidad para Mac, pero existe una nueva realidad. Cada vez se presta más atención a Mac y a macOS conforme se expande su presencia en la empresa.

El antivirus es un requisito básico para que la mayoría de los dispositivos de la organización proporcionen una seguridad básica. Apple incluye un mecanismo antivirus básico en macOS con XProtect, Gatekeeper y MRT. Sin embargo, estas herramientas se actualizan de manera esporádica y las organizaciones carecen de visibilidad respecto a sus acciones. Jamf Protect añade sofisticadas capacidades antivirus para prevenir y poner en cuarentena el malware para Mac y supera con creces lo que las soluciones centradas en Windows son capaces de ofrecer en macOS.

Las organizaciones no deben esperar a que surjan problemas de malware, adware u otro software no deseado. Necesitan implementar un antivirus que identifique y remedie eficazmente los ataques específicos de Mac sin invertir valiosos recursos en la búsqueda de amenazas para Windows en un dispositivo Mac. Tanto para la seguridad como para la experiencia del dispositivo es vital contar con capacidades antivirus para Mac que sean eficaces, eficientes e integrales. Al mismo tiempo, cualquier solución antivirus que interfiera con la capacidad de su usuario final para ser productivo solo generará molestias para todos los implicados. Jamf Protect está diseñado para proteger macOS del malware sin alterar la experiencia que los usuarios finales esperan de Mac.

El antivirus para Mac ya no es algo que se desee tener, sino una necesidad. No solo se necesita antivirus, sino un antivirus creado para Mac sin las limitaciones que conlleva un antivirus diseñado para su uso en varios sistemas.

CONFIGURACIÓN

La seguridad preinstalada para Mac es estupenda —es la mejor que existe—, pero con las amenazas modernas y en constante evolución del panorama de la ciberseguridad, no es suficiente. Necesita evaluar y hacer evolucionar su postura de seguridad para proteger sus dispositivos y datos. Y si reforzar su seguridad es fácil, ¿por qué no lo hace?

En la comunidad de seguridad existe un importante volumen de conocimientos y scripts para llevarlo a cabo.

Con Jamf, es fácil de implementarlos y ejecutarlos, así como controlar a cualquier usuario que intente modificar estas normas. Jamf elimina los obstáculos que quizás le hayan impedido implantar a usted una seguridad básica en todos sus dispositivos.

FileVault, la activación de los requisitos de firewall y contraseñas, la configuración del protector de pantalla y los requisitos de bloqueo son elementos que intervienen en el posicionamiento de sus requisitos de seguridad y puntos de referencia.

¿No sabe por dónde empezar? El CIS (Center for Information Security, Centro para la Seguridad de la Información) proporciona puntos de referencia de la industria y Jamf cuenta con certificación del CIS. Con Jamf, usted ya está en el proceso y contamos con recursos para ayudarle.



Obtenga más información sobre los puntos de referencia de seguridad del CIS y de Jamf con [nuestra lista de comprobación de seguridad de macOS](#).

DETECCIÓN Y RESPUESTA CENTRADA EN MAC

Las herramientas tradicionales de detección y respuesta de terminales (EDR) existen desde hace tiempo para Mac, pero la mayoría no están diseñadas para detectar con eficacia los ataques dirigidos específicamente a Mac. En cambio, intentan forzar los modelos de Windows en los dispositivos Mac. Gracias a que Jamf Protect se centra exclusivamente en Mac y macOS, Jamf minimiza los falsos positivos y maximiza las tasas de detección en Mac.

Al combinar Jamf Protect con Jamf Pro, se le conceden capacidades de resolución mínimamente invasivas que superan con creces las capacidades promedio de una herramienta EDR. Jamf permite a los equipos de IT y de seguridad establecer un plan de respuesta a incidentes sin interrupciones que posibilita la colaboración de sus equipos.



JAMF ES SEGURIDAD PARA LAS TERMINALES.

La protección de terminales Mac con Jamf Protect es compatible con el cumplimiento de las terminales, satisface las necesidades de antivirus al prevenir el malware para macOS, controla y protege las aplicaciones Mac dentro de la organización, y detecta y repara las amenazas específicas para Mac con un impacto mínimo en la experiencia del usuario final.

Y si se combina con Jamf Pro, Jamf desbloquea amplias capacidades de automatización, investigación y resolución a fin de mitigar los riesgos de seguridad de los puntos terminales, ya sean grandes o pequeños.

Solicite una prueba gratuita

o comuníquese con su distribuidor Apple preferido cuando esté listo para reforzar su seguridad.

Obtenga más información sobre las [funcionalidades de protección de terminales de Jamf para Mac](#).

