Guía avanzada para la administración de dispositivos Mac

Panorama de la seguridad

La ciberseguridad sigue mejorando.
Según el informe 2023 Global Digital Trust Insights (Perspectivas mundiales de la confianza digital 2023) de PwC, publicado recientemente, la ciberseguridad ha mejorado en muchos aspectos desde 2020: más del 70 % de 3,522 líderes de la C-Suite de una amplia gama de industrias y ubicaciones de todo el mundo iniciaron mejoras en la ciberseguridad en 2021.

Aún nos queda mucho camino por recorrer.
El 38% de los encuestados considera que ha mitigado completamente los riesgos relacionados con el trabajo remoto e híbrido; por ejemplo, mientras que el 48% cree que los ha mitigado moderadamente. el 35% afirmó haber mitigado por completo los problemas relacionados con la adopción acelerada de la nube.

Sin embargo, **solo el 3% afirma haber mitigado por completo los riesgos cibernéticos emergentes**. Solo el 5% informó que estaban optimizando los cinco aspectos del flujo de trabajo de seguridad: identificar, proteger, detectar, responder y recuperar.

Por desgracia, los ciberdelincuentes sólo necesitan una vía de entrada para causar estragos.
¿Cómo pueden los administradores de InfoSec y Mac asegurarse de que se aplican **todos los protocolos de seguridad** en **todas las áreas** del entorno digital?

Solo

38%

informa que han mitigado completamente los riesgos cibernéticos emergentes

Una administración adecuada de dispositivos Mac es una administración segura del Mac

Esta Guía 201 sobre administración de dispositivos Mac, continuación de nuestro libro electrónico sobre Administración de dispositivos Mac para principiantes, explica cómo la gestión de dispositivos macOS es la clave para proteger su flota Apple. Una administración adecuada no es la fotografía completa del panorama de la seguridad, pero es la base sobre la que deben construirse todas las organizaciones.

Siga leyendo para saber más sobre la administración adecuada de la seguridad. También cubriremos las capacidades, los flujos de trabajo y las configuraciones clave necesarias para administrar de forma segura su flota Mac y cubrir todas las bases.

Certificados PKI y push

Certificados PKI
Un certificado PKI es un archivo de texto que contiene datos de identificación sobre máquinas, usuarios y dispositivos. Básicamente, confirma la seguridad de la computadora y protege la información que se envía de un lugar a otro mediante cifrado.

En Jamf Pro puede optar por utilizar una autoridad de certificación (CA) integrada, integrarse con una CA de terceros de confianza (DigiCert, Venafi o Active Directory Certificate Services) o configurar su propia PKI si tiene acceso a una CA externa compatible con el protocolo simple de inscripción de certificados (SCEP). La CA puede utilizarse para emitir certificados tanto para computadoras como para dispositivos móviles. Cuando se utiliza Jamf Pro, el certificado CA incorporado, revoca y renueva, crea un certificado incorporado a partir de una solicitud de firma de certificado (CSR) y crea una copia de seguridad.

Se pueden utilizar certificaciones para Single Sign-On (SSO), perfiles de inscripción, administración de dispositivos con Jamf Binary, perfiles de configuración y mucho más. Los administradores pueden implementarlos manualmente a través de un portal web, mediante la automatización con un tercero como Jamf Connect, o mediante una solicitud directa de certificado: un proceso automatizado en el que el dispositivo se comunica con el servidor a través de Jamf Pro.

El cifrado con certificados no solo protege todas las comunicaciones, sino que también permite revocar inmediatamente el acceso a las personas que abandonan la empresa o a los dispositivos que incumplen la normativa.

Certificados push

Un certificado push es un archivo cifrado generado por Apple que establece la confianza entre un servicio de terceros como Jamf Pro y Apple Push Notification Service (APNs). Un certificado push es creado por Apple, pero necesita un servicio de terceros, como Jamf, y APNs. Utilizan un ID de Apple propiedad de la organización en lugar de un ID de Apple personal.

Los certificados push permiten la comunicación entre el servidor Jamf Pro y los APNs. Los APNs controlan la información, en concreto la información de las aplicaciones, que se envía desde y hacia los dispositivos. Las notificaciones push son la forma en que las aplicaciones de los dispositivos reciben la comunicación.

Como se trata de un archivo cifrado generado por Apple, puede desinstalar una aplicación de forma remota basándose en esta información de seguridad. Las certificaciones Push son válidas durante un año y deben renovarse con el mismo ID de Apple que la creó inicialmente.

Cómo encontrar certificados

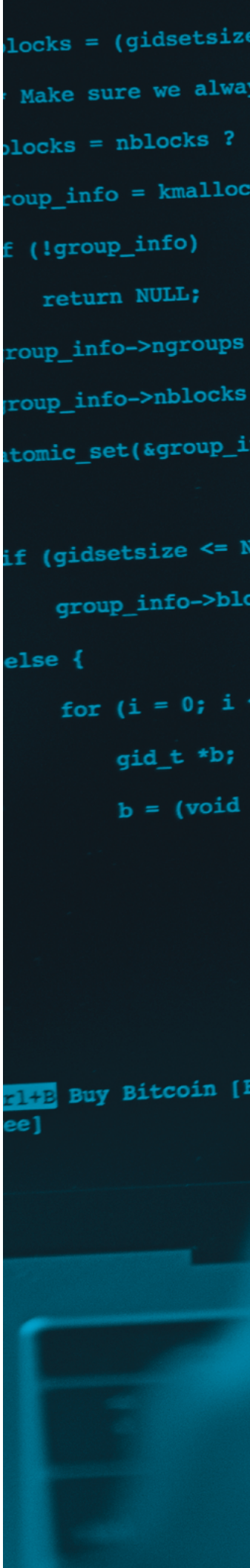
Puede ver una lista de certificados exportándola a archivos .csv, .txt o XML. Jamf Pro facilita este proceso indicando al administrador de IT cómo crear un certificado push (.pem) y cargarlo en Jamf Pro. Necesitará un Jamf ID y un Apple ID válidos, y es fundamental que los administradores de Mac mantengan estos certificados actualizados. Si caducan, los APNs perderán la conexión con sus servidores de administración de dispositivos móviles (MDM) o con terminales.

Acceso condicional

Debido a la nueva normalidad del trabajo remoto desde casa, cafeterías o incluso en vuelos, las empresas ya no pueden crear una red y proteger los dispositivos y usuarios mediante un cortafuegos.

El acceso condicional permite a una organización establecer parámetros para proteger los datos de una organización en muchas ubicaciones. Puede bloquear el acceso a datos de la organización —como el correo electrónico, OneDrive, Word y Excel— y aplicaciones en la nube —como Jamf Pro— evaluando el riesgo en ese momento.

Al exigir un dispositivo y un usuario de confianza para acceder, se mejora la administración y la seguridad, independientemente de dónde se trabaje.



Los dispositivos Mac de la organización son administrados por Jamf y registrados en Microsoft Intune a través de un conector en la nube o un conector manual. La sólida asociación entre Jamf y Microsoft garantiza que esto funcione a la perfección: Jamf envía el inventario de dispositivos macOS a Intune. Intune evalúa el cumplimiento y genera un informe de cumplimiento. Azure AD aplica controles de acceso.

Para obtener más información sobre la creación de una política de cumplimiento exhaustiva para Mac que mantenga la seguridad de sus dispositivos, usuarios y datos organizativos, lea Administración del cumplimiento para principiantes.

TeamViewer: acceso remoto a administradores Mac

TeamViewer es una solución rápida y segura para acceder a computadoras y redes de forma remota. Establece una conexión remota con pantalla compartida entre un administrador de Jamf Pro y la computadora de un usuario final.

Esto mejora la seguridad y el cumplimiento, ya que los administradores pueden ver, evaluar y resolver problemas rápidamente sin que se pierda información en el desplazamiento. Asimismo, acelera la resolución de problemas. Cuando esos problemas afectan a la seguridad, la velocidad realmente importa.

Necesitará una configuración de integración de TeamViewer añadida a su instancia de Jamf Pro para acceder a esta capacidad.

API de Jamf

El objetivo de la API de Jamf es propiciar que Jamf sea más accesible. Permite a las organizaciones que Jamf Pro se ajuste a su pila tecnológica, creando un sistema cohesionado en el que está integrada la administración de Mac. Esto potencia la interconectividad entre Jamf y otros proveedores y permite integraciones como Jamf Protect/Jamf Connect, la app Jamf School Parent, la app Jamf Teacher y otras.

El esquema de autenticación basado en tokens de la API Jamf refuerza la postura de seguridad de los dispositivos que interactúan con aplicaciones e integraciones de terceros. Es una interfaz RESTful, lo que significa que sigue los estándares de comunicación de software seguro.

Flujo de trabajo

1. Utilizando la autenticación básica, solicite un token de portador enviando un POST a `/v1/auth/token.`

2. Deberá recibir una respuesta que incluya un token y una fecha de caducidad similar a la del siguiente ejemplo:

```
{
    "token": "eyJhbGciOiJIUzUxMiJ9...",
    "expires": "2022-01-24T21:35:20.373Z"
}
```

3. Puede utilizar el token generado previamente para realizar llamadas a cualquier otra terminal de la API Jamf Pro incluyéndolo en un encabezado con el formato Authorization: `Bearer TOKEN VALUE.`

Las integraciones permiten una visión más holística de las capacidades de Jamf, y una conexión hermética con Jamf Protect, capacidades de protección de terminales con prevención de amenazas de red para Mac. Esto permite que los administradores se prevengan contra malware de macOS, se protejan contra eventos específicos y supervisen las terminales y solucionen los problemas rápidamente.

Webhooks

Los webhooks permiten que un administrador de Mac se suscriba a un evento específico en una instancia de Jamf Pro. Cuando se produce el evento, se envía una carga útil HTTP POST a una URL especificada. Permiten que los administradores utilicen los eventos en tiempo real de Jamf Pro para crear flujos de trabajo personalizados sobre la marcha, utilizando el lenguaje de programación de su elección.

Los webhooks apoyan la ciberseguridad manteniendo a los administradores de IT al día sobre los eventos en tiempo real en sus instancias, enviados como XML o JSON. Y pueden permitir que los administradores creen cargas útiles genéricas como ComputerAdded (nueva computadora inscrita), ComputerCheckin (verificación de tareas) o ComputerPatchPolicyCompleted (política de parches informáticos completada).

Puntos de distribución

Los puntos de distribución son servidores utilizados para alojar archivos que se distribuyen a computadoras (y dispositivos móviles). Los paquetes, scripts, apps internas y libros pueden distribuirse mediante un punto de distribución.

Jamf Pro admite puntos de distribución de archivos compartidos y un punto de distribución en la nube. Jamf se pondrá en contacto con los puntos de distribución locales para encontrar aplicaciones y distribuirlas en los dispositivos/usuarios mediante el uso compartido de archivos. Los administradores también pueden distribuir aplicaciones utilizando el punto de distribución alojado en la nube de Jamf: Jamf Cloud Distribution Service (JCDS).

Los puntos de distribución pueden ser un punto débil en la seguridad de las organizaciones, ya que se encuentran más seguido en la nube con usuarios ubicados en todo el mundo. Es fundamental distribuir archivos a los dispositivos Mac a través de un punto de distribución absolutamente seguro.

Cómo funcionan los puntos de distribución con Jamf

De manera preestablecida, el primer punto de distribución que usted añada a Jamf Pro será el punto de distribución principal. Todos los demás puntos de distribución dependerán del primero como fuente autorizada para todos los archivos durante la replicación. Los puntos de distribución garantizan que los archivos se envíen al dispositivo o usuario correctos de la forma correcta.

Creación de scripts (scripting), perfiles de configuración y cifrado de disco: trabajando juntos

Creación de scripts
La automatización de tareas comunes multiplica la seguridad 10 veces: elimina el error humano en la implementación, así como la posibilidad de que un administrador olvide una tarea importante. Esto puede hacerse mediante la creación de scripts. La creación de scripts puede automatizar muchas tareas y ofrece un mayor control a los administradores sobre sus aplicaciones Mac.

Este método solo es cuestión de práctica y de empezar poco a poco. ¿Tiene alguna tarea que le gustaría automatizar? Utilice Jamf Nation y otros foros de administradores Mac para buscar scripts que otros ya hayan creado para ese fin.

¿Quiere sumergirse en scripts y tareas específicos? Lea Automatización de tareas comunes con scripts de Apple y con Jamf

Perfiles de configuración
Una forma importante en la que los scripts pueden ampliar y asegurar el control de un administrador es mediante la implementación de perfiles de configuración.

Los perfiles de configuración son archivos XML (.mobileconfig) que permiten definir ajustes y restricciones para dispositivos y usuarios fácilmente. Suelen utilizar APNs. Al crear un perfil de configuración de equipo, los administradores deben especificar el nivel en el que se aplicará el perfil: nivel de equipo o nivel de usuario. Cada nivel tiene un conjunto único de cargas útiles y unas pocas que son comunes a ambos.

Los perfiles de configuración pueden reforzar y mejorar la seguridad por sí mismos, aplicando protocolos de seguridad en las contraseñas, el comportamiento y mucho más.

Los perfiles de configuración están integrados en Apple Configurator 2, Profile Manager y Jamf Pro, y pueden implementarse en dispositivos y usuarios con una MDM activada. Hay dos formas diferentes de distribuir un perfil de configuración: instalarlo automáticamente (no requiere interacción por parte del usuario) o ponerlo a disposición en Autoservicio.

Cifrado del disco
Aunque las secuencias de comandos y los perfiles de configuración son herramientas potentes, todo lo que pueda controlar las acciones de un dispositivo debe estar absolutamente protegido. El cifrado de discos garantiza que la información esté segura detrás de una contraseña. Cifra códigos y scripts pasándolos a un estado ilegible que será difícil de descifrar. Y está integrado en Mac.

El cifrado de discos también permite a los administradores de Mac administrar y activar FileVault en las computadoras. FileVault codifica la información de los dispositivos Mac, impidiendo que cualquiera pueda leerla sin una contraseña)

Atributos de la extensión

Los atributos de extensión son campos personalizados que usted puede crear para recopilar casi cualquier tipo de datos de inventario de los dispositivos. Puede utilizar atributos LDAP personalizados para crear atributos de extensión. Y si lo desea, puede obtener atributos de extensión aún más avanzados con scripting.

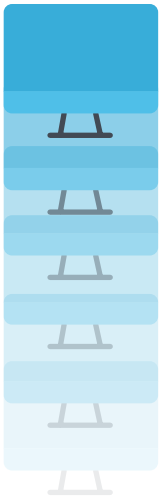
Cómo utilizarlos
Una vez que los datos de los atributos de extensión están en el registro de inventario, los administradores pueden actuar con Smart Groups con Jamf Pro: agrupar dispositivos y/o usuarios en grupos basados en uno o más atributos de inventario. Los administradores de IT no sólo pueden crear manualmente atributos de extensión que se adapten a sus necesidades, sino que también pueden aprovechar las plantillas de atributos de extensión de Jamf Pro para crear atributos de extensión de forma sencilla y eficiente.

El uso de atributos de extensión con los grupos inteligentes de Jamf Pro puede permitirle mantener su flota segura con acciones de grupo en dispositivos con cualquier sistema operativo que necesite alguna actualización y mucho más. La implementación de atributos de extensión también proporcionará una comprensión más cohesiva de los datos en su instancia, lo que permite una mejor visión de lo que está fuera de cumplimiento o puntos débiles en el sistema.

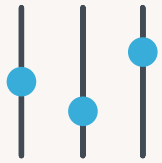
Acciones masivas

Otra forma de realizar múltiples tareas tediosas en muchas computadoras simultáneamente son las acciones masivas. Con Jamf Pro, los administradores pueden crear acciones masivas en cualquier Smart Group o grupo estático, resultados de búsqueda de computadoras o listas de coincidencias de uso de licencias. Las acciones masivas pueden ser cualquier cosa. Algunos ejemplos: comandos remotos, edición de un panel lateral o envío de correos electrónicos a los usuarios.

Esto mantiene los entornos más seguros; ya sea que se administren 5 o 5,000 computadoras, las acciones masivas garantizan que no haya prácticamente ninguna posibilidad de que se pase por alto un dispositivo que pueda causar una brecha de seguridad.



Administración de apps



Dado que las apps siguen siendo la parte más dominante de la experiencia del usuario final, la administración de aplicaciones de Mac es un elemento vital para administrar y proteger los dispositivos. Desde el aprovisionamiento y el alojamiento hasta la actualización y la implementación, es fundamental una administración adecuada de las aplicaciones para garantizar la seguridad de una flota Apple y, al mismo tiempo, apoyar la productividad de los usuarios finales.

Muchas de las apps más utilizadas hoy en día no están en el Mac App Store. App Installers ofrece a los administradores de Mac una forma mejor de crear, alojar, actualizar e instalar aplicaciones en sus computadores o usuarios automáticamente. Las apps obsoletas son un grave problema de seguridad.

Por eso Jamf ofrece formas de estar al tanto de la actualización de las aplicaciones:

App Installers
App Installers es una colección de paquetes de instalación administrados y proporcionados por Jamf, que agilizan la implementación y ofrecen una alternativa simplificada a los complejos flujos de trabajo necesarios para parchar aplicaciones de terceros.

Para garantizar la seguridad, también validan la integridad de las definiciones de los parches antes de permitir su implementación. Una vez verificada, la nueva versión de la app se implementará automáticamente en todos los dispositivos Mac compatibles.

Son los paquetes que Jamf crea, reempaqueta y aloja. Este catálogo de Jamf App es una colección de títulos de software que incluye una lista de más de 1,000 títulos de software para macOS de terceros compatibles con Jamf Pro.

Los App Installers deben estar en un grupo de computadoras inteligentes en Jamf Pro. Si un equipo de destino de un grupo inteligente tiene instalado el título del software, App Installer implementa la actualización cuando se publica una nueva versión.

Flujos de trabajo de políticas de parches
La mayoría de administradores de Mac están familiarizados con el proceso manual de implementación de políticas de parches. Jamf ofrece flujos de trabajo para estas acciones, que se encargan de la corrección de errores, algo vital para la seguridad de la red, ya que los errores en las aplicaciones de terceros son una de las formas más utilizadas para entrar en entornos que, de otro modo, serían seguros.

Una comprensión completa de su entorno de aplicaciones le permitirá saber qué aplicaciones están obsoletas y en qué computadoras. Este proceso se automatiza con los instaladores de aplicaciones y puede ejecutarse en segundo plano.

Title Editor
Title Editor es un servicio alojado en Jamf que amplía la administración de parches, proporcionando títulos de software personalizados, anulando las definiciones de parches existentes y la capacidad de crear definiciones de parches personalizadas.

Soluciones de seguridad Jamf para Mac

Aunque está claro que una administración diligente de los dispositivos Mac es vital para una seguridad adecuada, es importante recordar que la gestión de los dispositivos es la base de la seguridad. Utilizar herramientas específicas de seguridad sobre esa base firme es la última pieza del rompecabezas de la seguridad. Para obtener una visión general básica, lea Protección de terminales Mac para principiantes.

Protección de terminales de Jamf Protect

Jamf Protect va más allá de una simple herramienta antivirus para malware. Se trata de una solución integral de seguridad para terminales con detección basada en el comportamiento que anticipa y reconoce los comportamientos utilizados a menudo en los ataques.

También descubrirá la importancia de otros sistemas de seguridad, como la administración de identidades y accesos, la prevención y corrección de amenazas, el filtrado de contenidos y el acceso a redes de confianza cero (ZTNA) para mantener seguros a los usuarios, los dispositivos y los datos de la organización.

Cómo puede ayudar Jamf

Jamf Pro

Para una base sólida y segura, pruebe Jamf Pro: el estándar en administración de dispositivos Apple. Puede obtener más información y solicitar una prueba directamente a nosotros, o ponerse en contacto con su distribuidor preferido para empezar.

Seguridad más allá de la administración de dispositivos

Lea nuestro informe sobre el estado de la seguridad de Apple en la empresa, en el que se encuestó a 1,500 profesionales de IT e InfoSec. Incluye el uso y los enfoques actuales de los dispositivos, los retos para la seguridad de los dispositivos y el estado futuro de la seguridad de los puntos finales.

Trusted Access

Trusted Access es la solución de Jamf para la seguridad más allá de la administración. Trusted Access es un flujo de trabajo único que conjunta la administración de dispositivos, la identidad de los usuarios y la seguridad de las terminales para ayudar a las organizaciones a crear una experiencia de trabajo que aprecien los usuarios y un lugar de trabajo seguro en el que las organizaciones confíen.

Al garantizar que solo los usuarios de confianza con dispositivos seguros y registrados puedan acceder a los datos de la empresa, Trusted Access con Jamf incrementa drásticamente la seguridad de su lugar de trabajo moderno a la vez que agiliza el trabajo de sus usuarios, independientemente de dónde lo realicen.

¡Obtenga más información sobre las vanguardistas ofertas de seguridad Mac-first de Jamf para ver cómo podemos ayudarle a seguir administrando y protegiendo su flota de Mac!

En Jamf.com/es/soluciones descubra más sobre:

- **Administración de la identidad y el acceso**
- **Filtrado de contenidos y seguridad en Internet**
- **Protección de terminales**
- **Zero Trust Network Access (acceso a redes de confianza cero, ZTNA)**
- **Prevención y resolución de amenazas**
- **Visibilidad y cumplimiento de la seguridad**

Y si está listo para sumergirse en la administración y seguridad de sus Macs con Jamf, **¡solicite una prueba gratuita hoy mismo!**

Fuente:
1. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html