La identidad en la nube, clave para reforzar la seguridad en los Mac

El nuevo perfil de los profesionales de hoy abre la puerta a nuevas oportunidades.

Durante años, los trabajadores iban a una oficina, encendían su ordenador, se conectaban a la red de la empresa con sus credenciales y empezaban la jornada laboral.

Sin embargo, trabajar con horarios fijos en una oficina física está cada vez más fuera de la norma. Según un informe de Gallup, el 43 % de los empleados de Estados Unidos trabajan a distancia.[1] Ante este aumento de la movilidad de los profesionales, es vital que puedan acceder a los recursos de una forma igual de segura que sus compañeros que trabajan de manera presencial, sin tener que conectarse a la red de la empresa. Y tanto unos como otros necesitan sistemas seguros para acceder al creciente número de aplicaciones y recursos alojados en la nube. Para estar a la altura del desafío, las tecnologías de la empresa y las prácticas en materia de IT tienen que adaptarse.

El primer paso para poner en manos de los empleados las herramientas modernas que exigen sus nuevas realidades laborales es crear un programa de elección de los dispositivos. Con este programa, los trabajadores pueden elegir un PC o un Mac para sus necesidades laborales. Y a medida que aumenta el número de empleados que apuestan por un Mac, el equipo de IT necesita una solución optimizada para proteger los dispositivos y los usuarios, estén donde estén.

En este documento técnico planteamos nuevas y mejores formas de utilizar la identidad en la nube para proteger el Mac, el usuario y los datos del Mac, y también la organización en la que trabaja dicho usuario.

La autenticación en un Mac hoy

Aunque Active Directory (AD) y Lightweight Directory Access Protocol (LDAP) han prestado un gran servicio durante años para la autenticación en el Mac, estas tecnologías están quedando cada vez más anticuadas en los entornos modernos de hoy.
Los usuarios siguen viéndose obligados a hacer lo que se ha hecho siempre: estar en la red de área local (LAN) de una organización o utilizar una red privada virtual (VPN) para conectarse a los recursos internos, lo que se traduce en una experiencia de baja calidad. Si utiliza el plugin de Active Directory, los usuarios solo pueden modificar sus contraseñas cuando AD está disponible, lo que suele provocar confusión y el envío de costosos tickets al servicio de asistencia.
Este proceso, desfasado y repleto de parches, presenta dos grandes problemas:

1. Uso de recursos de IT innecesarios
Cuando los empleados trabajan a distancia, no están conectados automáticamente a una red de la empresa. Y ahí es cuando pueden producirse problemas relacionados con contraseñas. Gartner calcula que hasta el 40 % del volumen de trabajo de un servicio de asistencia tiene relación con restablecimientos de contraseña.[2] Muchos de estos restablecimientos son a petición de teletrabajadores que no recuerdan una contraseña.

Cada ticket de asistencia cuesta dinero. Según Gartner, el coste medio de una consulta al servicio de asistencia era de 17,88 USD.[2] Y si las organizaciones externalizan este servicio, seguramente tendrán que pagar un tanto fijo por cada ticket recibido, aunque solo sea para un restablecimiento de contraseña.

Al final los tickets van sumando y la factura no deja de crecer. Hoy día, muchas empresas están perdiendo miles de euros únicamente en restablecimientos de contraseñas.

2. Aumento de las amenazas a la seguridad
Resulta muy complicado introducir la autenticación multifactor o incluso plantearse reforzar la seguridad con métodos como la confianza en los dispositivos utilizando AD, LDAP y Kerberos como principal sistema para la autenticación de los usuarios.

iPass elaboró un informe que reveló que la mayor amenaza para la seguridad de los datos de una empresa son los empleados que trabajan fuera de la oficina. De hecho, el 57 % de los CIO y responsables de IT de todo el mundo entrevistados sospecha que sus teletrabajadores han estado expuestos a riesgos o han provocado un problema de seguridad en el último año.[3]

Las herramientas locales no son adecuadas

Active Directory de Microsoft ha sido el gran referente en la gestión local de cuentas e identidad. Active Directory mantiene los datos y las aplicaciones de la empresa fuera del alcance de cualquier persona que no figure en el directorio y que no sea un empleado.
Hasta hace poco muchas empresas usaban Active Directory para resolver problemas vinculados a la autenticación, pero la realidad es que ya no sirve para los desafíos de hoy.

¿Por qué?

Cada vez son más las empresas que sustituyen Windows por Apple y, en esta tesitura, muchos profesionales de IT cuestionan los métodos para la integración de los Mac con Active Directory.
De hecho, actualmente resulta muy problemático garantizar una autenticación práctica y segura de los teletrabajadores a través de Active Directory:

1. Si la autenticación se realiza a través de Active Directory, los empleados tienen que estar en el dominio. Eso excluye a los teletrabajadores.

2. Tradicionalmente, las organizaciones han utilizado Active Directory como proveedor de identidad principal, pero cada vez son más las empresas que ofrecen dispositivos Mac, lo que dificulta el control de los usuarios de Apple remotos y limita las opciones de gestión de usuarios. Esto obliga a utilizar complementos de terceros, lo que suma complejidad a la gestión de usuarios y aumenta los costes.

3. Los administradores de IT no pueden implantar comandos y scripts en forma de documentos de políticas que aplican sus ajustes a los ordenadores y usuarios bajo su control.

Durante 20 años, jugárselo todo a la carta de un dominio de Active Directory era una gran solución para resolver los problemas de autenticación. Sin embargo, en la nueva era de los dispositivos móviles, las contraseñas y los relojes no siempre están sincronizados, los registros DNS (sistema de nombres de dominio) a veces no están disponibles externamente y Active Directory ya no es tan viable.

Optar por sistemas y procesos de IT anticuados no es la mejor solución. Los empleados de hoy quieren poder trabajar desde cualquier sitio con garantías de seguridad y sin complicaciones.

En este contexto, ¿cómo puede eliminar la necesidad de vincular un Mac a Active Directory, pero sin sacrificar la seguridad de la cuenta? ¡Con la identidad en la nube!

Identidad en la nube: conceptos clave

Sin las herramientas adecuadas, la seguridad de los dispositivos remotos está en riesgo. La forma de entender la identidad y la seguridad tiene que adaptarse a esta nueva realidad. Los proveedores de identidad en la nube, como Microsoft, Google, Okta, IBM y OneLogin, así como Security Assertion Markup Language (SAML) y Open Authorization (OAuth), marcan el camino que llevará a la culminación de esta transición.

¿Qué es la identidad en la nube?

La identidad en la nube permite al equipo de IT gestionar de forma centralizada y en remoto usuarios, grupos y contraseñas, así como acceder a aplicaciones de las organizaciones y recursos en la nube.

Teniendo en cuenta que un 81 % de las empresas utiliza varias soluciones en la nube y un 26 % gasta más de 6 millones de dólares al año en infraestructuras públicas en la nube, controlar todo lo relacionado con la identidad y la seguridad es más difícil que nunca.[4]

Por todo lo expuesto, Microsoft anima a las organizaciones a dejar de usar Active Directory en local y a empezar a confiar en la solución en la nube Microsoft Azure Active Directory.

Microsoft Azure es un servicio en la nube que permite a las empresas crear, gestionar e implantar aplicaciones en una red a gran escala y global, utilizando herramientas y entornos específicos. De hecho, el 95 % de las empresas de la lista Fortune 500 lo utiliza.[4]

Sin embargo, Microsoft Azure no es el único proveedor de identidad en la nube. Hay opciones para todos los gustos. ¿Cuál es la mejor solución para cada organización?

Jamf Connect para la integración de la identidad en la nube

Con Jamf Connect, el proveedor de identidad en la nube elegido no tiene importancia. Jamf Connect es garantía de una distribución sencilla de perfiles de datos de usuarios desde un servicio de identidad en la nube en un flujo de trabajo de Apple y ofrece, además, autenticación multifactor.
Permite tener controlados los usuarios locales con las mismas políticas y controles que ya utiliza su servicio de directorio o proveedor de identidad.
Con Jamf Connect, un usuario puede sacar su Mac de la caja, encenderlo y acceder a todas las aplicaciones aprobadas del sistema tras iniciar sesión con unas aires de cambio: nuevos procesos

para sustituir las imágenes de identidad en la nube.

Estas son las ventajas:

1. Proceso de inscripción seguro: Las técnicas de autenticación modernas garantizan que el usuario correcto esté utilizando el dispositivo antes de distribuir contenidos confidenciales a dicho dispositivo.

2. Creación de cuentas al instante: Cree cuentas locales basadas en identidades de Okta, Azure, Google Cloud, IBM Cloud y OneLogin.

¿Y sus instalaciones físicas?

La respuesta la tiene NoMAD. Exprima al máximo el potencial de sus Mac de la mano de NoMAD, una ágil solución para sincronizar cuentas en entornos que utilizan Active Directory.

Gestión de dispositivos móviles (MDM) y acceso condicional

Ahora que cada vez más organizaciones dejan de usar Active Directory en local y aumentan sus flotas de Mac, es fundamental que puedan proteger su información y, al mismo tiempo, brindar a los usuarios la increíble experiencia marca de la casa de Apple.
La integración de proveedores de identidad en la nube con Jamf Connect permite a los administradores de IT gestionar las contraseñas de los usuarios y su acceso a aplicaciones de la empresa, lo que garantiza la seguridad de la información en un mundo donde la movilidad es la norma.
Utilizando la inscripción de MDM automática, el proceso es sencillo y seguro:

1. Un usuario recibe una invitación para apuntarse a la inscripción de MDM automática.

2. Durante la inscripción, se descarga el paquete de Jamf Connect y se instala desde el servidor de MDM.

3. A los usuarios les aparece directamente la ventana de inicio de sesión de Jamf Connect. No tienen que crear su propio nombre de usuario o contraseña.

El usuario tiene el mismo nombre de usuario y contraseña para todo, lo que es garantía de una experiencia excepcional y también de un gran nivel de seguridad de la cuenta.

De hecho, si se utiliza una solución de MDM diseñada específicamente para Apple, la configuración se realiza de forma automatizada, tanto si el empleado está en la oficina como si se encuentra en otro continente.

A su servicio

Si quiere reforzar la seguridad de su entorno y reducir el número de tickets de asistencia de IT relacionados con contraseñas, hable con nosotros y le ayudaremos a descubrir un nuevo nivel de seguridad para sus dispositivos Apple.

Deje que Jamf le ayude a resolver sus problemas de autenticación.

Póngase en contacto con nosotros para empezar hoy mismo o solicite una prueba gratuita de Jamf Connect y descubra las claves de nuestras integraciones de identidad en la nube.

Contactar ahora **Solicitar prueba**

O póngase en contacto con su distribuidor autorizado de Apple para realizar una prueba gratuita de Jamf Connect.

FUENTES:
1: http://news.gallup.com/reports/199961/7.aspx#aspnetForm
2: Gartner Document #G00258742
3: https://www.ipass.com/mobile-security-report/
4: https://www.rightscale.com/lp/state-of-the-cloud

jamf

www.jamf.com

Si quiere ver cómo puede ayudarle Jamf Connect en su transición a unos flujos de trabajo más modernos, visite **www.jamf.com**.