jamf

Cómo estar seguro sin contraseña

Contraseñas, P@sswords1, P@$$word$1234!

Las contraseñas ha servido durante mucho tiempo como barrera para mantener afuera a los que no deberían tener acceso y deja entrar a los que sí. Son los guardianes de la puerta de tu dispositivo y de tus datos. Han permanecido admirablemente en la entrada de sus dispositivos y los han defendido con toda la fuerza que pueden reunir un mínimo de ocho caracteres, un número y un carácter especial.

A medida que nuestra huella digital siga en auge y el ecosistema de dispositivos crezca, las necesidades de los imparables usuarios se amplían, lo que ha hecho que el valor y la comodidad de la contraseña sean cada vez menos eficaces. Los usuarios individuales interactúan ahora con más dispositivos y apps, con más frecuencia que nunca en cualquier día determinado, y cada uno de ellos presenta una oportunidad para una ruptura de la seguridad en caso de que la contraseña se vea comprometida.

Todos los administradores de IT han visto la indeseable lista de contraseñas más utilizadas —y es indeseable— porque casi todas las interacciones que los usuarios finales tienen con sus dispositivos, y los datos de esos dispositivos, implican tener que demostrar que son quienes dicen ser.

Las 10 contraseñas más utilizadas[1]

1. 123456
2. 123456789
3. qwerty
4. contraseña
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

1. Según Cybernews.com

En este documento, analizaremos:

- Mayor seguridad frente a facilidad de uso
- Cuál es el significado "sin contraseña"
- Por qué las organizaciones deben preocuparse por los flujos de trabajo sin contraseña
- La respuesta de Jamf a los inconvenientes de las contraseñas

Mayor seguridad frente a facilidad de uso

¿Cuál es el principal problema de seguridad de las organizaciones hoy en día? ***El robo de credenciales de acceso.*** ¿Sorprendido? ¿Y qué pasa con el hecho de que **el 80% de las transgresiones de datos tienen que ver con contraseñas robadas o débiles**? Incluso con la aplicación de políticas de contraseñas más estrictas, las transgresiones a los servidores pueden exponer las contraseñas y, por tanto, la información de la empresa y de los empleados. Además, los adversarios de InfoSec son cada vez más sofisticados en su metodología y tipos de ataques. Los ataques de suplantación de identidad, las notificaciones push y los fraudes de robo de cuentas se dirigen directamente a los usuarios susceptibles, intentando obtener acceso directo a los dispositivos y a los datos críticos.

Con el tiempo, la necesidad de aumentar la seguridad ha llevado a las IT a exigir una mayor complejidad de las contraseñas y a rotarlas como solución. Aunque estas medidas añadidas ayudaron y deben considerarse "buenas prácticas", también se convirtieron en puntos de fricción en la experiencia de usuario. Muchos usuarios simplemente redujeron su carga creando contraseñas más débiles, anotando la contraseña en papel o digitalmente, e incluso escondiéndolas debajo de su teclado para que todos las encontraran. Los que sí crearon y utilizaron contraseñas complejas tuvieron sus propios contratiempos: el aumento de tíckets de asistencia debido al olvido de esas cadenas aleatorias de letras, números y caracteres.

Aunque el restablecimiento de una contraseña puede no ser el más complejo de los tíckets de asistencia a resolver, se convierte en algo tedioso para cualquier administrador de IT contratado para trabajar en objetivos de IT más importantes que la ayuda a la administración de contraseñas. Para ir más allá, cuesta dinero hacer que el equipo de IT dedique su valioso tiempo a resolver insignificantes tíckets. **El restablecimiento de una contraseña única cuesta a las empresas una media de 70 dólares**. Y cuando se suma todo el tiempo que se invierte en estos tíckets, es una cantidad de dinero asombrosamente grande para algunas organizaciones empresariales. Para el usuario final, olvidar una contraseña y tener que esperar a que se restablezca paraliza el trabajo y la productividad. Aun así, estos costos de tiempo y dinero no siempre son suficientes para que las contraseñas reciban la atención que merecen por parte de los equipos de seguridad o los usuarios.

El aumento de las necesidades de seguridad para prevenir ataques contra las empresas y proteger los datos de compañías y clientes ha hecho que aumenten los presupuestos de seguridad de las empresas. Sin embargo, las filtraciones también aumentan y la asignación de fondos destinados a prevenir las filtraciones de contraseñas comprometidas no es proporcional al problema que plantean. De hecho, **menos del 10% se destina a eliminar las credenciales comprometidas, pero es donde se origina más del 80% de las transgresiones**. Aquí es donde los flujos de trabajo sin contraseña intervienen para ayudar.

Entonces, ¿qué significa "sin contraseña"?

Para 2022, **Gartner predice que el 60% de las empresas grandes y globales, y el 90% de las medianas, implementarán métodos sin contraseña en más del 50% de los casos de uso**.

¿Por qué? Porque, por su naturaleza, un flujo de trabajo sin contraseñas para la autenticación de usuarios elimina el problema de las contraseñas débiles, alivia la fatiga de las contraseñas de los usuarios y significa que las organizaciones no necesitan almacenar contraseñas que podrían quedar expuestas y en peligro. En otras palabras, alivia casi todos los puntos conflictivos de las contraseñas físicas mencionados al principio de este artículo.

Para introducir con éxito los flujos de trabajo sin contraseña, una organización debe ofrecer a sus usuarios una forma de autenticación, o de demostrar su identidad, durante el proceso de inicio de sesión en los recursos, datos o software a los que han sido autorizados a acceder y utilizar por parte de IT. Los líderes de la seguridad y la administración de la identidad y el acceso (IAM) deben estar familiarizados con los conceptos de autenticación y autorización como punto crucial de la administración de la identidad.

Un ejemplo de método de autenticación es un sistema de tarjetas inteligentes. Una tarjeta inteligente es una tarjeta física, parecida a una tarjeta de crédito que alberga claves criptográficas vinculadas directamente a un usuario y se utiliza como método seguro de autenticación. El problema es que la implantación de estos sistemas lleva mucho tiempo, son muy caros y suponen una pieza adicional de hardware que el usuario final debe manejar. A menos que su organización sea un caso de uso de alto riesgo, el costo y el potencial de que los usuarios finales pierdan o averíen la tarjeta inteligente suelen superar la amenaza potencial, lo que hace que ese nivel de seguridad sea innecesariamente excesivo.

¿Qué es la autenticación de varios factores (MFA)?

La autenticación de varios factores (MFA) es un proceso de autenticación que requiere que el usuario proporcione dos o más factores de verificación para obtener acceso a un recurso. Este podría ser un PIN en el teléfono de un usuario, **FaceID**, verificación de huellas dactilares o algunas otras opciones.

El ejemplo más común con el que la gente está familiarizada cuando se trata de la ausencia de contraseña es el uso de la biometría. Face ID y Touch ID son ejemplos que todo usuario de Apple conoce. La biometría permite que un usuario se autentique sin necesidad de introducir una contraseña, o de requerir una pregunta secreta o un reto basado en un conocimiento que pueda ser robado o adivinado. Tu cara es tu cara, y tu pulgar es tu pulgar: son difíciles de robar. Si se añade el requisito de un PIN variable, la eficacia de la seguridad será doble.

Ya hemos hablado de que las contraseñas ya no son la forma más segura de que las organizaciones permitan a los usuarios acceder a sus dispositivos y recursos, ni la mejor experiencia para los trabajadores que tienen que introducir contraseñas muchas veces al día. Y con el cambio de panorama hacia entornos de trabajo a distancia e híbridos, las organizaciones deben ahora considerar mejores medidas de seguridad que tengan en cuenta la experiencia de usuario final. Veamos cómo la transformación digital está impulsando la necesidad de que las organizaciones implementen flujos de trabajo sin contraseña.

¿Qué es la autenticación sin contraseña?

La autenticación sin contraseña es un método de autenticación en el que un usuario puede iniciar sesión en un sistema informático sin necesidad de introducir una contraseña o cualquier otro secreto basado en el conocimiento

¿Qué es la autenticación basada en certificados?

La autenticación basada en certificados es el uso de un certificado digital para identificar a un usuario, máquina o dispositivo antes de concederle acceso a un recurso, red, aplicación, etc.

¿Por qué las organizaciones deben preocuparse por la ausencia de contraseñas?

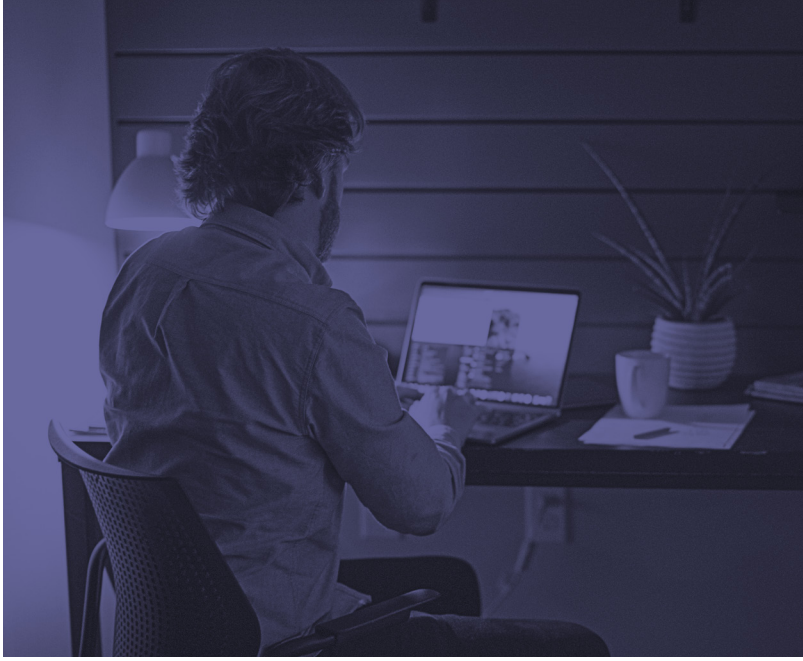
Si las vulnerabilidades de seguridad asociadas a las contraseñas que se han esbozado brevemente en el inicio de este documento no han sido suficientes para convencerle de que se una al movimiento hacia los flujos de trabajo sin contraseña, profundicemos un poco más en la transformación digital y en el efecto que tienen las contraseñas.

Trabajadores a distancia

El cambio al trabajo a distancia e híbrido ha acelerado la urgencia de la autenticación sin contraseña, ya que se está poniendo más énfasis en proporcionar una excelente experiencia de usuario y seguridad a distancia. Un componente importante es que los usuarios finales se conecten remotamente. Los usuarios pueden ir a cualquier parte —a casa, a la oficina, a una cafetería, al parque— para acceder a sus dispositivos y recursos, lo cual es flexible y cómodo, pero también conlleva el riesgo añadido de estar fuera del perímetro corporativo. Los usuarios pueden estar en redes no seguras, lo que abre agujeros en la capa de seguridad y hace más probables los ataques. Una forma fácil de reducir los riesgos de amenazas es un flujo de trabajo limpio y confiable sin contraseña para acceder a todo lo que necesita un usuario. Ya no hay que introducir contraseñas que se puedan robar y menos tíckets de asistencia: la seguridad se une a la eliminación de la fatiga de las contraseñas.

El trabajo está en la nube

La computación en nube ha cambiado el mundo, y adoptarla es sin duda un componente clave en la mayoría de las infraestructuras informáticas modernas. Dado que el perímetro corporativo local está cayendo y las organizaciones se están trasladando a la nube, su estrategia de administración de la identidad debe seguir el mismo camino. Las apps y los recursos están por todas partes en la nube. Las IT necesitan encontrar una forma segura de dar acceso a sus trabajadores y mantenerlos productivos, de modo que la ausencia de contraseñas puede ayudar a proporcionar un acceso seguro y sin contratiempos a la nube y a todas las apps que haya en ella.



Reducción de los costos de la administración de contraseñas

Según el Foro Económico Mundial, los empleados de todo el mundo dedican una media de 11 horas al año a introducir o restablecer contraseñas. Multiplique eso por el número de empleados que tiene en su organización y notará que es una enorme cantidad de tiempo desperdiciado en la administración de contraseñas. Aunque la implantación de una nueva solución tiene un costo, éste palidece en comparación con el derroche de horas de tediosos reajustes de contraseñas y una fuerza laboral desenfocada.

Promueve el aumento de la productividad

Al dedicar menos tiempo a la administración de contraseñas, los empleados y los trabajadores pueden dedicar más tiempo a sus tareas, con un acceso sin trabas a los recursos que están autorizados a utilizar, y una jornada laboral más productiva. No sólo se reducen los costos con menos gestión de contraseñas y dolores de cabeza relacionados con la seguridad asociados a los riesgos de las contraseñas, sino que la mejora de la productividad de los empleados también encabeza el aumento de los ingresos.

Estos son sólo algunos ejemplos adicionales de cómo algo como las contraseñas, un aspecto que muchos han pasado por alto durante años o que han aceptado como "suficientemente bueno", puede afinarse y mejorarse para contribuir a la estrategia global de seguridad de la empresa, a sus resultados y a su bienestar financiero. No es difícil entender por qué muchos ven los flujos de trabajo sin contraseña como un componente clave de sus planes de transformación digital.

La respuesta de Jamf a los inconvenientes de las contraseñas: Jamf Unlock

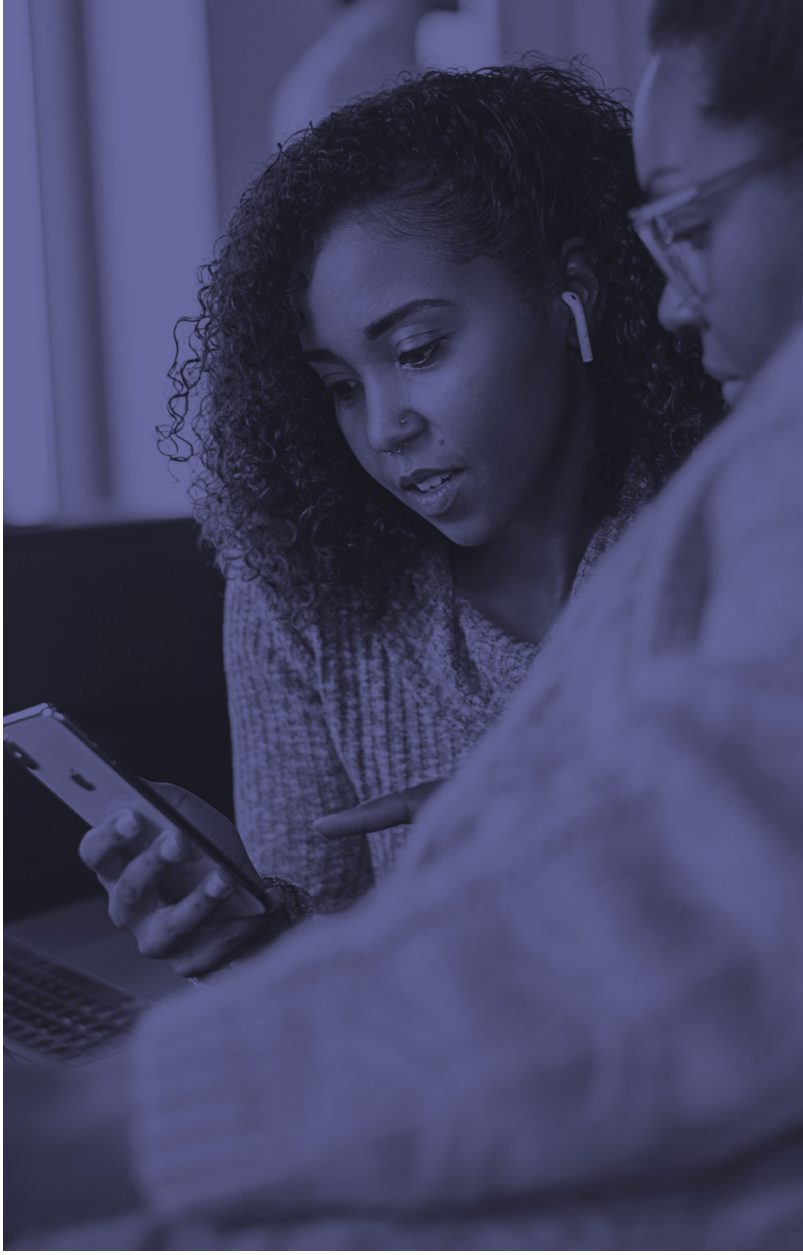
En lugar de depender de un costoso hardware no administrado, como las tarjetas inteligentes, Jamf Unlock —una característica integrada de Jamf Connect— proporciona un flujo de trabajo sin contraseña en el dispositivo que los usuarios siempre tienen —su iPhone— para desbloquear de forma segura su Mac y proporcionar un proceso de inicio de sesión y autenticación más seguro con una experiencia de usuario final sin problemas. El flujo de trabajo de Jamf Unlock satisface las necesidades de autenticación del sistema Mac con un autenticador que se ejecuta en el dispositivo iOS del usuario en lugar de introducir la contraseña en su Mac.

1. Los usuarios abren la app de iOS Jamf Unlock en su iPhone e inician la primera sesión con sus credenciales de identidad en la nube.
2. A continuación, los usuarios emparejan su iPhone con su Mac a través de un código QR.
3. En la Mac, los usuarios introducirán su contraseña local cuando se les pida que permitan el emparejamiento del dispositivo.
4. Una vez realizdo el emparejamiento, el usuario puede empezar a utilizar la app para desbloquear su Mac de forma segura con el método requerido por IT: ya sea con biometrías con o sin un PIN variable.

Jamf Unlock aprovecha los marcos Multipeer Connectivity, CryptoTokenKit y Core Bluetooth de Apple para realizar una autenticación inalámbrica basada en certificados entre un dispositivo móvil de un usuario y su Mac.

Aumente su seguridad y vaya un paso más allá con Private Access: Unlock es sólo una parte de la seguridad de los datos y recursos. Jamf Private Access —una verdadera solución de acceso a la red de confianza cero (ZTNA)— garantiza que, una vez que el usuario se autentifica en su dispositivo, las conexiones de la empresa son seguras.

Más información sobre Private Access



Los flujos de trabajo sin contraseña van a evolucionar indudablemente, pero sólo deberían ser un componente de una estrategia moderna de identidad y seguridad. Jamf Unlock es un componente de Jamf Connect para Mac que ofrece a las organizaciones un aprovisionamiento de cuentas justo a tiempo, capacidades de **gestión de la identidad** y una única identidad en la nube para acceder al Mac y a los recursos. Al integrarse con un proveedor de identidad en la nube, Jamf Connect permite al departamento de IT gestionar de forma remota los datos asociados a la identidad de cada usuario final y el software y los recursos autorizados a su cuenta. Esto no sólo aumenta la seguridad, sino que simplifica el aprovisionamiento de cuentas y permite a los usuarios abrir su nuevo Mac, encenderlo y obtener acceso seguro a todo desde el primer momento.

Esté más seguro hoy mismo

Ni qué decir tiene que el entorno laboral está en constante evolución, pero esa evolución viene acompañada de desafíos y oportunidades. Los avances, como las fuerzas de trabajo móviles y remotas, pueden abrir la puerta a los atacantes y a los hackers en busca de oportunidades para realizar acciones nefastas, pero también están dando lugar a flujos de trabajo y soluciones creativas para los administradores de IT, InfoSec y usuarios finales.

Aunque la InfoSec siempre tenga una mentalidad de "seguridad primero", se enfrentará constantemente al reto de equilibrar esa prioridad con los deseos y necesidades de sus usuarios finales, que están mucho más centrados en su propia experiencia de interacción con sus dispositivos a diario. Los usuarios finales no quieren flujos de trabajo laboriosos ni medidas de seguridad que les ralenticen enormemente y, aunque la mayoría de los usuarios entienden la importancia de la seguridad de los datos, esa comprensión sólo llega hasta cierto punto.

La facilidad de integración de Jamf Unlock con los flujos de trabajo existentes beneficia al usuario final y a los equipos de InfoSec/IT en este sentido. Y aunque los actores nefastos siempre tratarán de transgredir sus datos, la implementación de un flujo de trabajo sin contraseña utilizando Jamf Unlock y Jamf Connect, es una victoria fácil cuando se trata de proporcionar una capa adicional de seguridad con una gran experiencia de usuario final que mitiga el riesgo que los impostores pueden llevar.

La implantación de un entorno sin contraseñas debe ser un proceso bien pensado para cualquier organización, como la mayoría de los planes de seguridad, pero es una mejora que hace avanzar a cualquier organización y ofrece una oportunidad de crecimiento. Hay que centrarse en simplificar el proceso y ahorrar en gastos generales, no en incorporar hardware innecesario y añadir más costos. Eso es exactamente lo que Jamf Unlock demuestra y precisamente por eso es el mejor método para asegurar el Mac de su organización.

Contáctenos, o póngase en contacto con su distribuidor Apple, para poner en práctica las capacidades de administración de identidades y sin contraseña de Jamf Connect en su organización.