MobileIron Access:

Una plataforma de seguridad sencilla e inteligente para la nube corporativa

En los últimos años, el mercado para las tecnologías móviles y en la nube ha cambiado por completo el comportamiento de los usuarios de las empresas. Ahora es posible trabajar desde cualquier lugar y dispositivo, y acceder a las aplicaciones y a los datos corporativos desde aplicaciones móviles y servicios en la nube. La seguridad estática, delimitada por un perímetro, ya no da abasto con todos los puntos de conexión, los usuarios, las aplicaciones y los datos que llegan más allá del firewall de la empresa. Depender de un enfoque de seguridad anticuado, como el control del acceso solo mediante contraseñas, ya no es suficiente para segurizar esta vasta infraestructura móvil en la nube, especialmente si tenemos en cuenta que el robo de credenciales de usuarios fue la primera causa de las filtraciones de datos en 2017.

El robo de credenciales de usuarios fue la primera causa de filtraciones de datos en 2017.

Verizon, *Informe de investigaciones sobre filtraciones de datos de 2018*

MobileIron

401 East Middlefield Road

Mountain View, CA 94043 (EE. UU.)

Tel. +1 650 919 8100

Fax +1 650 919 8006

info@mobileiron.com

MKT ES-ES v3

En la era de los equipos PC bloqueados y controlados por el departamento informático, las contraseñas por sí solas podían proporcionar suficiente autenticación para los recursos back-end. Sin embargo, en el mundo de la movilidad en la nube, las contraseñas resultan inadecuadas por los siguientes motivos:

Las contraseñas no son seguras.

A menudo, los usuarios adoptan hábitos peligrosos al crear contraseñas para que sean más fáciles de recordar. Por ejemplo, crean contraseñas débiles, las escriben en notas adhesivas o, incluso, no se dan cuenta de que han sido víctimas de phishing.

El uso de contraseñas no es óptimo.

Escribir las credenciales en las pantallas pequeñas de los dispositivos varias veces al día es perjudicial para la productividad. No solo lleva mucho tiempo, sino que a menudo los usuarios olvidan sus credenciales o las teclean mal las suficientes veces como para que se bloquee el acceso a sus cuentas. Entonces hay que llamar al servicio técnico para que restauren el acceso, lo que a su vez conlleva aún más tiempo de inactividad.

Las contraseñas no son inteligentes ni tampoco son conscientes del entorno del usuario.

Desde el punto de vista informático, las contraseñas no aportan ninguna información sobre el punto de conexión, la aplicación ni la red que se han utilizado para acceder a los datos corporativos. El uso de contraseñas tampoco permite discernir si el dispositivo ha sido sometido a un *jailbreak* o está ejecutando aplicaciones maliciosas en redes inalámbricas comprometidas. Esta falta de visibilidad y de control pone en riesgo los datos corporativos.

Un acceso seguro a la nube exige más que contraseñas

Para proteger el acceso a las aplicaciones y datos basados en la nube, las organizaciones necesitan una solución que sea sencilla para el usuario y lo suficientemente inteligente como para adaptarse a entornos complejos. Para satisfacer estos requisitos, una solución real de seguridad en la nube debería proporcionar:

- **Autenticación multifactorial (MFA):** debido a que las contraseñas se pueden *hackear*, se pueden perder o pueden ser robadas fácilmente, la MFA garantiza que solo los usuarios verificados puedan acceder a las aplicaciones y a los datos corporativos.
- **Inicio de sesión único (SSO) sin contraseñas:** las contraseñas son engorrosas. Sustitúyalas por un proceso de inicio de sesión seguro que ofrezca una autenticación lo más fácil y fluida posible para el usuario.
- **Potente motor de confianza:** el departamento informático necesita un motor de confianza que aproveche la posición de los dispositivos y de las aplicaciones, la identidad de los usuarios y su ubicación, entre otros datos, para garantizar que solo los usuarios, los puntos de conexión y las aplicaciones de confianza puedan acceder a los servicios corporativos en la nube.

Por qué se quedan cortos los enfoques tradicionales

En la actualidad, en el mercado hay disponibles distintas soluciones que ayudan a las organizaciones a resolver cuestiones puntuales del reto de la seguridad móvil en la nube, pero no ofrecen la plataforma integral necesaria.

Administración de identidades y acceso (IAM)

Las soluciones de administración de identidades y acceso (IAM) se centran principalmente en la administración de la identidad y el control del acceso. Si bien permiten un control del acceso a los servicios en la nube basado en la identidad, tienen una capacidad limitada a la hora de permitir o denegar el acceso basándose en la posición del dispositivo o de la aplicación.

Administración de dispositivos móviles (MDM)

La administración de dispositivos móviles (MDM) se centra en segurizar los dispositivos móviles. Cabe destacar que no todos los proveedores de MDM abordan la seguridad en la nube de forma adecuada. Muchos de ellos también carecen de controles adecuados para bloquear el acceso no autorizado a los servicios corporativos en la nube, tales como Office 365 y Salesforce.

Agentes de seguridad para el acceso en la nube (*Cloud access security brokers*, CASB)

Los CASB aportan visibilidad, un control del acceso pormenorizado en cinco niveles y seguridad de los datos para los servicios en la nube. Sin embargo, están muy limitados en lo que se refiere a la creación de perfiles en los dispositivos, el análisis de su posición y a la hora de impedir el acceso por parte de dispositivos que no cumplen la normativa o de aplicaciones no autorizadas a servicios corporativos en la nube.

Aunque es cierto que, por lo general, estas soluciones desempeñan sus funciones individuales bien, son soluciones aisladas difíciles de integrar, lo que da lugar a brechas de seguridad que hacen que los datos corporativos sean vulnerables.

MobileIron Access:
Una solución sencilla e inteligente para la seguridad móvil en la nube

Las organizaciones que utilizan los servicios corporativos en la nube, como Box, G Suite, Office 365 y Salesforce, tienen que proporcionar un control de acceso condicional a todos estos servicios. MobileIron Access ayuda a establecer una confianza de base en el entorno del usuario basándose en una serie de factores, como el dispositivo, la aplicación, la red, la ubicación y el usuario. Esto permite que entonces el departamento informático aplique la política adecuada para adaptar el riesgo actual a la sensibilidad de los datos a los que se está accediendo. En otras palabras, Access puede habilitar un SSO sin contraseña si el riesgo es relativamente bajo o requerir una MFA si el riesgo es mayor. Por ejemplo, si el director de marketing quiere acceder a documentación confidencial sobre el lanzamiento de un nuevo producto usando la conexión Wi-Fi de un aeropuerto, Access podría requerir la MFA como parte de la respuesta de seguridad a la solicitud del usuario.

Las siguientes prestaciones permiten que las organizaciones adopten con tranquilidad las tecnologías móviles en la nube y reducen el riesgo de que se filtren datos.

Aplicación MFA fácil de usar

MobileIron Authenticator es una sencilla aplicación de MFA que reemplaza los caros y engorrosos tokens físicos por una solución MFA móvil que es rentable y fácil de usar. También ayuda a prevenir el uso indebido de las credenciales corporativas de un empleado en caso de robo.

Configuración con un solo toque

Authenticator es extremadamente fácil de configurar a través de la plataforma de MobileIron, lo que elimina los confusos códigos QR y las guías de configuración. El usuario solo tiene que iniciar Authenticator para activar la aplicación con un solo toque. Una vez que la activación ha finalizado, el usuario está listo para comenzar a verificar los intentos de inicio de sesión en su smartphone configurado.

Notificaciones push

MobileIron Authenticator envía notificaciones instantáneas a los teléfonos móviles administrados de los usuarios, lo cual les ofrece un método fácil y rápido para empezar a aprobar los intentos de inicio de sesión.

Autenticación adaptable

MobileIron Authenticator proporciona flujos de autenticación inteligentes que se adaptan en función de los distintos datos que reciben, incluidos la posición del punto de conexión, la aplicación, la red y la ubicación del usuario.

Experiencia nativa de inicio de sesión para puntos de conexión modernos

MobileIron Access ofrece prestaciones de inicio de sesión que permiten la autenticación de los usuarios sin que tengan que introducir ninguna contraseña cuando se está usando una aplicación y un punto de conexión autorizados.

Experiencia móvil SSO nativa

Access permite que los usuarios se conecten de manera segura a los servicios corporativos a través de aplicaciones móviles nativas sin tener que autenticar sus credenciales previamente mediante otra aplicación o portal SSO.

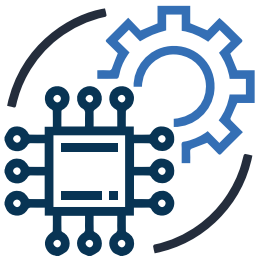
Verificaciones de la posición e inicio de sesión inteligente

Access incluye verificaciones de la posición que tienen en cuenta el contexto, lo cual es una prestación de la que carecen las soluciones de SSO tradicionales. Dichas verificaciones de SSO comprueban la identidad del usuario, así como el estado y la posición del punto de conexión y de la aplicación. Si un punto de conexión o aplicación no autorizados intentan iniciar sesión, el usuario recibe un flujo de trabajo con pasos fáciles para poner remedio a la situación.

SSO fluido

Las políticas adaptables permiten que los usuarios se autentiquen sin necesidad de contraseñas cuando se conectan a través de aplicaciones y puntos de conexión autorizados.

Motor de confianza para las políticas inteligentes



Access también ofrece un motor de políticas consciente del entorno que le otorga al departamento informático el poder de decisión sobre el control inteligente del acceso más allá de la identidad del usuario, como puede ser mediante el dispositivo, la aplicación, el servicio, la ubicación y la red, entre otros.

Políticas adaptables

El departamento informático puede relacionar los datos en función de distintas señales y, a continuación, aplicar políticas adaptables y basadas en el nivel de riesgo que reflejen el entorno del usuario.

Flujos de trabajo de corrección de problemas intuitivos

El motor de políticas crea flujos de trabajo de corrección de problemas que ayudan a los usuarios a resolver rápidamente y por sí mismos los problemas para que puedan continuar trabajando dondequiera que estén.

Seguridad basada en estándares

Se puede segurizar cualquier servicio en la nube mediante un enfoque basado en estándares, y eso permite que las empresas puedan elegir las tecnologías móviles en la nube que necesiten para satisfacer sus crecientes necesidades.

Complejo motor de creación de informes

El departamento informático puede hacer un seguimiento de todos los puntos de conexión, las aplicaciones y los usuarios que se conectan a los servicios corporativos en la nube para identificar a los usuarios y dispositivos que estén infringiendo las políticas y tomar medidas para volver a ponerlos en conformidad.

MobileIron Access:
Una solución para asegurar la transformación empresarial basada en la nube

La adopción de las tecnologías móviles en la nube está impulsando un cambio a todos los niveles en las organizaciones de todo el mundo. Estas nuevas tecnologías permiten que las organizaciones simplifiquen los procesos corporativos, abaraten los costes y fomenten la productividad de los empleados en cualquier lugar. Sin embargo, segurizar las aplicaciones móviles y los servicios en la nube requiere una seguridad que vaya más allá de las contraseñas y los enfoques antiguos que no se diseñaron para el mundo móvil en la nube.

La empresa moderna actual exige una plataforma integral y unificada como MobileIron Access, diseñada desde los cimientos para segurizar las aplicaciones móviles, los puntos de conexión y los servicios en la nube, todo desde un único punto de control.

Obtenga más información sobre MobileIron Access en **www.mobileiron.com/access**

MobileIron Access:
Seguridad total basada en la nube

Aplicación MFA fácil de usar
Access reemplaza los caros y engorrosos tokens físicos por MobileIron Authenticator, una sencilla aplicación de autenticación multifactorial (MFA) que es fácil de configurar y de usar.

Experiencia móvil SSO nativa
Access permite que los usuarios se conecten de manera segura a los servicios corporativos a través de aplicaciones móviles nativas sin tener que autenticar sus credenciales previamente mediante una aplicación o portal SSO.

Motor de confianza
Access aprovecha la posición de los dispositivos y de las aplicaciones, la identidad de los usuarios y su ubicación, entre otros datos, para garantizar que solo los usuarios, los dispositivos y las aplicaciones de confianza puedan acceder a los servicios corporativos en la nube.

Plataforma unificada
Access es una plataforma única, fácil de implementar y unificada que ayuda a las organizaciones a proteger las aplicaciones y los datos empresariales en el mundo móvil en la nube.

Seguridad basada en estándares
Access se integra fácilmente con los mejores proveedores de identidad y puede segurizar cualquier servicio en la nube compatible con el estándar SAML 2.0, sin necesidad de dedicar tiempo a una integración personalizada.