**El auge del inicio de sesión único (SSO) y la autenticación de múltiples factores (MFA)**

La mayoría de las empresas mantienen sus datos de manera segura mediante sistemas de autenticación. Los nombres de usuario y las contraseñas son las llaves que desbloquean la información para un gran número de organizaciones. Sin embargo, ¿son suficientes estas credenciales? La seguridad de la información se enfoca en gestionar el acceso y la autorización de los usuarios a la información.

Anteriormente, aprendiste sobre los tres factores de autenticación: conocimiento, posesión e inherencia. Dos tecnologías populares para implementar estos factores de autenticación son el inicio de sesión único (SSO) y la autenticación de múltiples factores (MFA). En esta lectura, conocerás cómo funcionan estas tecnologías y por qué las empresas las están adoptando.

**Una mejor aproximación a la autenticación**

El **inicio de sesión único** (SSO) es una tecnología que combina varios inicios de sesión diferentes en uno solo. Cada vez más empresas recurren al SSO como solución para sus necesidades de autenticación debido a tres razones fundamentales:

1. **Mejora la experiencia de usuario** al eliminar la necesidad de recordar múltiples nombres de usuario y contraseñas.
2. **Permite a las empresas reducir costos** al simplificar la gestión de servicios conectados.
3. **Mejora la seguridad general** al reducir la cantidad de puntos de acceso que los atacantes podrían utilizar para infiltrarse en el sistema.

Esta tecnología surgió a mediados de la década de 1990 como una forma de combatir la *fatiga de contraseñas*, que se refiere a la tendencia de las personas a reutilizar las contraseñas en distintos servicios. Recordar muchas contraseñas diferentes puede ser un desafío, pero usar la misma contraseña repetidamente representa un importante riesgo de seguridad. El SSO resuelve este dilema al aliviar a los usuarios de la responsabilidad de autenticarse repetidamente en múltiples servicios.

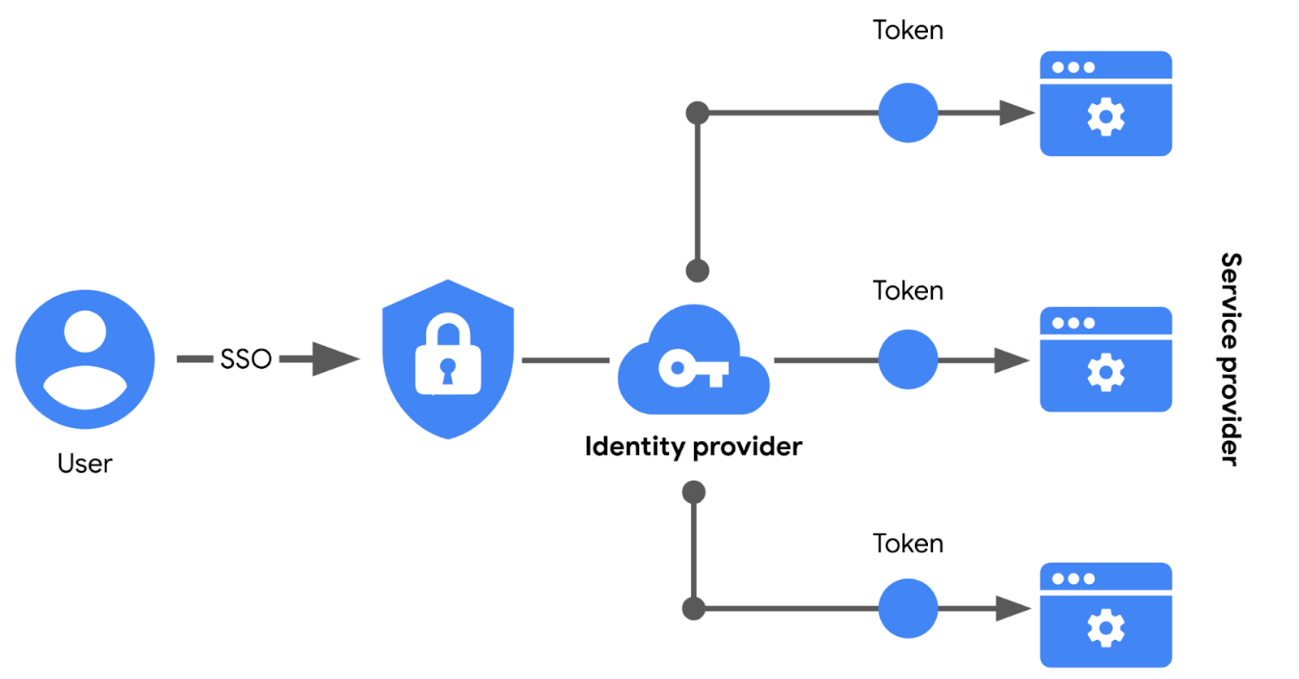
**Cómo funciona el inicio de sesión único (SSO)**

El inicio de sesión único (SSO) funciona automatizando el establecimiento de confianza entre un usuario y una empresa proveedora de servicios. En lugar de requerir que el empleado o cliente se encargue de la autenticación, las soluciones de SSO utilizan terceros de confianza para demostrar la identidad del usuario. Esto se logra mediante el intercambio de tokens de acceso cifrados entre el proveedor de identidad y el proveedor de servicios.

Estos tokens de acceso se intercambian utilizando protocolos específicos, al igual que ocurre con otros tipos de información digital. Las implementaciones de SSO suelen basarse en dos protocolos de autenticación diferentes: el Protocolo ligero de acceso a directorios (LDAP) y el Lenguaje de marcado para confirmaciones de seguridad (SAML). El LDAP se utiliza principalmente para transmitir información dentro de las instalaciones, mientras que el SAML se emplea sobre todo para transmitir información fuera del entorno local, como en servicios en la nube.

**Nota:** Los protocolos LDAP y SAML suelen utilizarse juntos.

Este es un ejemplo de cómo el SSO puede conectar a un usuario a múltiples aplicaciones con un token de acceso:



**Limitaciones del inicio de sesión único (SSO)**

La autenticación mediante nombres de usuario y contraseñas por sí sola no siempre es la forma más segura de proteger la información confidencial. Si bien el inicio de sesión único (SSO) ofrece ventajas útiles, aún existen riesgos asociados con el uso de una única forma de autenticación. Por ejemplo, si se pierde o roba una contraseña, podría exponerse información en múltiples servicios. Afortunadamente, existe una solución a este problema.

**La autenticación de múltiples factores (MFA) al rescate**

**La autenticación de múltiples factores, o multifactor,** (MFA) requiere que un usuario verifique su identidad de dos o más formas para acceder a un sistema o red. En cierto sentido, la MFA es similar al uso de un cajero automático para retirar dinero de la cuenta bancaria. Primero, insertas una tarjeta de débito en la máquina como forma de identificación. Luego, ingresas tu número PIN como segunda forma de identificación. Ambos pasos o factores se combinan para verificar tu identidad antes de obtener la autorización para acceder a la cuenta.



**Refuerzo de la autenticación**

La autenticación de múltiples factores (MFA) se basa en los beneficios del inicio de sesión único (SSO) y funciona al requerir que los usuarios demuestren que son quienes dicen ser. Para autenticar su identidad, el usuario debe proporcionar dos factores (2FA) o tres factores (3FA). El proceso de MFA solicita que se brinden las siguientes pruebas:

* **Algo que el usuario conoce:** un nombre de usuario y contraseña, generalmente.
* **Algo que el usuario tiene:** típicamente proporcionado por una empresa proveedora de servicios, como un código de acceso de un solo uso (OTP) enviado a través de SMS.
* **Algo que el usuario es:** se refiere a las características físicas de una persona, como sus huellas dactilares o escaneos faciales.

Requerir múltiples formas de identificación es una medida de seguridad efectiva, especialmente en entornos en la nube. Puede ser difícil para las empresas en la nube asegurarse de que los usuarios que acceden a sus sistemas de forma remota no sean agentes de amenaza. La MFA puede reducir el riesgo de autenticar a usuarios incorrectos al requerir formas de identificación difíciles de imitar o forzar mediante ataques de fuerza bruta.

**Conclusiones clave**

Implementar tanto los controles de seguridad inicio de sesión único (SSO) como la autenticación multifactor (MFA) mejora la seguridad sin comprometer la experiencia de usuario. Confiar únicamente en las contraseñas representa una importante vulnerabilidad. Al emplear el SSO se reducen los puntos de entrada, pero esto no es suficiente. La combinación de SSO y MFA se convierte en una forma efectiva de proteger la información, permitiendo a los usuarios tener una experiencia optimizada mientras se mantiene alejada a cualquier persona no autorizada del acceso a información importante.