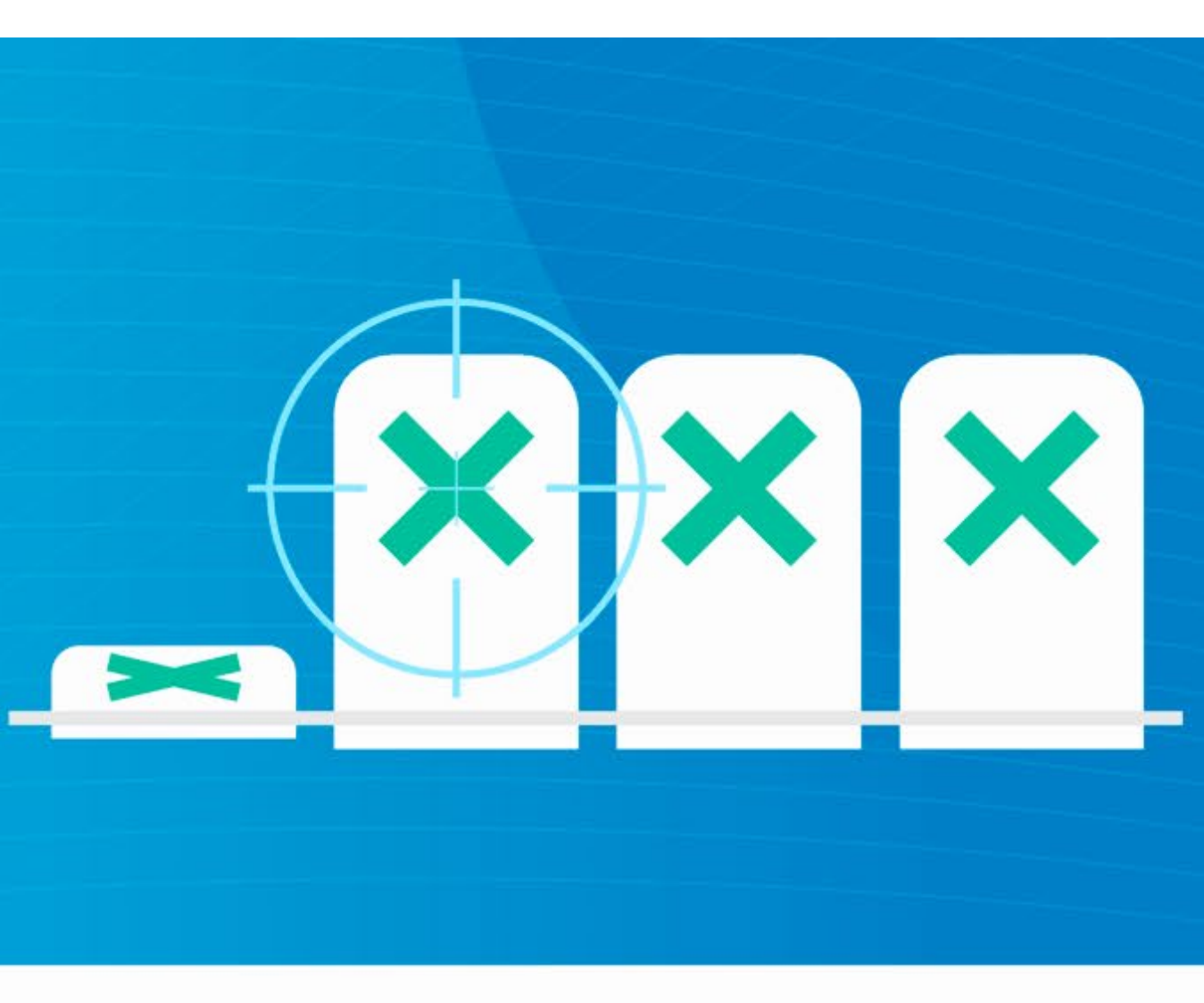
Inicio de sesión único: cuatro mitos habituales desmentidos

El inicio de sesión único (SSO) es la piedra angular de cualquier estrategia IAM que se precie, pero la gente suele confundirse con lo que realmente puede ofrecer al departamento de tecnología informática y a toda la empresa.

Inicio de sesión único: **cuatro mitos habituales desmentidos**



Cada vez más empresas se dan cuenta del valor del inicio de sesión único (SSO).

En una encuesta reciente sobre el SSO llevada a cabo por Okta, se observó que:

88 %
de las empresas encuestadas ya han incorporado alguna solución de SSO.

95 %
de los responsables de la toma de decisiones de tecnología informática encuestados consideran al SSO una parte muy importante de su pila de tecnologías informáticas.

20
aplicaciones que suele proteger una solución de SSO, llegando, en algunas empresas, a proteger más de 30.

Pese a su valor más que evidente, siguen existiendo algunos mitos sobre el SSO. Echemos un vistazo a algunos de los más frecuentes.

El mito
El SSO es caro

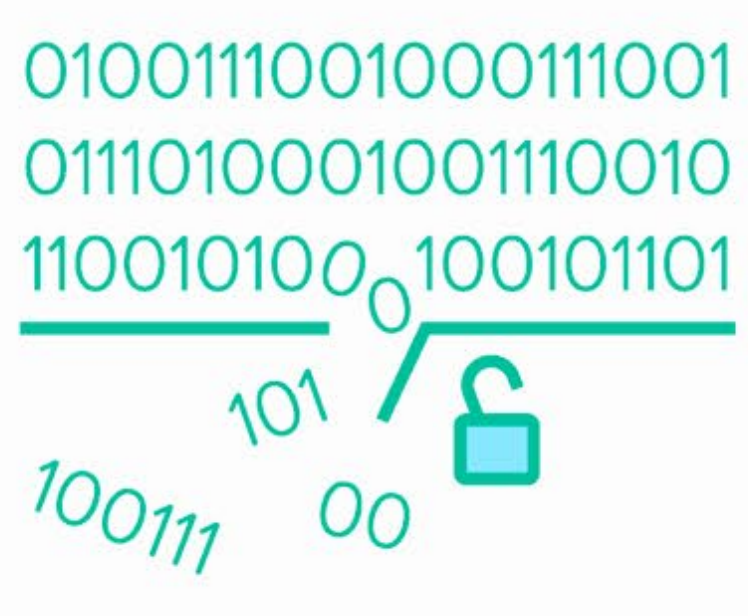
Algunos responsables de la toma de decisiones de tecnología informática siguen pensando que el SSO no es una herramienta fundamental y que el coste adicional no merece la pena.
Sin embargo, lo que sí merece la pena es consultar los costes de *no* usar el SSO.

La realidad

Cuando las empresas *no* adoptan una solución de SSO:

El departamento de tecnología informática invierte la mayoría de su tiempo en gestionar solicitudes de restablecimiento de contraseñas. En promedio este departamento gasta 8 USD por cada una, lo que se incrementa con rapidez a medida que la organización se expande.[1]

Los empleados se frustran al tener que gestionar numerosas credenciales, lo que reduce su productividad y frena a la empresa. Las empresas pierden 10 USD en productividad por cada empleado que tenga que restablecer su contraseña, lo que ocurre una vez al año en promedio.[1]



Se exponen a un riesgo mayor de sufrir un pirateo. El coste medio de las vulneraciones de datos es de 7,9 millones de dólares en EE. UU.[2] y el 81 % de ellas da lugar al robo de credenciales,[3] lo que se puede reducir de manera significativa con el SSO.

El mito
El SSO crea un único punto de fallo

Dado que el SSO proporciona una única contraseña para todas las aplicaciones, hay quienes lo critican a menudo por crear un único punto de fallo: así, los piratas informáticos solo tienen que robar una contraseña en lugar de varias.

La realidad

Ya existe un único punto de fallo: el usuario. Las personas suelen reutilizar contraseñas sencillas en varias cuentas, de manera que los piratas informáticos podrían acceder a numerosas cuentas con una sola combinación de credenciales.

Lo que hace el SSO moderno, en realidad, es eliminar este punto único de fallo con medidas adicionales de seguridad, como la herramienta de autenticación multifactor (AMF):

El SSO permite al departamento de tecnología informática instaurar políticas que aseguren que todas las contraseñas:

- **Expiren** transcurrido un tiempo determinado.
- **Difieran** de las anteriores.
- No coincidan con las **credenciales robadas**.
- **Se bloqueen** tras una serie de intentos fallidos.

El SSO tiene en cuenta el contexto de una solicitud de inicio de sesión y considera:

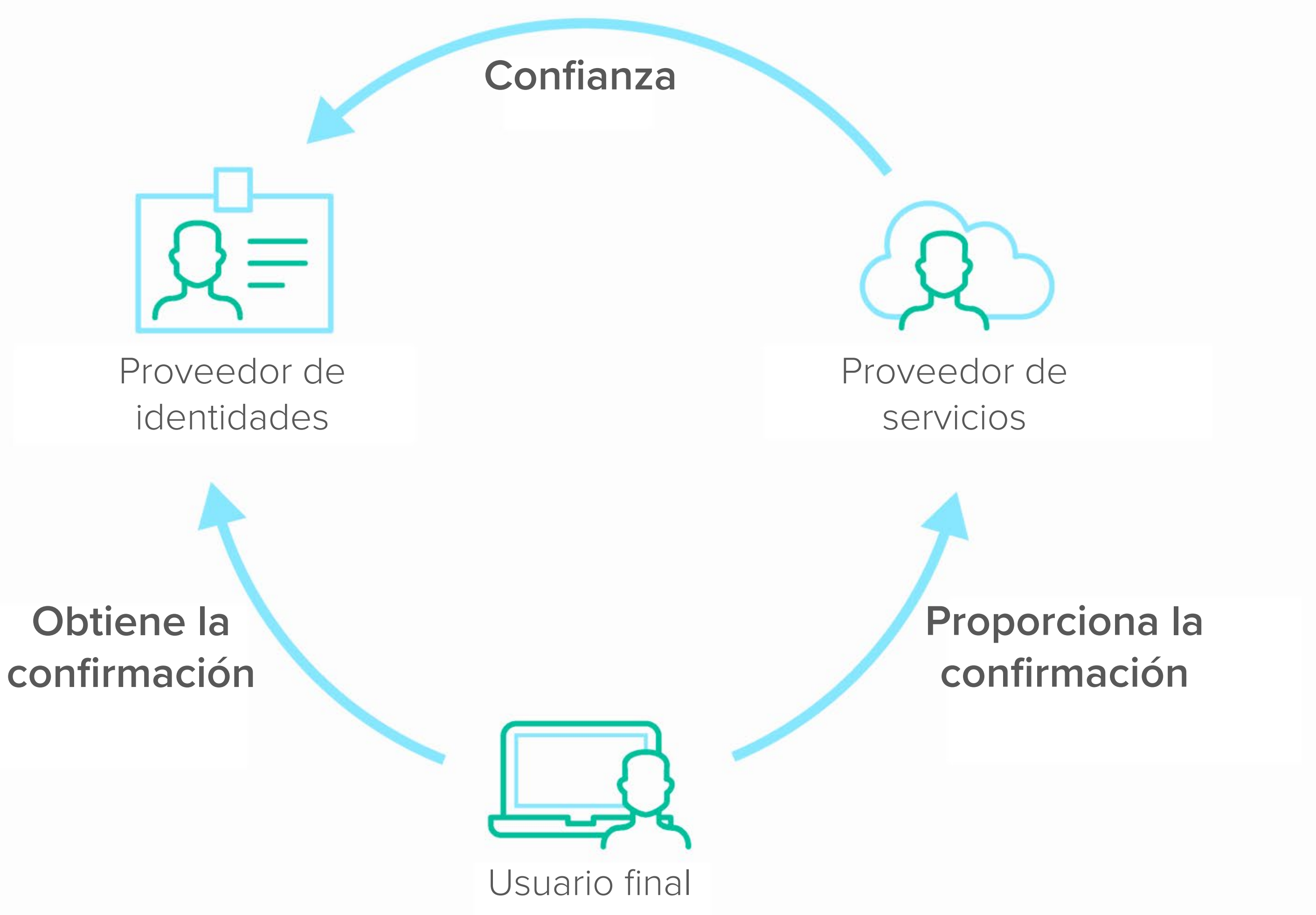
- ¿A qué **aplicación** se está intentando acceder?
- ¿De qué **grupo** forma parte el usuario?
- ¿Cuál es la **ubicación** del usuario? ¿Es de confianza?
- ¿Qué **dispositivo** se está utilizando? ¿Se ha utilizado antes?
- ¿Cuál es la **IP** del usuario? ¿Resulta sospechosa?

El mito
El SSO es igual que un administrador de contraseñas

Al proporcionar el SSO una única contraseña que permite acceder a distintas aplicaciones, a veces, puede resultar parecido a un administrador de contraseñas.

La realidad

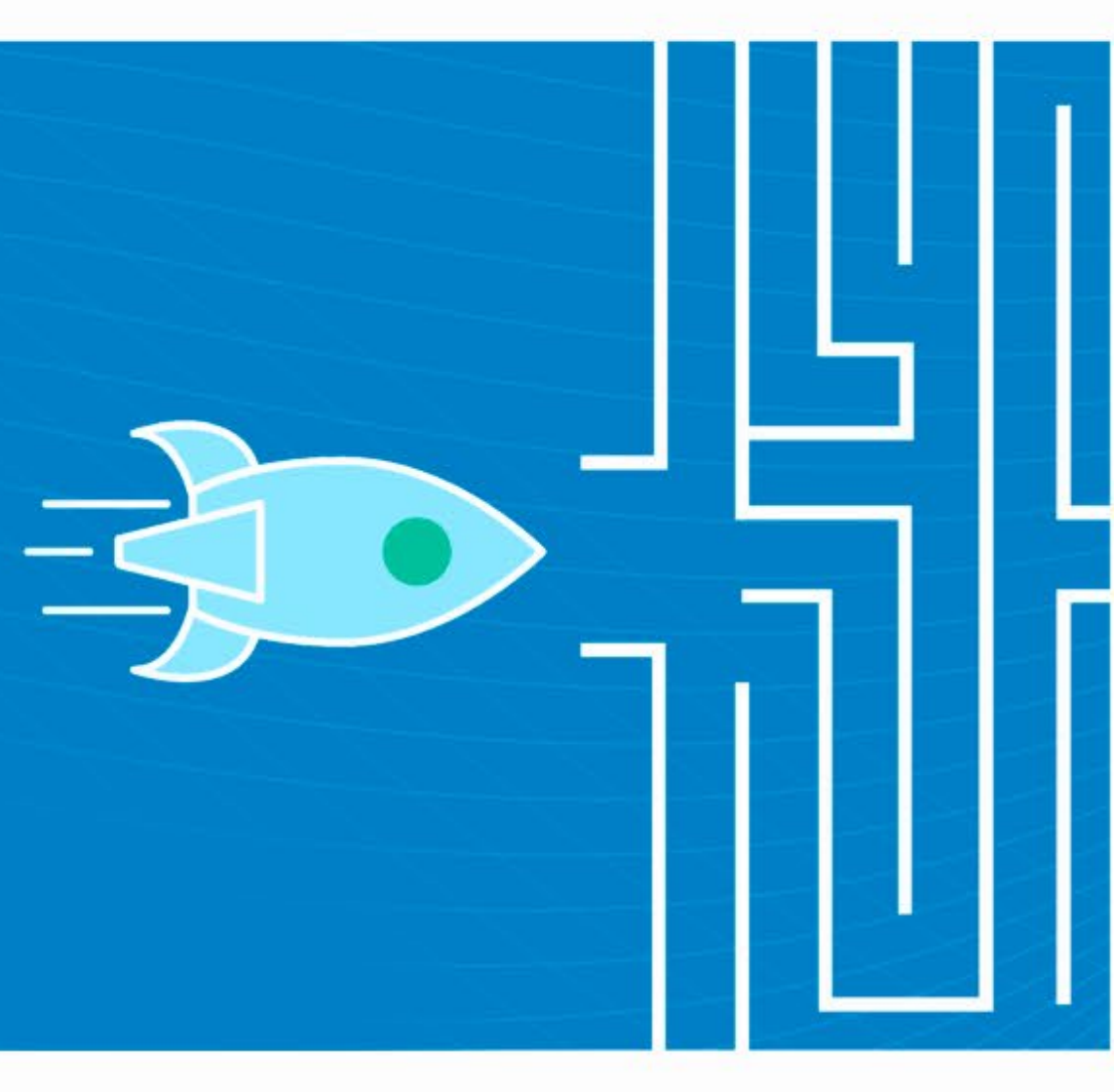
El SSO no se centra en las contraseñas, sino en el acceso. Para ello, emplea la identidad federada, es decir, el intercambio de atributos de identidad entre sistemas de confianza, pero que, por lo demás, son autónomos.



El SSO moderno utiliza protocolos de federación como SAML 2.0 y OpenID Connect. De hecho, el 91 % de nuestros encuestados afirmó que emplea estos protocolos con su solución de SSO.

Además, el SSO moderno se integra con:

El mito
El SSO es difícil de implementar



La mayoría de las empresas dependen de una infraestructura de aplicaciones locales y en la nube, lo que dificulta la implementación de una solución de SSO que abarque todo.

La realidad

Las soluciones de SSO moderno cuentan con integraciones prediseñadas para todos los recursos de la tecnología informática tanto para los locales como los de la nube, por lo que no se requieren servidores locales adicionales ni cambios en el cortafuegos.

Integraciones completas y prediseñadas para miles de las aplicaciones más usadas.

Integraciones basadas en las normativas, como SAML, OIDC y SCIM, que se pueden usar con aplicaciones locales y en la nube.

Herramientas que permiten que las aplicaciones personalizadas admitan fácilmente el SAML.

Conexión a un directorio AD o LDAP para extraer automáticamente usuarios.

Para obtener más información

Eche un vistazo a nuestros artículos del blog sobre SSO:

- Realidad o ficción: el SSO es igual que un administrador de contraseñas
- Realidad o ficción: el SSO crea un único punto de fallo
- Realidad o ficción: el SSO ralentiza al departamento de tecnología informática
- Realidad o ficción: el SSO es difícil de implementar

También puede ver nuestro seminario web:

- Lo que no sabe sobre el inicio de sesión único

O visite nuestra página sobre el SSO

okta

Fuentes

1. Forrester, Making The Business Case For Identity And Access Management, agosto de 2018
2. Ponemon 2018: https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf
3. Verizon