THE SECURITY LEADER'S GUIDE TO SSO

When security leaders think of single sign-on (SSO), they usually think of user convenience and experience. But SSO also plays a critical role in delivering security for data and applications.

Relying on passwords for user authentication is risky business. Eighty-one percent of confirmed data breaches studied in the 2017 Verizon Data Breach Report involved weak, default or stolen passwords. Yet the average enterprise employee struggles to manage 15 to 30 passwords. Not surprisingly, users frequently choose easy-to-guess passwords and store them in places where they can be easily stolen.

SSO replaces multiple usernames and passwords with one set of corporate credentials to access resources securely. By minimizing the passwords available to be pilfered, SSO decreases the chance of a security breach.

But not all SSO solutions are created equal. Some manage authentication for users accessing resources from desktops in a single security domain. Others deliver universal SSO across complex hybrid environments, boasting one-click access from any device and location to legacy on-premises applications as well as cloud-based and software-as-a-service (SaaS) apps.

This guide explores four key capabilities an SSO solution should deliver to create a true one-stop-shop authentication authority that maximizes security across complex environments.

01

FEDERATION

A key differentiator among SSO solutions is federation.

Traditionally, organizations managed their own employees' identities. They used simple SSO solutions to manage identities when all users and applications were in the same security domain. These simple SSO solutions relied on password vaulting and password replay. Vaulting stores user passwords in a directory (usually in the cloud), and password replay retrieves passwords from the vault and replays them to the application.

Federated identity management takes advantage of standards (such as security assertion markup language (SAML), OAuth2 and OpenID Connect) to securely exchange user information across partners, suppliers and customers. Federated SSO offers greater security than simple store-and-forward solutions for two reasons. First, it replaces passwords with signed assertions (or tokens), which minimize attack vectors. Second, because it's based on standards, federated SSO gives organizations control over who has access to what information and resources, regardless of where those resources reside and which type of device users choose for access.

With federated SSO, users authenticate once and then use that authenticated session to access all of the applications they're authorized to use. They can use desktops, laptops or mobile devices to sign on to mobile, SaaS and enterprise web applications. Application servers, web services and even mobile transactions can also use federated SSO to take advantage of identity information with security and auditability.

With federated SSO, users authenticate once and then use that authenticated session to access all of the applications they're authorized to use.

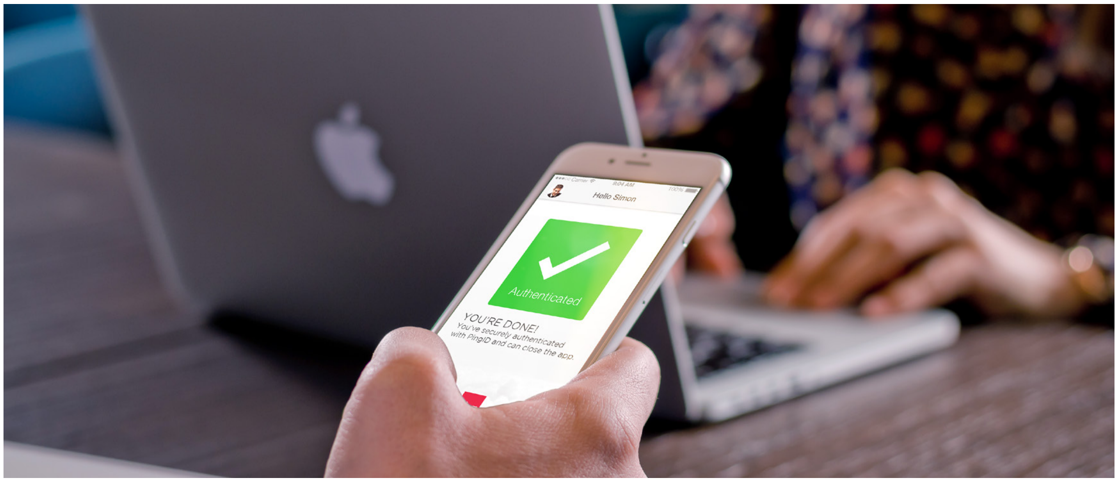
02

CONTEXT-SENSITIVE AUTHENTICATION

Every SSO process starts by verifying that users are who they say they are. While usernames and passwords are the traditional authentication method, security improves when authentication services rely on more than one factor. Factors can include two or more of the following: what you know (e.g., a PIN), what you have (e.g., a smartphone) or who you are (e.g., a fingerprint). SSO solutions that allow you to combine multiple authentication factors improve assurance that the individual attempting to authenticate is the one in question. Even if one factor is compromised, the chance that other factors are also compromised is low.

Some modern enterprise SSO solutions now provide an extensible framework for authenticating users with more than just a username and password. They provide context-sensitive authentication that allows you to create risk-based policies that look at the context as the user is authenticating and dynamically determine which authentication actions to require the user to take. Contextual data can come from a myriad of sources and include location, IP address network, and time of day to determine whether a user's identity is authentic or not.

For example, many banks authenticate users with ID and password, but they actually verify other factors like IP address, existence and status of browser cookies, and other data to determine if the user should answer additional security questions.


Hello Simon
Authenticated
YOU'RE DONE!
You've securely authenticated with PingID and can close the app.

03

AUTHENTICATION AUTHORITY

Do you apply the same authentication policies for all users attempting to access any application or service on any device—with no exceptions? The most advanced SSO solutions can play the role of the authentication authority, ensuring all users are consistently authenticated across all applications.

Having an authentication authority gives you a single point of control for creating and applying identity management policies that specify exactly how you will authenticate users as they request access to applications. When an SSO solution only works for some but not all of the applications your users access, it falls short of the role of authentication authority and dilutes control across multiple systems, weakening security and increasing administrative burden.

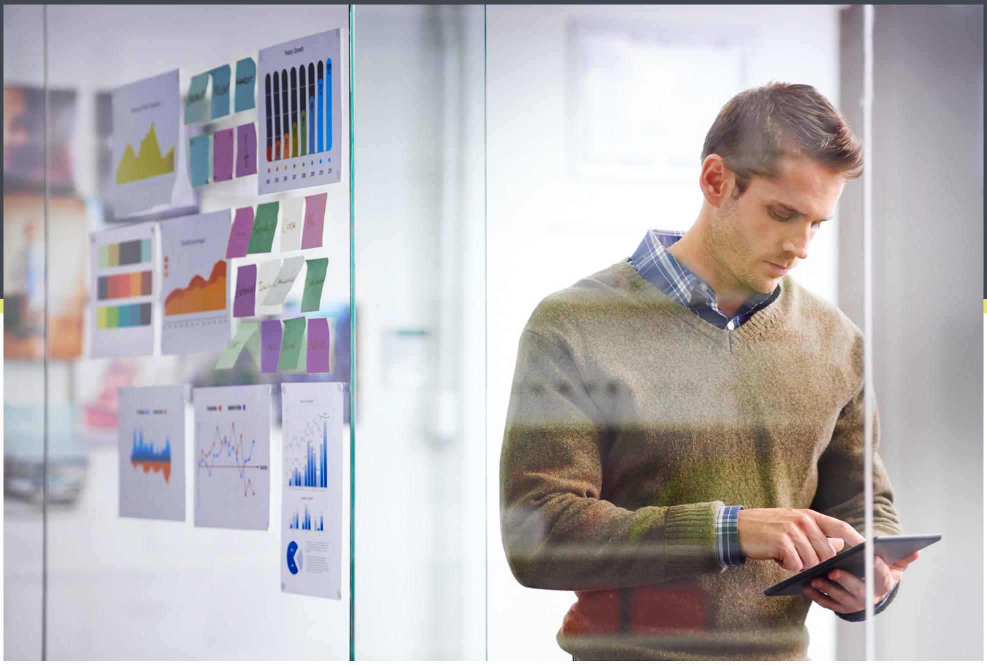
04

HYBRID DEPLOYMENT

Most SSO solutions that use SAML standards to connect to SaaS and other cloud-based solutions offer federated SSO. But legacy SSO solutions that organizations have adopted for on-premises applications may not comply with federation standards. Some large organizations may also have multiple domains with multiple SSO or federation servers.

Siloed SSO solutions leave your organization fragmented across the enterprise. Users may continue to need separate credentials for each domain, potentially leading, once again, to password proliferation. Security managers need multiple solutions for managing authentication policies, which can lead to gaps and inconsistencies. Since not every SSO solution supports contextual authentication, a consistent policy will meet the lowest common denominator—simple password protection.

A hybrid SSO deployment allows you to connect users with all applications in the cloud and on-premises giving the enterprise the control and power of in-house software and the simplicity and ease of use of a cloud service.



MOVING TOWARD UNIVERSAL SSO

Not every SSO solution is the same. They vary from simple systems that store and forward passwords to applications in a single security domain to those offering universal SSO across all types of on-prem, online, mobile and even machine-to-machine systems (yes, the Internet of Things). This guide has described what you'll need to deploy the most secure SSO across complex environments while maintaining an excellent user experience. The choice is yours on how to ensure the most appropriate level of security for your enterprise and your users.

To learn more, read our Ultimate Guide to Single Sign-on.

?

MORE INFO

Visit our website
http://pingidentity.com
To speak with a Product
Specialist in the U.S. call
toll-free 1 (877) 898-2905

ABOUT PING IDENTITY: Ping Identity leads a new era of digital enterprise freedom, ensuring seamless, secure access for every user to all applications across the hyper-connected, open digital enterprise. Protecting over one billion identities worldwide, more than half of the Fortune 100, including Boeing, Cisco, Disney, GE, Kraft Foods, TIAA-CREF and Walgreens trust Ping Identity to solve modern enterprise security challenges created by their use of cloud, mobile, APIs and IoT. Visit pingidentity.com. #3209 | 08.17 | v00c