WHITE PAPER

SSO Over the Internet:
The CISO’s Misperceptions and Realities

Ping Identity™

Executive Summary

Ping Identity conducted anonymous interviews of seventeen Chief Information Security Officers (CISOs) and Information Security Officers across financial services, healthcare, education, insurance and business services. What we learned was surprising: many of the survey participants share three common misperceptions about secure Internet single sign-on (SSO). This paper identifies those misperceptions and provides clarifications to help readers understand the realities of delivering secure Internet SSO by deploying federated identity management.

"We do not want to be a data leak story in the newspaper."

- Anonymous CISO

In an anonymous research study funded by Ping Identity, seventeen Chief Information Security Officers (CISOs) and Information Security Officers across financial services, healthcare, education, insurance and business services were interviewed to learn their thoughts about single sign-on (SSO) that works over the Internet. This paper identifies three common misperceptions that the survey uncovered and provides clarifications to help readers understand the realities of delivering secure Internet SSO by deploying federated identity management.

Clarification is provided by Patrick Harding, Ping Identity's Chief Technology Officer and former security vice president and architect at Fidelity Investments. At Fidelity he was responsible for aligning identity management and security technologies with the strategic goals of the business, and he was integrally involved with the implementation of federated identity technologies.

CISOs were interviewed regarding their perceptions about identity and access management. Specific emphasis was placed on identity federation, which allows organizations to share credentials and attributes for authentication and authorization, thus reducing the need to maintain user credentials in multiple systems. Federated identity management is a key enabler of secure Internet SSO, standards-based methods that provide users safe access to applications across the Internet without the need to re-login.

A majority of the CISOs interviewed were responsible for user management, privacy and security. Their names and organizations are not disclosed for their privacy.

Misperception #1: Federated Identity Management Projects Often Fail

When asked about identity management and their ability to provide SSO both inside of the organization and to external resources, a majority of CISOs lamented that identity and access management projects are challenging in general, especially when it comes to delivering federated identity management. Many organizations have tried to deliver federated identity management as part of an identity and access management suite deployment project, but projects failed due to the tightly-coupled nature of the suite components, incomplete functionality, steep learning curves and expensive upgrade requirements.

Reality #1: Standalone Federated Identity Management Projects are Successful

For any organization looking to provide SSO that works over the Internet, choosing a standalone software application is the best option. Vendors focused solely on delivering Internet SSO provide simplified configuration and administration without the heavy lifting of a complete identity and access management system. In addition, dedicated federated identity software vendors also offer implementation expertise and assistance that can help customers deploy secure Internet SSO in days or, at most, weeks.

For many years large incumbent vendors (sometimes referred to as stack vendors for providing a complete identity and access management stack) promised SSO that works over the Internet, but due to integration constraints and a lack of focus on identity federation, many vendor solutions are still not viable today. Large identity and access management vendors have little incentive to invest in federated identity technology. Federated identity often represents a lower-cost, easier-to-deploy method of delivering internal Web SSO than an expensive-for-the-user yet profitable-for-the-vendor Web Access Management system. Some vendors attempt to profit from federated identity by implementing products with dependencies on other components of their product lines. These vendors force organizations to purchase a complete identity and access management stack simply to provide federated identity management.

Misperception #2: Internet SSO Is Not Secure

When asked if their organizations provide SSO, a majority of CISOs responded that they have not implemented any SSO to date. Although users are demanding SSO to the applications they use on a day-to-day basis and IT organizations want to meet their needs, security is a major concern. One CISO commented on why they do not provide SSO: “Should someone hack in and there is a hole we are not aware of, [they find it]. It is more about exploiting information they should not get their hands on; we worry about that more than them corrupting the system. We do not want to be a data leak story in the newspaper.”

Many CISOs were skeptical about being able to provide SSO that works over the Internet securely, and believed implementation would be extremely difficult. While current solutions often include repeated provisioning of users and regular audits of user identities—both for enterprises and service providers—CISOs are still concerned with the secure transfer of data: “We are most vulnerable around the area of business partners where administrators make mistakes setting up access.”

"We are most vulnerable around the area of business partners where administrators make mistakes setting up access."

- Anonymous CISO

Reality #2: Standards-based Internet SSO is Secure

From an identity management perspective, the most cost-effective way to increase security is to centrally manage credentials, add strong authentication and provide SSO that leverages that strong authentication mechanism both internally, for legacy applications, and externally over the Internet.

Although a centralized point of access can be a point of attack, the truth is that today users have many passwords to access different applications, and each is vulnerable to attack. SSO eliminates the requirement for a login page for every application, thus reducing the login frequency and opportunity to expose usernames and passwords.

Internet SSO software that leverages proven standards, such as SAML and WS-Federation, relies on mature security and peer-reviewed standards. However, incorrectly-configured SSO mechanisms expose the organization to attacks due to the complexity of underlying technologies such as XML digital signatures. Furthermore, free open source SSO toolkits provide a limited subset of the specifications; organizations have to ask, "Is that enough to cover my security concerns?”

Misperception #3: Integrating with Federated Identity Management Does Not Scale

With decreasing costs and easier access to federated identity management, many CISOs see a future for SSO that works over the Internet, but they still perceive inhibitors when trying to integrate with existing identity infrastructure and target application environments. With complex infrastructures that include legacy and proprietary applications, CISOs are apprehensive to take on identity federation projects with their incumbent stack vendors due to integration costs associated with supporting complex environments. Vendor-specific identity and access management systems often integrate with a limited set of components, specifically within their own product lines; many organizations are still faced with developing custom code to integrate with other identity infrastructure elements and target application environments.

Reality #3: Standalone Federated Identity Management Software Provides Easy First and Last-Mile Integration

Federated identity management software should not be tied to a sole vendor; organizations need options to integrate with their legacy environment. A key element of providing secure Internet SSO is the ability for enterprises and service providers to easily integrate with authentication systems, identity management infrastructure and target applications. Standalone federated identity management software is not tied to a specific vendor and is designed to provide out-of-the-box integration with authentication systems, identity management systems, Web servers, application servers, commercial applications, portals and custom applications developed with PHP, .NET, and Java.

The Truth Behind Secure Internet SSO

Given the notion that SSO that works over the Internet can be secure, CISOs should recognize the benefits from both organizational as well as user perspectives. Most common are improved user productivity—through convenience and mobility—and mitigated risks associated with compromised identities and human errors in provisioning. Finally, CISOs should evaluate standalone federated identity management software that eliminates the need to install an expensive, all-inclusive identity and access management system.

About Ping Identity Corporation

Ping Identity's dedication to delivering secure Internet single sign-on software and services for over 150 customers worldwide has earned us recognition as the market leader in federated identity management. PingFederate®, the world's first rapidly deployable identity federation software, provides an organization's users safe access to Internet applications without the need to re-login. With PingFederate and PingEnable—Ping Identity's expert support, services, and methodologies—external connections can be operational in less than a week. Download a free trial at www.pingidentity.com.

PingIdentity™