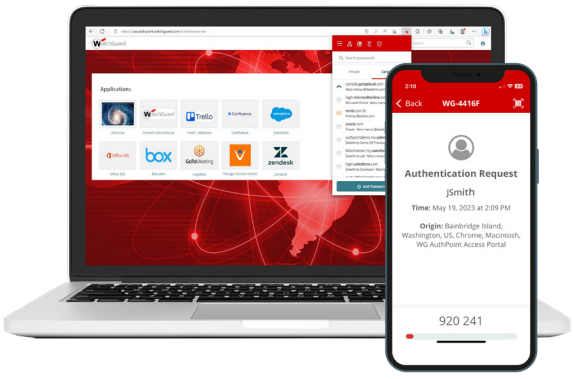
Empowering the Workforce with Seamless Single Sign-On (SSO)

Executive Summary

Access management is crucial to ensure that only authorized users can access resources and systems. Methods such as passwords, multi-factor authentication, and biometrics are used to manage access. However, these methods alone are not enough to enable secure access without compromising efficiency and user experience. Enter single sign-on (SSO) authentication.

This paper discusses the main operational challenges that organizations often encounter when managing multiple user identities, providing access for both remote and on-premises users, and dealing with an overload of password-reset tickets in the IT department. By implementing SSO, many of these issues can be resolved, enabling employees to have a seamless user experience and improving the overall management of identity security.



SSO Is Important to the Modern User Authentication Experience

Single sign-on (SSO) is an access management solution that simplifies the authentication process across multiple applications. By allowing users to access various systems with a single set of credentials, SSO eliminates the need for multiple individual logins for each application.

Deploying SSO can be a powerful move to take identity security to the next level, hassle-free. By giving users a tool to log in to multiple applications effortlessly, organizations can maintain or even increase productivity levels.

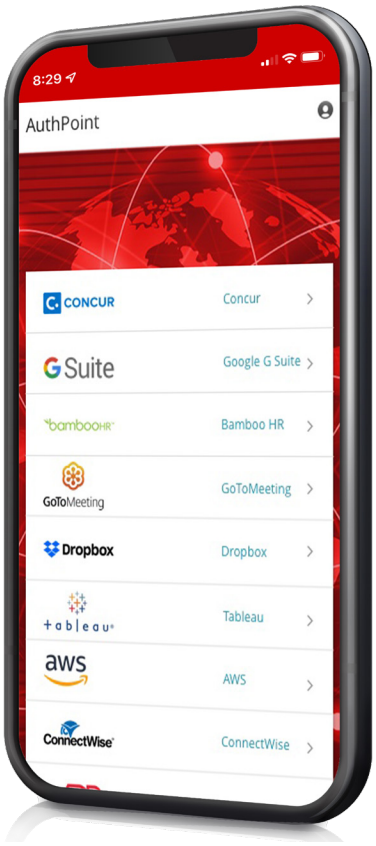
Solve Performance and Productivity Challenges

- Avoid credential-related vulnerabilities: In 2022, 74% of data breaches involved the human element, including using and losing credentials. People play the largest role when it comes to potential vulnerabilities in security.
- Address password fatigue: An average employee manages 27 passwords, from work email to CRM systems. The number of passwords can take a toll on employee productivity, leading to increased stress levels and burnout.
- Reduce password reuse: The reuse rates of passwords in the workplace are high at 61% and even worse among personal reuse rates, where it increases to 73.3%.
- Protect and empower remote employees: Hybrid work continues to rise, with more businesses allowing employees to work from the office and home.
- Deploy Cloud-based security: An estimated 68% of employees switch between ten Cloud applications every hour. Eliminating multiple logins can save a company time and money.

Adding SSO Means Comprehensive Security and Fewer Issues to Manage

Simplify Everyone's Work

With SSO, you can offer a seamless and efficient experience for accessing work applications. Users only need to remember one login credential to access all their authorized applications. This eliminates the need to remember multiple passwords, which can lead to wasted time in resetting forgotten passwords or attempting to enter login credentials manually.



Make Network Security Stronger

SSO can also lead to better-integrated security as it provides a seamless way to authenticate anyone on a network. This integration gives you more user information so you can correlate it to the traffic you're seeing on the firewall. Plus, you can enforce access control by creating firewall policies for specific groups and users.

Streamline User Onboarding and Reduce Help Desk Tickets

By implementing SSO, you can provide a convenient and secure way for new users to access all necessary resources and applications with a single set of login credentials. This streamlines the user onboarding process and reduces the need for help desk tickets. It also makes it easier to manage both new and existing users.

Boost Compliance Posture

With the growing number of regulatory requirements, such as GDPR, HIPAA, and other privacy regulations, companies must comply with specific access control measures. Single sign-on can help improve compliance by providing a centralized authentication system that is easy to audit and monitor. Additionally, SSO can be used as an extra layer of security, reducing the risk of unauthorized access to data.

Deploying SSO Can Be Super Easy (Depending Who You Work With)

SSO is built on a concept called federated identities. It enables the sharing of ID information across trusted but independent systems.

- A Service Provider: in this context, it can be an application, portal, or target system used to initiate an authentication request.
- An Identity Provider: responsible for validating user credentials via authentication requests and then granting access.
- A Token Provider: exchanges requests between the service provider and identity provider on behalf of the user to issue and validate access tokens.

Whether you run in-house or outsourced cybersecurity, single sign-on deployment can seamlessly make work better for everyone. If you have a managed service provider, they will likely have a preferred vendor. Ideally, SSO is available with your existing MFA provider.

Here are steps to implement SSO securely and efficiently:

Step 1: Assess Requirements in Your Organization

Determine the number of applications you need to connect to SSO. Understanding the type of users, their access locations, and the most commonly used resources can help in creating an SSO structure based on user groups.

Step 2: Define the Appropriate Deployment Path

Your identity provider will help determine which protocol to use for SSO configuration. Security Assertion Markup Language (SAML) and Lightweight Directory Access Protocol (LDAP) are the most commonly used protocols in this scenario, and hundreds of SAML- or LDAP-based applications can be integrated into your SSO portal.

Step 3: Evaluate User Privilege

Once your SSO infrastructure is established, ensure that appropriate access control is in place for SSO users. Implementing least-privilege access and risk policies based on user groups provides the best balance between security and user experience.

Step 4: Customize the SSO Application Portal

An SSO solution that allows customization is ideal, so your users have a smooth experience with a branded look and feel. This makes all the difference in providing the best UX experience as it tells users they are accessing a familiar and inherently trustworthy environment.

The Key to Enabling Strong Access Management

Choose a Comprehensive Identity Security Provider

A strong identity security infrastructure is in high demand. When choosing your security provider, evaluate the solutions and features that can effectively protect users, identities, data, and applications. Look for standard and advanced capabilities that address key use cases like remote/hybrid work, credentials-based data breaches, IT efficiency, and compliance.

Enforce Access Control Protocols

Single sign-on (SSO), multi-factor authentication (MFA), and user risk policies are some of the most effective tools to enforce access control protocols. SSO enables users to log in to various systems using a single set of credentials, simplifying the user experience while enhancing security. MFA adds an extra layer of verification, requiring users to provide multiple pieces of evidence to prove their identity. By adding a risk framework layer, you can evaluate user behavior and identify areas needing least-privilege access and data-breach risk monitoring, while still providing a seamless user experience.

Adjust Your Architectural Model When Needed

It may not be essential for all users to have single sign-on (SSO) access to every application they utilize, especially if providing SSO connectivity to a rarely used or soon-to-be-replaced app would be costly. Apply the principle of 80/20.

Conclusion

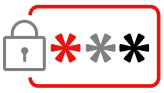
Start Leveraging SSO Today

Build a secure and easy-to-work-in work environment. No more juggling numerous passwords for different accounts and applications. SSO provides a seamless login experience. This empowers your users with productivity, eliminates time-consuming authentication hassles, and simplifies user account management. Upgrade user login experiences today with SSO and unlock a world of efficiency and enhanced protection.

About AuthPoint Identity Security

Mitigate the risks associated with widespread workforce credential attacks.

Multi-Factor Authentication (MFA): With offline and online authentication methods available, you can easily ensure that strong MFA security is in place. The broad integrations ecosystem and SAML standard provide full-range access, giving organizations the ability to control user access privileges quickly and effectively.



Single Sign-On (SSO): Included with AuthPoint MFA, AuthPoint's web single sign-on application portal is built with user-friendly features and admin tools to deliver seamless and secure access to resources.

Credentials Monitoring: AuthPoint Total Identity Security's Dark Web Monitor is a proactive service that notifies customers when compromised credentials from monitored domains are found in a newly acquired credentials database published in our service.