RESOURCE CENTER

アイデンティティとアクセス管理の状況

アイデンティティとアクセス管理の6つの主要な要素と、それらを組織に適用する方法について説明します。

Get the full interactive view at
https://bitwarden.com/ja-jp/resources/charting-the-identity-and-access-management-landscape/

bitwarden

A closer look at the

Identity and Access Management Landscape

In order to grow, every company, business, or organization must have a systematic method to arrange employees or members. Today that method frequently falls under the banner of Identity and Access Management (IAM), or also sometimes known as Identity Credential Access Management (ICAM). In both cases, the overall framework outlines how to onboard new employees to the organization, and manage succession and de-provisioning of accounts when needed.

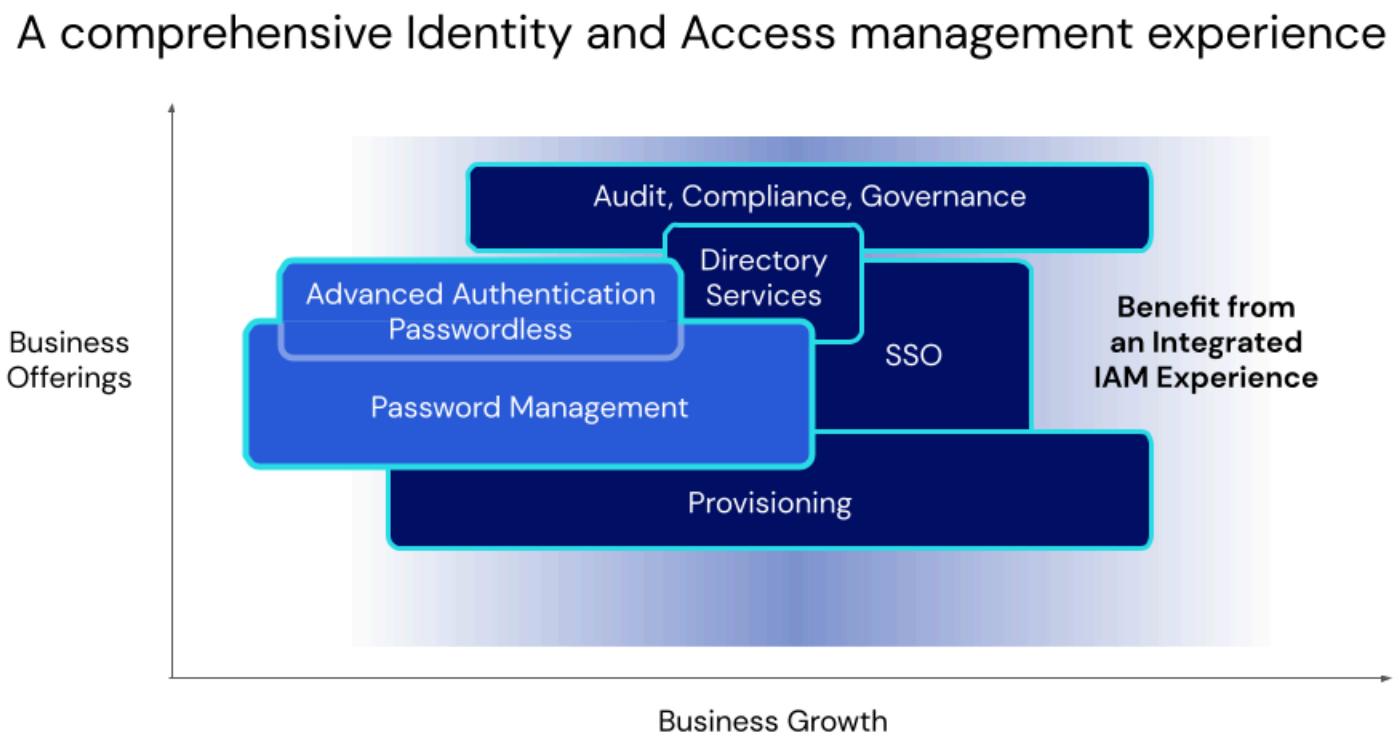
Elements of Identity and Access Management pertain to all companies of all sizes. It is never too early to start thinking about how an organization should manage and maintain employees or members.

In this paper, we explore the six primary elements of Identity and Access Management, and how you can apply them to your organization.

Table of Contents

- Provision for success
- Directory Services for Group Organization
- Login with SSO for unified access
- Auditing for Compliance and Governance
- Delivering an Integrated Identity and Access Management Solution

Six Elements of Identity and Access Management



Across a number of industry and analyst reports, the primary areas of Identity and Access Management fall into

- Password Management
- Advanced Authentication

- Provisioning
- Directory Services
- Single Sign On
- Audit, Compliance, Governance

Start with Password Management

Every organization begins with one or more individuals, and it makes sense to begin with password management and enable employees from the start.

For example, even **before** individuals begin setting up new accounts, they need the ability to generate long and unique passwords for each website or service they need. A password manager with a built in password generator makes this easy. Now right from day one, employees put themselves in the best position to succeed by keeping accounts separate and secure with long and unique passwords.

Add sharing to password management for team collaboration

Once individuals have a password manager to generate long and unique passwords, and retain those for easy access, you can advance to securely sharing credentials within a team.

Business-oriented password managers allow for the management of organizations and secure, structured sharing among groups of users. Those groups can be assigned to different collections of sensitive items such as company logins, shared credit cards, or office wifi passwords.

By establishing an end-to-end encrypted platform for secure sharing, every organization sets the proper foundation for employee and company security.

Incorporate advanced authentication

With a long, complex, random, and unique password per account, users put themselves in a strong position to stay protected. An even stronger step is to add two-step login, or two-factor authentication, to both the login for your password manager as well as other websites and services.

With your password manager, two-step login can be configured with authenticator applications, security keys, email, or SMS. Note that these days SMS is considered to be one of the more susceptible methods for hacking due to the prevalence of SIM jacking as a break-in strategy.

Whichever path users choose, be sure that everyone understands the ramifications of two-step login, retains a copy of website two-step login recovery codes if offered, and has a method to back up the authentication keys offered during the two-step login registration process.

Using a password manager with built-in two-step login

Some password managers offer built-in authenticators. This delivers tremendous convenience for users, especially in shared settings. Users can now share a login, including the two-step login sequence, and not have to worry about calling or texting each other to find out the secret code.

Of course, some might ask about the point of including a built-in authentication step with your password manager, and does that negate the value of authentication. Ultimately, users have choices, and employers can educate on preferred practices. These are the reasons to

pursue an integrated approach

1. Your Password Manager Vault should have two-step login itself using another method. (Important: you should not use your password manager's built-in authenticator to protect your password manager account.) Therefore your vault and accounts are currently protected with a high level of security and, in fact, two-step login.

2. Having two-step login enabled for websites and applications provides more security than not having it enabled. A tighter bundling of two-step login makes it easier to use more frequently, which promotes better security practices.

3. If you need to share an item, you can share it with two-step login enabled, which, again, promotes better security. This is a collaboration and two-step login power move.

4. You do not need to remember which authentication app you used, since it remains built-in.

5. You can always choose, on an individual basis, which login to authenticate internally within your password manager authenticator, or externally using a separate authenticator app.

Read more

The basics of two-factor authentication with Bitwarden

Evolving to Passwordless

As the world moves to passwordless, be sure that your password manager, and overall Identity and Access Management strategy involves passwordless options. For example

- Ensure you can log into devices with biometrics, as well as enable autofill capabilities for credentials with biometrics
- For Single Sign On, also discussed later, explore options that offer passwordless experiences
- Consider the use of security keys throughout your organization
- When deploying security keys have redundant options in mind, as well as backup and recovery procedures if keys go missing, of if keys are connected to company-critical user accounts
- For example, it might make sense for an employee to list the location of any backup security key(s) in their password management vault, only available to view upon account takeover and emergency access

Read more

Access your Bitwarden vault without a password

How to go passwordless with Bitwarden

Provision for success

The faster employees ramp up within a new company, the faster they can be productive and contribute to success. Unsurprisingly, provisioning occupies a large budget portion of Identity and Access Management, but remains spread across a number of systems and tools.

Companies frequently customize their onboarding processes based on the primary systems in place such as email, messaging, directory services, and Single Sign On discussed in more detail shortly.

To facilitate the best onboarding experience for employees and ensure that the password manager can fit within an overall framework, look for password managers that offer

- A robust application programming interface (API) to integrate with existing systems
- A fully featured command line interface that enables scripting for custom processes
- The ability to integrate with existing Identify and Access Management Systems such as
  - Directory Services
  - Single Sign On
  - Auditing and Logins

Directory Services for Group Organization

Larger companies often deploy directory services to keep employees organized by department. For example, there may be groups based on sales, marketing, engineering, IT, and finance. These existing directory services provide a means to arrange employees by function, add new employees to the right groups quickly, and de-provision accounts when necessary.

Enterprise level password managers integrate with directory services to arrange groups of users within the password management organization vault. If a group of finance employees has access to a specific set of tax services credentials, a new member of that group will automatically gain access to those credentials.

Some companies use directory groups to facilitate ad hoc teams as well. For example, a cross departmental tiger team may form around a new business initiative. The team may request a password management group of its own. With directory integration, this new tiger team can be synchronized to the password management application and quickly enable a set of secure credentials.

Login with SSO for unified access

With the boom in software-as-a-service (SaaS) applications, many companies took advantage of Single Sign On to enable unified access to website accounts. Of course, Single Sign On requires that the website or service has that feature available. While many websites catering to businesses offer Single Sign On, there remains a world of websites and services that do not. A password manager fills that gap and more.

Some password managers can also integrate with Single Sign On, allowing companies to auto-provision users into an organization.

Of course, an end-to-end encrypted application such as a password manager is a bit different from your typical SaaS service. Since a password manager security model with zero-knowledge encryption guarantees that the provider cannot see anything within your vault, the context of Single Sign On takes a different flavor.

The root premise for a password manager is that the end user holds the key to encrypt and decrypt their data. The password manager does not know the key, and cannot provide it to the user should it be lost. Similarly, a password manager cannot just blindly give an end user decryption key to another 3rd party service (such as an identity provider) and rely on that other provider to keep the key safe.

Recognizing this, a secure model to integrate with existing Identity Providers enables the authentication through the Identity Provider, but retains the encryption and decryption with a master password retained by the user, specific to the password manager. This ensures that no 3rd party has access to decrypt the end user vault. It also means that the encryption and decryption master password should be unique to the password manager.

This approach also ensures that users can benefit from every client application offered by the password manager across browsers, mobile operating systems, desktop operating systems, web access, and command line interfaces.

Read more

Onboarding and Succession with Directory Services and Single Sign On

Auditing for Compliance and Governance

At a larger scale, companies need to monitor their systems, including access and use by employees. Frequently companies deploy logging and auditing solutions as receivers of information from a variety of sources. Popular enterprise logging and analytics systems include Splunk, along with Kibana from Elastic.

Robust password management systems provide the logging information via application programming interfaces (APIs) that can feed the existing logging systems. This delivers

- A single place for IT and security teams to collect information
- The ability to correlate events between a password manager and other elements of an overall Identity and Access management approach
- The option to feed into existing alerts

Delivering an Integrated Identity and Access Management Solution

Businesses have choices when deploying the right mix of Identity and Access Management tools, and can expand as they grow. Regardless of your point in the journey, all companies should be empowering employees to manage credentials securely, generate long and random passwords when needed, and facilitate end-to-end encrypted sharing for sensitive information.

To bring these capabilities to your own company, get started with a free Bitwarden business trial today.