IDENTITY AND ACCESS MANAGEMENT

1Password

SSO isn’t enough to secure every sign-on

Single sign-on has been considered a table stakes requirement since back when there was a clearly defined perimeter to protect. And it makes sense: SSO secures access to managed applications. But SSO was never enough to secure every sign-on.

Because – no matter how much we wish it were true – employees don’t stick solely to managed applications. They never did, but they *certainly* don’t now. SSO isn’t enough to secure the way we work today.

The benefits of single sign-on

SSO secures access to the services the company knows about by putting access to those services behind a single, strongly vetted identity. That reduces your attack surface by reducing the number of passwords in circulation.

It also lessens the need for employees to find creative ways to manage those passwords. Sticky notes tacked onto a monitor, for example. Password spreadsheets. Reusing passwords.

And because SSO brings all managed logins under one umbrella, security policies like MFA requirements can be applied to all of them at once.

34% of employees use unsanctioned apps.[1]

61% of employees have poor password practices.[1]

Use of credentials is the #1 way attackers gain access to systems.[2]

[1] 1Password State of Enterprise Security, 2024
[2] Verizon Data Breach Report, 2024

The limitations of single sign-on

34% of workers use unsanctioned apps. SSO can’t secure those sign-ins, because the company doesn’t know about those sign-ins. And they often sign in to those unprotected services with bad passwords: 61% admit to using poor password practices.

That’s low-hanging fruit for attackers. Leveraging compromised credentials is the number one initial action taken during breaches. It’s the easiest way in.

SSO doesn’t protect against that.

Enterprise password managers (EPMs) like 1Password make it easy for employees to create, store, manage, and share the logins that SSO doesn't cover. Instead of requiring a service to be placed behind SSO, EPMs meet employees where they are, offering to create strong, unique passwords via a browser extension when employees create a new account. Once those credentials are stored in 1Password, employees can log in to those services automatically. No need to remember – let alone manage – a password for every account.

The Cybersecurity and Infrastructure Security Agency (CISA) recommends that businesses use an enterprise password manager to ensure that employees use strong, secure passwords for every account.

> "You can keep your business safe by requiring employees to use strong passwords and password managers."
>
> CISA: Require Strong Passwords

How to secure every sign-in

1 Eliminate the competing demands of security and productivity.

Security teams and workers struggle with competing priorities. 54% of employees say they're lax about company security policies. 44% say security would be less of an issue if security tools were easier to use and policies easier to follow. 1Password makes it easy for admins to set policy, and for employees to follow that policy.

2 Combine the strengths of SSO with the strengths of EPMs.

1Password policies help you govern how and where employees use 1Password. You can require two-factor authentication, for example, or set firewall rules to deny sign-in attempts from certain locations. 1Password can connect to your identity provider, too, to extend your IdP's security policies to 1Password. You can even require employees to unlock 1Password through single sign-on.

3 Extend access management to every sign-in for every app on every device.

In order to be truly secure, businesses must have full confidence that every identity is authentic, every application sign-on is secure, and every device is healthy.

1Password® Extended Access Management (XAM) extends beyond traditional IAM to secure the unmanaged applications and devices that are commonplace in the modern work environment. Employees can use the tools they need to be productive – and access is still secure across identity, device used, application accessed, and location.

For more information on closing the gaps left by SSO, or to request a demo of 1Password Enterprise Password Manager or 1Password Extended Access Management, contact us to speak with a security specialist.

1Password