LastPass ••• | enterprise
by LogMeIn

Protecting your business means securing every access point.

More devices, applications, networks and users increase the complexity of managing – and protecting – user access in your business.

Single sign-on connects employees to high-priority apps while eliminating passwords.

Enterprise password management captures and stores all other credentials.

When combined in one solution, every access point is secured, and password friction is eliminated.

We know poor credential management is a serious cyber security risk – and productivity drain.

93% of cyber incidents can be prevented with the right tools.[1]

80% of confirmed data breaches are caused by weak, default or stolen passwords.[2]

$3.9 million is the average cost of a data breach.[3]

6 months is the average time to detect a breach.[4]

42% of people manually keep track of passwords in a file.[5]

Single sign-on eliminates password risks – and boosts productivity.

SSO relies on SAML, a secure, behind-the-scenes protocol, to authenticate users to cloud, mobile, legacy and on-premise apps. Passwords are eliminated and access speeds up.

154 times On average, an employee types out login credentials **154 times a month.**[6]

36 minutes **36 minutes a month** are wasted on password-related activities.[7]

76 percent **76% of employees** experience regular password problems.[8]

Why SSO?

Faster deployment: Employees can be onboarded and offboarded quickly, and new apps are provisioned instantaneously.

Improved productivity: With no password to remember, apps are easy to access and use – and helpdesk calls go down.

Better security: Removing passwords reduces risky behaviors, and IT oversight means more compliance.

SSO alone isn't enough.

What about the services IT doesn't know about? Or the ones they can't or won't integrate with SSO?

over 50% of the most popular websites and apps in use in businesses worldwide do not have out-of-the-box support for SSO.[9]

191 passwords is how many passwords the average employee has to manage.[10]

Password sharing remains a reality.

Whether or not IT teams are aware, employees often share passwords with their co-workers.

6 passwords are shared by the average employee.[11]

An enterprise password manager secures the rest.

A password manager captures and stores all remaining credentials an employee uses, giving IT control and visibility without the added work of integrations and approvals.

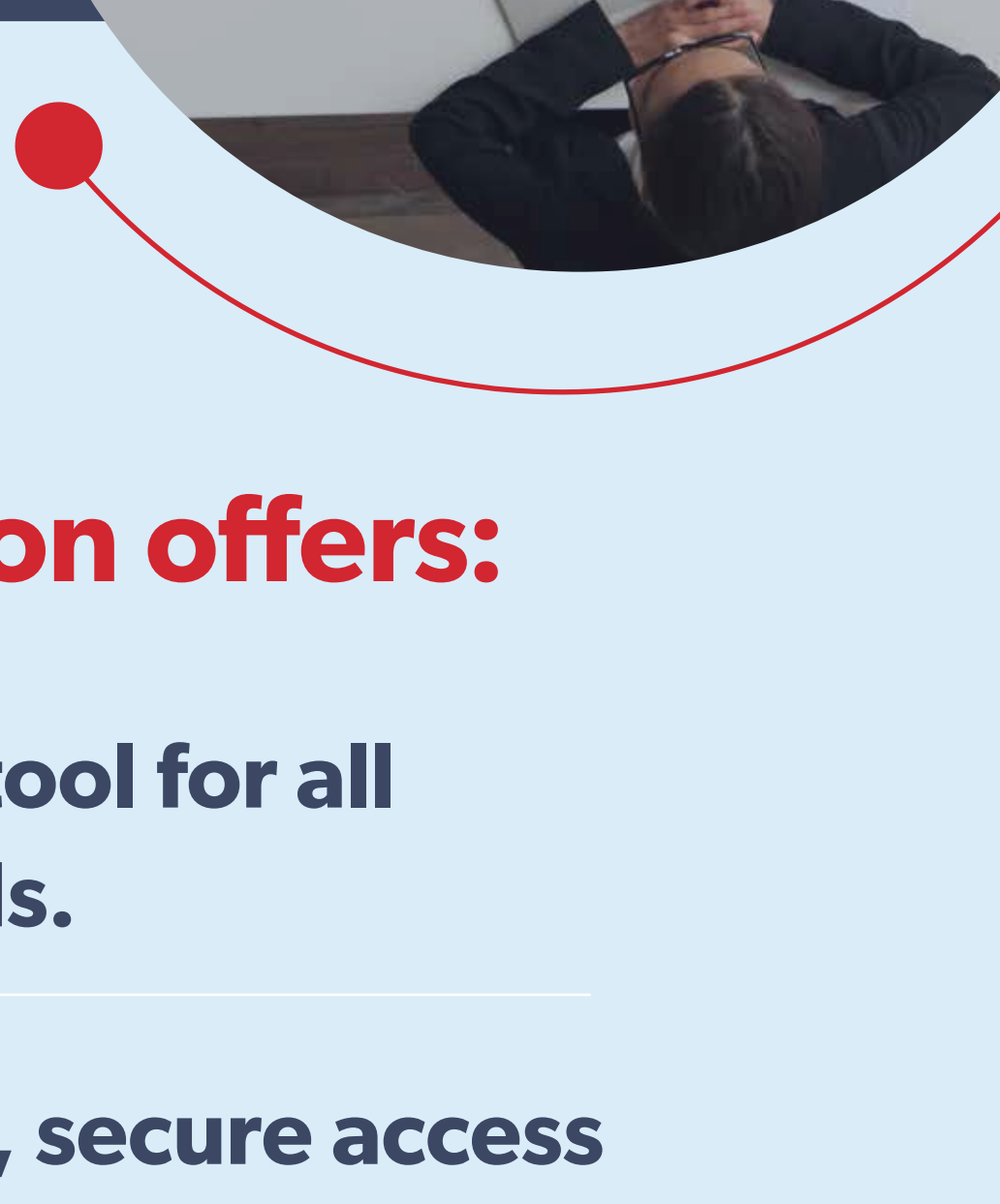
78% of IT execs say they do not have complete control over cloud apps used by employees.[12]

61% of IT executives rely on employee education alone to enforce strong passwords.[13]

69% of employees would use a password manager if offered one.[14]

Together is best.

The best access solution seamlessly combines single sign-on with password management in one platform to secure every access point in your business.



The best solution offers:

- One single tool for all access needs.
- Centralized, secure access for every credential.
- Ease of use for employees.
- Quick onboarding and deployment.

See how simple security can be with LastPass Enterprise.

www.lastpass.com/products/enterprise-password-management-and-sso

Sources:

1. The Online Trust Alliance's 2018 "Cyber Incident & Breach Trends Report".
2. Verizon 2019 Data Breach Investigations Report (DBIR)
3. Ponemon Institute's 2018 "Cost of a Data Breach Study"
4. FireEye M-Trends 2019 Report.
5. LastPass 2017 report "The Psychology of Passwords: Neglect is Helping Hackers Win"
6. LastPass 2017 Report "The Password Exposé: 8 truths about the threats – and opportunities – of employee passwords"
7. LastPass 2017 Report "The Password Exposé: 8 truths about the threats – and opportunities – of employee passwords"
8. Ovum's 2017 Report "Closing the password security gap: Employee education isn't the only answer"
9. LastPass 2017 Report "The Password Exposé: 8 truths about the threats – and opportunities – of employee passwords"
10. LastPass 2017 Report "The Password Exposé: 8 truths about the threats – and opportunities – of employee passwords"
11. LastPass 2017 Report "The Password Exposé: 8 truths about the threats – and opportunities – of employee passwords"
12. Ovum's 2017 Report "Closing the password security gap: Employee education isn't the only answer"
13. Ovum's 2017 Report "Closing the password security gap: Employee education isn't the only answer"
14. Ovum's 2017 Report "Closing the password security gap: Employee education isn't the only answer"