LastPass •••|

Four Ways to Protect Your Business in the Cloud

This is your wake-up call.

More devices, applications, networks and employees increase the complexity of managing – and protecting – user access in your business. While employees just want to work efficiently, IT needs to ensure the proper controls are in place to protect the company.

80% Of breaches are due to poor passwords.[1]

53% Of people don't change a password after a known breach.[2]

76% Of employees experience regular password problems.[3]

43% Of all cyberattacks target small businesses.[4]

[1] Verizon, 2019. "Data Breach Investigations Report (DBIR)"
[2] LastPass, 2018. "Psychology of the Password Report"
[3] Ovum, 2017. "Closing the Password Security Gap"
[4] SCORE, 2018.

Make access control a serious priority.

A modern BYO-anything workforce means more access points, hidden apps and hurdles to secure across the organization. Even as cyberthreats rise, employees expect technology to be fast, convenient and easy to use. Businesses must prioritize an access solution that secures the organization while helping employees stay productive wherever they are.

Best practices include:

- **Know your apps:** Track and vet the apps in use across your organization.
- **Specify permissions:** Assign specific access privileges based on organizational role.
- **Keep access simple:** Provide one-click access to all apps and tools.
- **Set access standards:** Create, communicate and enforce strong policies.
- **Support all use cases:** Build systems that give the right access, to the right people, at the right time.

> *"The threat level and risk to [Midsize Enterprises] continue to rise, with the volume and frequency of attacks, while the resources available to defend against them remain flat. Security breaches that exploit user behavior and the weaknesses of passwords are prevalent. Gartner recommends that MSEs use stronger authentication methods in addition to, or instead of passwords."*
>
> **– Gartner, 2018. "Midmarket Context: 'Magic Quadrant for Access Management, Worldwide'"**

Establish strong access policies.

An effective strategy looks to centralize employee access in a single portal, where all apps and credentials are controlled by policies. IT visibility into employee access and security behaviors is critical to protecting the business.

Create policies that enforce the following best practices:

- **Protect all access points:** Safeguard access to every app and login in a portal that's secure, backed up frequently and difficult for others to access.
- **Automate password storage:** Capture and store passwords for new services, whether they're managed by IT or not.
- **Get extra protection:** Require multifactor authentication wherever possible.
- **Share passwords safely:** Send one or more passwords to others in an encrypted format – discouraging insecure methods like text, email or written notes.
- **Stop password reuse:** Generate and store unique, random and strong passwords.

6 Months is the average time to detect a breach.[5]

$3.9 Million is the average total cost of a data breach.[6]

93% Of cyber incidents can be prevented with the right tools.[7]

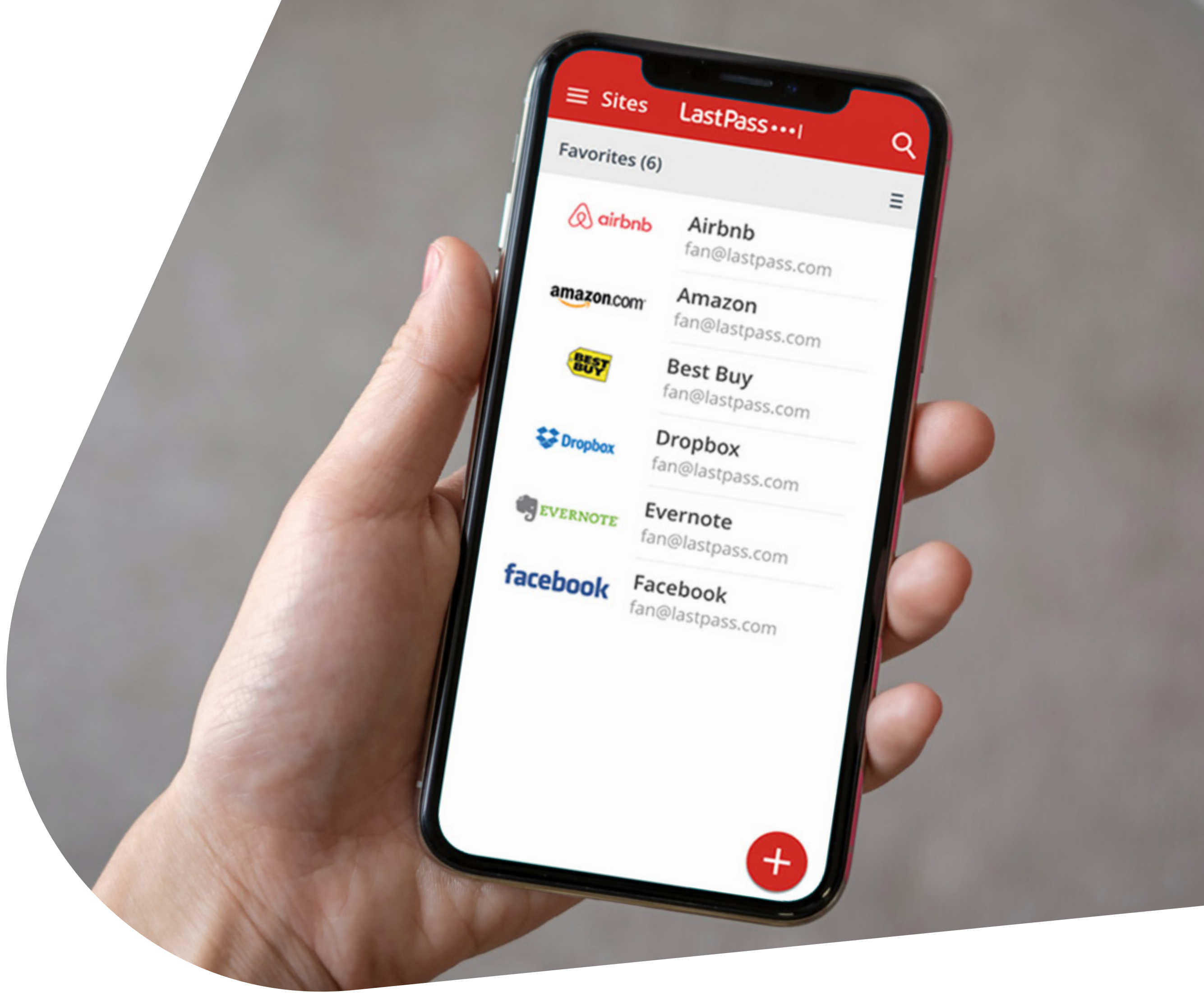
[5] FireEye, 2019. "M-Trends Report"
[6] Ponemon Institute, 2018. "Cost of a Data Breach Study"
[7] Online Trust Alliance, 2018. "Cyber Incident & Breach Trends Report"

Eliminate passwords.

Eliminate passwords where possible with single sign-on (SSO). For services that don't yet support SSO (or aren't yet worth IT investment), enable strong, unique passwords that are captured and filled for the employee – creating passwordless access to everything throughout the workday.

SSO best practices include:

- **Leverage SAML connections:** Connect to critical apps, from cloud to mobile to legacy, with a web-based authentication protocol that securely eliminates passwords.
- **Deploy pre-integrated apps:** Reduce IT workload with catalogs of pre-integrated apps when deploying new or existing cloud apps across the business.
- **Unify your solutions:** Invest in a complete solution that combines out-of-the-box SSO with easy enterprise password management (EPM) to ensure every access point to the business is secured.
- **Authenticate with many factors:** Look for platforms that leverage factors like device, identity, location, time, proximity, biometrics and more to provide adaptive, context-based authentication.



69% Of employees say they would use a password solution if it were offered to them.[8]

OVER 50% Of the most popular cloud services do not have out-of-the-box support for SSO.[9]

[8] Ovum, 2017. "Closing the Password Security Gap"
[9] LastPass, 2017. "The Password Exposé"

Get employees on and off systems fast.

You need to give employees convenient, secure access to the tools they need to do their jobs, with the appropriate level of permissions.

Onboarding and offboarding best practices:

- **Streamline IT processes:** From one centralized admin dashboard, get a unified view of employee access across the organization.
- **Connect with existing infrastructure:** Integrate with your existing user directory to automatically provision new employees, with the right privileges to the right resources.
- **Jump-start new employees' productivity:** Give employees a central portal toaccess so they are up and running from day one.
- **Have a kill switch:** Immediately and completely turn of access privileges when an employee leaves.

"One of our biggest challenges was onboarding people. Giving out passwords to hundreds of sites is daunting. [Now], the distribution and management of passwords across the organization is completely streamlined."

– Bryan Fernandez
Director of Product, FlightNetwork

Today's complex, hybrid IT environment demands an access solution that is simple, integrated and seamless while also increasing security.

For more than 70,000 businesses, LastPass Business reduces friction for employees while increasing control and visibility with a password management solution that is easy to manage and effortless to use. LastPass Business empowers employees to generate, secure, and share credentials seamlessly, while ensuring protection through LastPass' zero-knowledge security infrastructure.

In addition to password management, LastPass Business offers additional security features, such as single sign-on (SSO) with simplified access to up to three cloud applications and multi-factor authentication (MFA) that secures the LastPass vault and those single sign-on applications.

LastPass•••|

Protect your employees from anywhere.

Learn More