Four Ways to Protect Your Business in the Cloud.

LastPass••• | enterprise

This is your wake up call.

Businesses are challenged to provide employees with the convenience and flexibility of cloud-based tools, while simultaneously ensuring the protection and confidentiality of important company information.

4.2B
credentials stolen in 2016 alone.[1]

$4.0M
average total cost of a data breach.[3]

63%
breaches used weak/default/stolen passwords.[2]

1. Make access control a serious priority.

Businesses must protect their data with access management that secures the organization's digital assets, while helping employees stay productive wherever they are.

> Passwords are one small, but important, piece in the security puzzle. For growing businesses looking to scale, continuing to stay on the forefront of identity and access management is critical.
>
> — Brian Masson,Information Security Officer, Wave Apps

Best practices include:

Know your apps: Track the apps being used across your organization.

Specify rights: Assign specific access privileges based on organizational role.

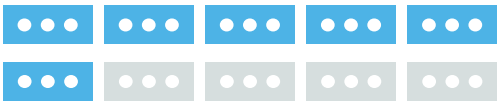
Keep access simple: Provide one-click access to all apps.

Set password standards: Create, communicate, and enforce a strong password policy.

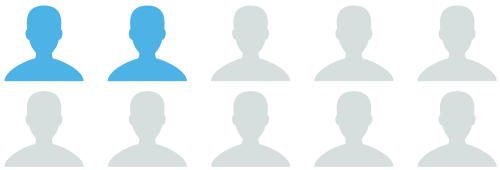
Check the security of new apps: Create a process for vetting the security of any new services.

2. Establish strong password practices.

While businesses can establish strict password policies, it's just not realistic to expect full compliance from employees. The responsibility falls on the organization to build systems that make strong passwords the default.



59% of surveyed respondents reuse their passwords.[4]



22% share passwords with a co-worker.[4]

73% don't reset their password after sharing it with someone.[4]

Make sure employees use these password strategies:

Stop re-using passwords: Use a password manager to generate and store unique, random, and strong passwords.

Get double protection: Turn on two-factor authentication wherever possible.

Protect your passwords: Safeguard passwords in a password manager that's secure, backed up frequently, and difficult for others to access.

Clear out your browser: Delete your cache and cookies on a regular basis.

Automate password storage: Automatically store any passwords for new services to a password manager.

3. Share passwords responsibly.

If password sharing isn't handled correctly, you could open the door for hackers.

> [With a password manager], passwords aren't lost when staff leave, and they can be securely shared among staff members. Administrators can ensure that access to technology is appropriate and controlled.
>
> — Michelle Page, *VP of Finance & Administration, Code.org*

Make password sharing safe with these precautions:

Apply the same best practice:
Ensure shared passwords are random, strong, and unique to each application.

Share via a password manager: Send one password or multiple passwords to others on a team in an encrypted manner by using a password manager.

Establish strict sharing policies: Discourage team members from sharing passwords via insecure methods like text, email, or post-it note.

Keep up with staff changes: Update passwords for shared accounts when a team member leaves the organization— and remove their access immediately.

4. Get employees on and off systems fast.

You need to give employees secure access with all of the proper rights, access levels and credentials.

On-boarding and off-boarding best practices:

Streamline IT processes: Provide a centralized team access management system to assign passwords and credentials.

Jump-start new employees' productivity: Give employees a central portal to access, so they are up-and-running from day one.

Have a "kill switch": When an employee leaves, you need to immediately and completely turn off access privileges.

> 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

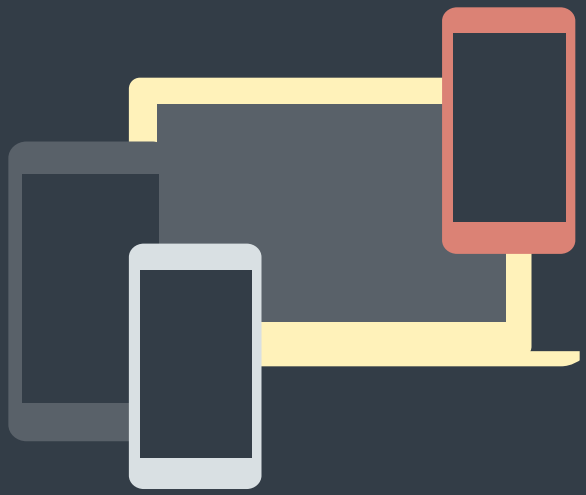
(LastPass)

The trusted solution for access control.

The challenge isn't just about accessing information on the go. It's about ensuring simple and secure acess.

Today, everyone carries multiple devices . Our critical and sensitive data resides in the cloud and the line between personal and professional apps is blurring more each day.

LastPass Enterprise simplifies access management for companies of every size, providing the tools to secure their business and centralize control of employee passwords and apps. Trusted by over 27,000 businesses, LastPass Enterprise empowers your organization to enforce a strong password policy and streamline admin control, so you can reduce risk across your entire company while boosting employee productivity.



1. 2016 Data Breach QuickView Report: pages.riskbasedsecurity.com/2016-ye-breach-quickview
2. Verizon DBIR 2016: verizonenterprise.com/verizon-insights-lab/dbir/2016
3. 2016 Ponemon Cost of Data Breach Study: www-03.ibm.com/security/data-breach
4. LastPass Password Sharing Survey 2016: blog.lastpass.com/infographic-keep-your-friends-close