Securing the Cloud

4 ways to protect your business in a work-anywhere world

LastPass •••|

welcome to the new workplace.

The Way We Work Is Changing.

Thanks to powerful mobile devices, emerging cloud technologies, and constant Internet connectivity, employees are no longer limited to one work location. Traditional 9-to-5 schedules have gone by the wayside. And the line between work and personal life is blurry at best. Businesses understand that to keep their systems and data secure in a work-anywhere world, they need to have the right protection in place—without slowing down employees.

the cloud challenge

Despite the potential for greater productivity and higher worker satisfaction, mobility and the cloud create a host of challenges:

- **Sensitive corporate data** gets accessed, stored, and shared in many different ways
- **Employees' use of third-party apps** becomes difficult if not impossible to track
- **Establishing and enforcing effective security controls** across an organization is difficult

More Work Is Happening in the Cloud

The promise of increased productivity and growth has motivated many businesses to implement cloud-based solutions for collaboration, data storage, utilities management, and more. Younger companies are leading the way, with 25% placing nearly half of their applications in the cloud.

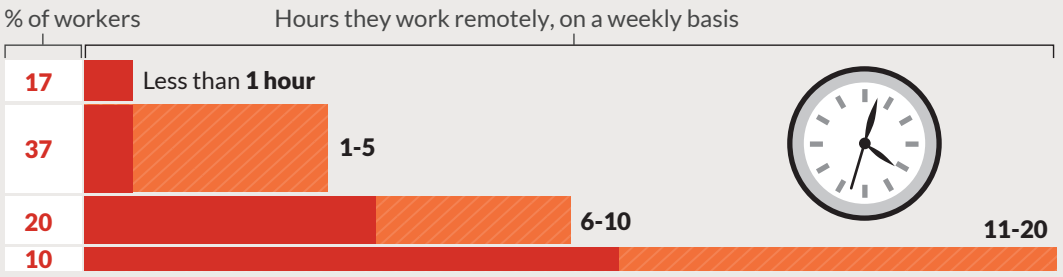
Given this transition, it's up to senior management and IT leaders to put the right systems in place to ensure security—without requiring any additional thought or effort from employees. Employees just want convenient, easy access to their apps and services to stay productive from wherever they are working.

THE EVOLUTION OF WORK

Almost half of knowledge workers say how they worked 10 years ago, no longer works today

10 years ago	5 years ago	Today
80%	50%	53%
Primarily logged in from their office desk	Mostly in the office but remote access via VPN	Access cloud apps via Wi-Fi from anywhere

Nearly 80% of people worked remotely in the past six months.



Source: Lab42 study conducted May 2015

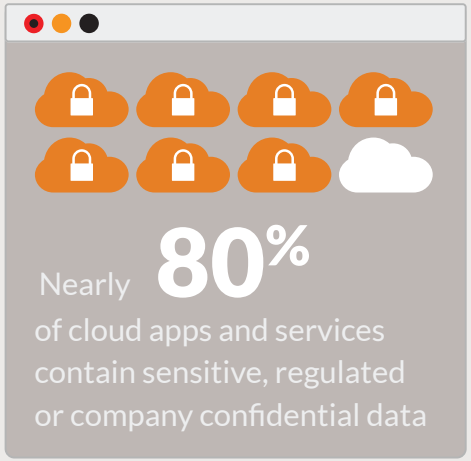
Data Security Is Getting More Complex

To keep data safe in the past, companies only had to consider the security of their internal network. The refrain used to be, "Secure the perimeter!" But now, with more employees working remotely—and more businesses allowing "bring your own device" (BYOD) and "bring your own app" (BYOA) arrangements—the traditional IT perimeter is all but gone.

With the transition to the cloud, the number of systems and accounts employees access has multiplied. But most employees repeatedly use just a couple of passwords. Corporate single sign-on solutions don't extend to the third-party cloud applications many employees use on their own, leaving companies vulnerable. A lack of proper security measures puts businesses just one weak password away from a devastating security breach. And with the proliferation of devices people use at work, an ever-greater number of platforms, and the rise of the Internet of Things, properly securing digital assets is only getting more complicated.

Too often, a lack of proper security measures puts businesses just one weak password away from a devastating security breach.

CLOUD SECURITY CONCERNS



25% of surveyed businesses have already suffered a security breach due to a compromised cloud account

Nearly **8 out of 10** SMBs are concerned about an account breach

Source: 2015 Enterprise Strategy Group & LogMeIn Research, 'Password Security in a Cloudy World'

> I have an aversion to signing up for new apps because I crave simplicity. Each one is something new to worry about—but there are so many apps that provide great services that we need.
>
> —*David Petersen, CEO of BuildZoom*

It's Difficult to Manage and Track Access

In the new app-centric world, more workers are utilizing personal devices, cloud services, and apps to get work done. They're just as likely to hop on a meeting via join.me as they are to pick up the phone. On average, employees use more than 25 different apps to collaborate, communicate, manage projects, store and share files, and access their work.

In addition, some work teams also need to share access to single accounts. For instance, multiple members of a social media or marketing team all may need to share access to a company's Facebook, Twitter, blog, or content management system, often managed with one account and one password.

The combination of so many apps and services has led to other complications:

Employees use weak passwords and repeat them everywhere because it's too hard to remember long and complicated ones

Companies have little or no control over employees' password behavior—weakening defense against breach

Single sign-on solutions don't accommodate all of the logins employees need to manage

Phishing schemes that target employee credentials remain a leading cause of breach, compounded by password reuse

Offboarding is complicated and laborious, exposing companies to risk when they don't turn off access quickly enough

Some passwords to single accounts are shared across teams, via insecure methods with no trackability or accountability

The growing number of logins to manage, though, means an increased burden on employees to remember many passwords. This has led to a significant loss in productivity for employees and the IT team when dealing with password resets and access problems.

Four Ways to Protect Your Business in the Cloud

Just as the future of remote collaboration and data storage is in the cloud—the future of security is also the cloud. With the ubiquity of mobile technology, even small organizations now have employees distributed over multiple locations—some in offices, some working from home, others always on the road.

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. Recent high-profile data breaches serve as a wake-up call that businesses need to protect their data and assets from lax or rogue employee behavior, hackers, competitors, and other internal and external threats.

42.8m

Security incidents were detected in 2014

48%

The increase in security incidents from 2013 to 2014

$3.5m

The average total cost of a data breach

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

Make Access Control a Serious Priority

In this new app-centric world, businesses must efficiently and securely manage employee use of cloud applications. Businesses must avoid issuing access credentials on an ad hoc basis—or worse, allowing employees to manage and share access themselves. Instead, they must protect their data with effective access management processes that secure the organization's digital assets, while helping employees stay productive wherever they are.

Best practices for IT within organizations include:

- **Know your apps**
  Have a system in place to track the apps being used across your organization
- **Specify rights**
  Assign specific access privileges to employees and anyone else on your network based on their organizational role
- **Keep access simple**
  Provide employees with a system for one-click access to all the apps they use, from every major web browser
- **Set password standards**
  Create, communicate, and enforce a strong password policy that everyone on your network understands and follows
- **Check the security of new apps**
  Create a process for vetting the security of any new applications and services your organization uses

Establish Strong Password Management Practices

The first line of defense in security largely starts with employees using strong passwords. But it's very hard for people on the move to create and remember unique, strong passwords for all of the many different applications they use each day. So they tend to fall back on one or two easily remembered passwords, which they repeat in multiple places. Plus, while some companies may think they're safe by implementing single sign-on (SSO) solutions, SSO protection only extends to a fraction of the third-party cloud services that employees are using.

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, without slowing down users. They need to ensure that no matter where employees connect from, or what apps they use, passwords will be strong and secure.

Make sure employees use these effective password management strategies:

- **Stop re-using passwords**
  Use a password manager to generate and store unique, random, and strong passwords for every application
- **Get double protection**
  Turn on two-factor authentication wherever possible, to gain an extra layer of security
- **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 browser cache and cookies on a regular basis
- **Automate password storage**
  Automatically store any passwords for new services to a password manager

59%
of surveyed respondents re-use their passwords

22%
share passwords with a co-worker

73%
don't reset their password after sharing it with someone else

> [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*

Share Passwords Responsibly

Sometimes multiple individuals on a team share access credentials to a system or third-party application. If password sharing isn't handled correctly, you could open the door for hackers and opportunists to break into your accounts. Fortunately, there is a way to facilitate password sharing without sacrificing security.

Make password sharing safe with these precautions:

- **Apply the same best practices to shared passwords**
  Ensure that any shared passwords are just as random, strong, and unique to each application as individual passwords
- **Share via a password manager**
  Send one password or multiple passwords to others on a team in an encrypted manner by using a strong password manager that includes a secure password-sharing feature
- **Establish strict sharing policies**
  Mandate password policies that 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

Get Employees On and Off Systems—Fast

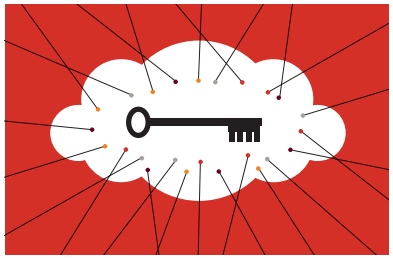
With the pressure to make sure even new hires become productive as soon as possible, the last thing you want is to sideline them with systems access issues. You need to give them quick, secure access with all of the proper rights, access levels and credentials.

By simplifying and streamlining on-boarding and off-boarding processes, you can also keep your IT department focused on productive work—instead of time-consuming administrative tasks.

Safeguard your company's data with these on-boarding and off-boarding practices:

- **Streamline IT processes**
  Alleviate the burden on IT staff when new hires join your company, by providing them with a centralized team access management system to assign passwords and credentials
- **Jump-start new employees' productivity**
  Give employees a go-to, central portal to access their apps and passwords, so they are up-and-running from day one with everything they need to get to work
- **Have a "kill switch"**
  When an employee leaves your organization, you need to immediately and completely turn off access privileges. Doing so prevents the possibility of a rogue or disgruntled ex-colleague from jeopardizing the security of company data

> 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 at FlightNetwork*



Try It Today! Experience Simple, Secure Password Control

See how companies of every size, from startups to Fortune 500's, are increasing productivity and securing their systems.

START YOUR FREE TRIAL OF LASTPASS ENTERPRISE

Visit www.lastpass.com/enterprise

LastPass Enterprise: The Trusted Solution for Access Control

SIMPLE, SECURE ACCESS MANAGEMENT

In a world where everyone carries multiple devices, critical and sensitive data resides in the cloud, and the line between personal and professional apps is blurring more by the day, the challenge isn't just about accessing information on the go—it's about making sure that access is simple and secure.

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 18,000 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.

We're committed to helping businesses manage identity and access in a constantly changing and complex working world. By staying at the forefront of emerging authentication technology, we help businesses gain the productivity and convenience benefits of the cloud—while boosting security organization-wide.

About LastPass

LastPass is the world's leading password managment solution that helps millions around the world organize their online lives. LastPass provides secure password storage to make going online easier and safer, supporting all browsers, platforms, and mobile devices. LastPass Enterprise scales Single Sign-On and password management for teams small and large, with the security businesses need and the convenience of one-click access that employees expect. Founded in 2008, LastPass is headquartered in Fairfax, Virginia and is a product of LogMeIn (NASDAQ:LOGM). LastPass is a trademark of LogMeIn in the U.S. and other countries. For more information, visit https://lastpass.com.

LastPass •••| **www.LastPass.com | sales@lastpass.com**