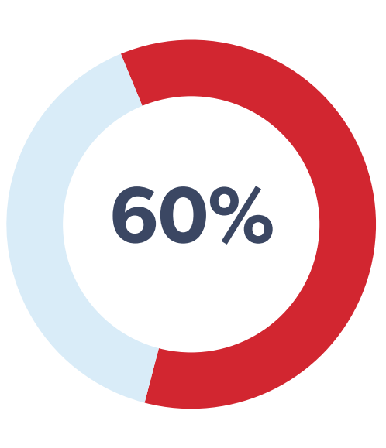
LastPass ••• |
by LogMeIn

What's the big risk?

Failing to effectively manage employee identity and access leaves your business exposed to threats.

Employees with too much access can pose an insider threat.

When employees have access to more than they need to do their job, there are more opportunities for mistakes, whether accidental or not.



Insider threats account for **60 percent** of cyber attacks, and they are incredibly difficult to detect.[1]

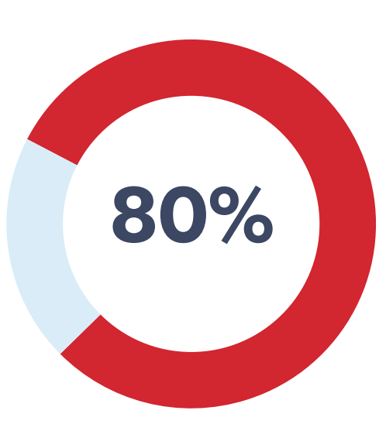
Lack of accountability means you don't know who did what, when.

If too many people have the same level of access and there is no way to tie actions to individuals, it's nearly impossible to know where a threat may lurk.

83% of IT professionals report employees storing company data on unsanctioned cloud services.[2]

Poor password habits leave the door open to outsiders.

People are notoriously bad at creating strong passwords and following password security best practices, leaving your business vulnerable.



80% of known data breaches are due to weak, reused, or stolen credentials.[3]

HBO SONY MANDIANT

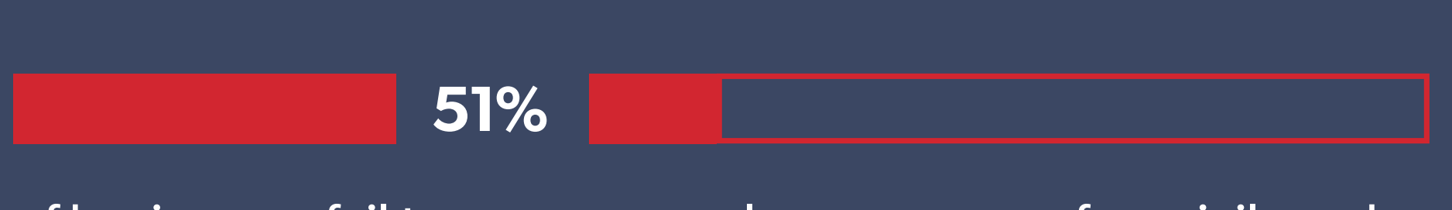
Passwords aren't enough to stop an attack.

Without additional security layers in place across the organization – like multifactor authentication – one stolen password can let hackers in.

Only 45% of businesses have employees using multifactor authentication.[4]

Treating privileged accounts like any other leaves the keys to the kingdom exposed.

Failure to protect, manage, and revoke access to privileged accounts makes you an easier target for attackers looking to gain administrative rights to your systems.



of businesses fail to use a secure logon process for privileged accounts.[5]

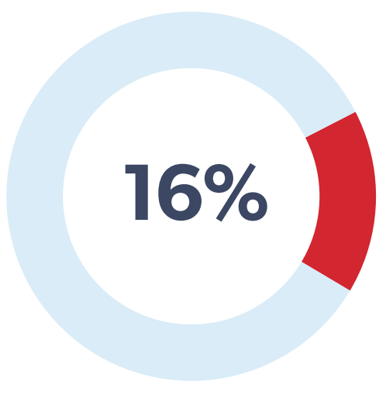
Shadow IT leads to sensitive data stored in unknown, unprotected apps.

Shadow IT drivers include increased efficiency **(60%)**, increased productivity **(62%)**, and to free up IT's time **(58%)** - but the lack of oversight and security means company data is at higher risk.

of employees use a 3rd-party cloud app without the approval or knowledge of IT.[6]

Disjointed systems mean you don't know who's coming and going.

Is access revoked when someone leaves the organization or changes roles? When onboarding and offboarding is manual, people retain access far longer than they should.



In only 16% of organizations does HR take the lead in ensuring that access to data sources, devices, accounts, etc. is disabled for departing employees.[7]

53%

Zombie accounts increase the attack surface.

Unused accounts that are left active are one more way for disgruntled employees or malicious attackers to gain a foothold.

53% of organizations don't monitor access to apps and data that people used when they were on the job.[8]

A distracted, overworked IT team can't focus on the bigger security picture.

Passwords alone pose a significant ongoing productivity drain for IT professionals, and competing priorities mean simple steps aren't taken to improve security.

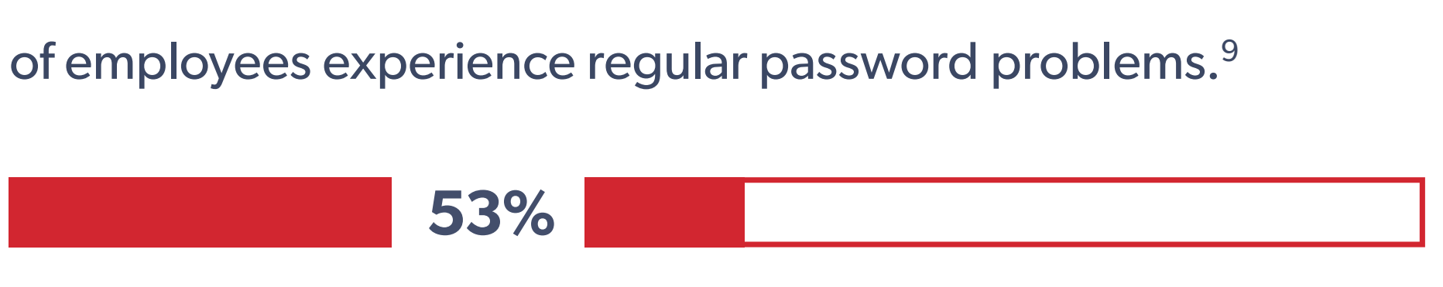
41% of IT teams struggle to balance day-to-day IT tasks with improvement projects.[8]

41%

Doing nothing leads to greater threats, inefficiencies, and costs.

The status quo may seem like enough but failing to modernize identity and access across the business leaves you exposed to breach and compounding obstacles.

of employees experience regular password problems.[9]



of midmarket companies have experienced a breach.[10]

The fix?
A comprehensive identity solution.

The longer these risks go unmitigated, the more likely it is a potentially-devastating data breach will affect your business. An identity solution that is simple, integrated and seamless can give IT teams centralized control and unified visibility across every entry point to the business, while providing frictionless access to users.

Learn more about how LastPass Identity can help

Sources:

1 2018 IBM X-Force Threat Intelligence Index
2 NTT Com Shadow IT Survey, 2016.
3 Verizon's 2019 DBIR
4 LastPass 2018 "State of the Password" Report
5 "Comply or Die: 2018 Global State of Privileged Access Management (PAM) Risk & Compliance"
6 NTT Com Shadow IT Survey, 2016.
7 Osterman Research "Protecting Corporate Data When Employees Leave Your Company" by RSA
8 Osterman Research "Protecting Corporate Data When Employees Leave Your Company" by RSA
9 Spiceworks 2019 State of IT Report.
10 Ovum's 2017 Report "Closing the password security gap: Employee education isn't the only answer"
11 Cisco's 2018 Report "Small and Mighty: How Small and Midmarket Businesses Can Fortify Their Defenses Against Today's Threats"

07.09.2019/PDF/LMI0638d