LastPass

LASTPASS BUSINESS FACT SHEET

Password Management for your ENTIRE organization

A password management solution should cover all employees -- not just specific departments and individuals.

Deploying a password management solution to select departments of your organization allows risks and vulnerabilities to persist, and even grow. In today's workplace, employees are spending 70% more of their time online, making their digital presence larger than ever. On top of that, password reuse is increasing: 92% of people know using the same password or a variation is risky, but 65% do it anyway*. Even if you implement security practices at your organization, individuals will continue to have poor password hygiene if they're not equipped with the right tools to be successful.

Think of passwords as a universal key to any door of your organization. Whether that door is frequently used or not, it's accessible. As flexible work continues, doors are added, and the universal key multiplies. Take, for example, the fact that 50% more online accounts were created in a year-over-year study. And for work-related accounts, only 32% had a strong password attached to them.

If anyone at your organization is creating, managing, or sharing weak or reused passwords, the keys to your business are at risk. Provide a password manager for everyone through a LastPass Site License to eliminate password fatigue and poor security posture.

Secure and streamlined collaboration

Employees can share credentials by securely granting (and revoking) access in real-time to individual accounts or shared folders, both internally and externally. Hide the actual password by enabling individuals to launch the shared account from a LastPass vault. Collaboration has never been so simple – maintain efficiency while increasing security.

Integrate with existing technology to fill security gaps

Many think that deploying one security solution covers the entire digital workplace, but only deploying a Single Sign On (SSO) solution, for example, only secures just a percentage of applications – not all. And often, SSO is deployed to protect business-related technology, like Workday and Slack. But what if your employees use their work device for personal use or vice versa? Use password management to augment or integrate with the technology you use most at your business, and rest assured every access point is secure.

*Last Pass Psychology of Passwords Report 2021

Deploy organization-wide, save big, and gain support

A LastPass Site License offers a LastPass Business account for every employee in your organization at a flat fee versus a seat-based rate. This option provides you the flexibility to scale your LastPass use as your company grows, without any added cost. You can also receive a Customer Success Manager (CSM) to assist with roll out of LastPass at your organization. Plus, every LastPass Business account holder will also gain a free Families account – granting a personal account and five more accounts to share with those closest to them.

Password Management for All: Identify everyday use cases and secure your business

IT	IT manages large volumes of passwords required to keep their technology and security infrastructure secure – and the business running. From servers to administrative tasks, IT needs a simple solution to secure and share credentials so data remains protected, employees are onboarded quickly, and technology issues are few and far between.
Sales and Business Development	These team tools include customer-management services, demo logins, and automation software to help manage client and vendor relationships. Plus, these individuals tend to be on the road using mobile devices, connecting to various Wi-Fi networks, and increasing their digital exposure.
Marketing	Marketing teams use websites and tools for PR, campaigns, and data analysis, and frequently engage with external partners for marketing services. In a recent study, Gartner found that Marketing spends more on technology than IT. Many individuals resort to sharing a single license for these tools.
Social Media	The social media team manages dozens (sometimes hundreds) of social accounts and content production, distribution, and data analysis tools. Many of these services do not support SAML SSO and cannot be federated, especially if the login is shared with multiple people.
Engineering / Development	As the lifeblood of many products, this team must share a company's secret notes, utilize internal and external tools and teams to accomplish product updates or releases against strict timelines.
Human Resources	The Human Resources team typically uses tools to oversee recruiting, payroll, employee benefits, performance, and attendance tracking. When employees join or depart the team, they need to be added or removed from the directory quickly.
Finance/Accounting/Legal	The Finance, Accounting, or Legal team typically uses tools to manage budgeting, earnings, costs, corporate credit or P-cards, electronic signatures, and strategic decision-making –some of your business' most confidential data.
Support/ Customer Services	This team typically uses tools to manage help desk tickets, bug reporting and tracking, product testing, and troubleshooting. Often, this team needs anywhere access immediately and a password manager that has the policies to allow for this.
Everyone Else	A consultant, an intern, office manager, operations leader – the list goes on. Whether your business includes individuals, departments, small or large teams, you must be able to securely collaborate. Everyone needs a password manager.

Get in Touch

Don't let one reused password put your entire business at risk.