LastPass

SOLUTION OVERVIEW

LastPass Security Overview

At every step, LastPass is designed to protect what you store.

Your information is kept safe through:

- **A proven security model,** setting the standard for transparency and best practices
- **Local encryption,** ensuring sensitive information is obscured before it's synced to LastPass
- **Powerful security features,** to give you tools to protect against threats and attacks

Stronger security

Greater control

Improved experience

Better compliance

Proven Security Model

LastPass is market-tested by over 100,000 companies, including Fortune 500 and leading tech enterprises. LastPass' infrastructure is protected by best practices, including regular updates and using redundant data centers to reduce the risk of downtime or a single-point-of-failure. Customers can trust LastPass' proven security model, including:

Service Organization Control 2 (SOC 2) Type II compliance: The SOC 2 Type II is a detailed review and validation of LastPass controls and processes to confirm products and systems are designed to be secure and reliable. As a widely recognized "gold standard" for software companies, completing and maintaining the SOC 2 is one of the many ways LastPass demonstrates a strong commitment to security and service availability.

ISO/IEC 27001:2013 Certified: LastPass has acquired ISO/IEC 27001:2013 certification from an industry leading certification body. The ISO 27001 certification provides requirements for an information security management system (ISMS). LastPass has the proven ability to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.

Regular audits and penetration tests: LastPass utilizes trusted, world-class, third-party security firms to conduct routine audits and testing of the LastPass service and infrastructure, including a detailed internal penetration test performed quarterly.

TLS for secure data transfer: Even though sensitive data is encrypted with AES-256, the TLS protocol secures the connection to LastPass to further protect a user's data from man-in-the-middle attacks.

Reliable service and storage: LastPass is operated out of multiple, geographically distributed facilities with redundancy. LastPass operates in two data centers in the United States and two in Europe. All data centers are in world-class hosting facilities that constantly monitor environmental conditions and provide 24-7 physical security. Business account holders can request that their vault data be stored locally in Europe, Australia, Singapore, or India instead of the United States.

Bug bounty program: LastPass incentivizes responsible disclosure and improvements to the service through the work of top security researchers: https://bugcrowd.com/lastpass. If an issue arises, an investigation is launched, followed by verification, leading to a quick resolution of any bug reports or vulnerabilities according to a documented incident response plan.

Secure Product Architecture

Securing an account begins the moment it's created. When a LastPass user creates their master password, it's used to generate a unique encryption key, even when enabling passwordless login. The master password and the encryption key are never sent to or shared with LastPass; they are only ever encrypted locally on the user's device. The encrypted data is unusable without that key. Further security product architecture details include:

Private master password: LastPass does not send or store the master password and cannot access your account.

End-point encryption: LastPass is devised to allow only the user to decrypt and access their vault. Encryption happens exclusively at the device level, rather than on LastPass' servers. Sensitive data is encrypted before being synced to LastPass for safe storage.

256-bit AES encryption: This algorithm is widely accepted as impenetrable – it's the same encryption type utilized by banks and the military.

PBKDF2-SHA256 for brute-force attacks: PBKDF2 strengthens the master password and encryption key against large-scale, brute-force attacks by increasing the amount of time it takes to make even one guess for a password. LastPass uses SHA-256 and performs 100,100 rounds of PBKDF2 to create the encryption key, before creating the user's login hash. By slowing down brute force attacks, PBDKF2 makes it difficult to try cracking even just one master password.

Powerful Security Features

LastPass also empowers customers to take security into their own hands. Available features and functionality augment the security of their LastPass account and improve their overall security posture, including:

Multifactor authentication: LastPass MFA offers adaptive authentication for added security with a flexible user experience. LastPass also integrates with leading authentication providers.

Passwordless login to the vault: Users can enable passwordless login to the LastPass vault via the LastPass Authenticator App, removing the need to enter a master password on trusted devices.

Business controls: Over 100 configurable policies help create a custom security environment, at a global or granular level, including restricting access to trusted locations. The admin dashboard gives visibility into the access security of the entire organization.

Automatic locks: LastPass can log out when a user steps away from a computer or loses a device.

Password audits: Identify and replace any weak, reused, compromised, and old passwords, across the organization.

Phishing protection: LastPass will only fill in passwords on sites that are saved and trusted.

For more in-depth technical details about the LastPass security, please see the LastPass Technical Whitepaper.