LastPass •••|

SOLUTION OVERVIEW

LastPass Security Overview

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

As a company that stores your most sensitive data and information, security and privacy are non-negotiable. Communicating clearly, transparently, and freqently on data security and privacy is critical to earning your trust.

Additionally, LastPass invests in security at the corporate policy and product level to ensure you are confident when it comes to securing your business with password management. Below these items are summarized, but you can always review progress via the LastPass roadmap, located on the support site.

Stronger Security

Proven Security Measures and Controls

LastPass is market-tested by over 100,000 companies, including Fortune 500 and leading tech enterprises. LastPass' infrastructure is protected by best practices to securely store and encrypt customer data, ensuring data is protected not only from external threats, but inaccessible to LastPass as well.

Full Transparency

Security and encryption best practices: LastPass is a host-proof solution, meaning it is designed to ensure that the user – and only the user (or their admin) – can access their sensitive data. Sensitive data is encrypted (using a key that we never have) locally in a 'vault' that is stored on the end user's device and on our servers. LastPass' encryption and cryptography standards defend against brute-force attacks.

Strict Privacy

Industry-tested compliance: LastPass holds third-party security certifications like ISO 27001, SOC2 Type II, SOC3, BSI C5, TRUSTe, and more. Completing and maintaining this compliance is just one way we demonstrate our commitment to data security, safeguarding of information, and service availability.

Top-level global data storage: LastPass uses data storage in world-class hosting facilities that follow best practices for redundancy and stability.

Timely incident response: Our team reacts quickly to investigate, verify, and resolve or mitigate reports of bugs or vulnerabilities. Our bug bounty program incentivizes responsible disclosure and improvements to our service. LastPass and our customers benefit from the positive relationship we maintain with top security researchers.

Better Compliance

Regular audits and penetration tests: We engage trusted, world-class, third-party security firms to conduct routine audits and annual testing of the LastPass service and infrastructure.

Company-wide security measures: LastPass delivers the security technologies and controls that are typical of a software company, and we continually evaluate new methods and solutions based on the evolving threat landscape. These controls exist across LastPass infrastructure, endpoints, and cloud estates, allowing us to bolster our security posture.

Experienced security professionals: LastPass has and will continue to expand our security team significantly, spreading and honing security expertise across all dimensions of the business. Some examples include: threat intel, detection and response, and security architecture.

Secure Product Architecture

LastPass continues to make investments in the security and technology of our product, demonstrating our committment to protect customers.

Strong Master Password: When a user registers their LastPass account, they begin by creating a strong master password. Using their master password and email address, an encryption key and an authentication hash are derived.

Local only encryption: The master password is never sent to LastPass and therefore cannot be recovered using typical password recovery methods. The vault can only be decrypted by successfully entering the user's email address and correct master password. Encryption happens exclusively at the device level.

AES-256 with thousands of rounds of PBKDF2 SHA-256: LastPass has implemented AES-256 with thousands of rounds of PBKDF2 SHA-256, a password-strengthening algorithm, to produce the user's encryption key. PBKDF2 is an adaptive one-way function which hashes a password multiple times with a hashing algorithm that can be chosen by the service provider. This makes it difficult for a computer to check that any one password is the correct master password during a brute-force attack.

LastPass has opted to use SHA-256, a slower hashing algorithm that provides more protection against brute-force attacks. By default, LastPass performs 600,000 rounds of the function to derive an encryption key, before a single additional round of PBKDF2 is done to create the user's login hash.

LastPass can increase the number of rounds over time to render brute-forcing the master password infeasible even as computers advance. Users can also increase the rounds of PBKDF2 in their account settings. Increasing the number of iterations increases the work required to derive the hash. This makes verifying a password take longer, but in turn it also significantly increases the work needed to brute-force a password with a given hash.

For more in-depth technical details about the LastPass security