LastPass •••|

Technical Whitepaper

Summary of Key Security Principles

As the leading cloud-based password vaulting and single sign-on solution, LastPass helps consumers and businesses increase productivity and decrease the likelihood of password-related breaches.

Key security features of LastPass include:

- **Universal access to data**: When you entrust your passwords to LastPass, you need to know you can always access them. Universal access is core to our service, and we endeavor to ensure you can manage and view your passwords whenever and wherever you need to. Users access their data through the LastPass plug-in or by logging in to www.lastpass.com. Pending authentication, data is available both offline and online.

- **Local-only encryption**: Sensitive data is encrypted locally in a 'vault' that is stored on the end user's device and on our servers. LastPass is a host-proof solution, meaning the system is designed to ensure that only the user can access their data.

- **Centralized control for admins**: For businesses, LastPass provides a cloud-based admin dashboard for easy deployment and management of the service. The dashboard includes configurable security policies, provisioning of shared credentials, and real-time reports. LastPass has been built to help you adapt quickly to changes in your security environment. You set your own policies based on your unique needs.

- **Security and encryption best practices**: LastPass offers industry standard, best-practice cryptography that is strong enough to defend against brute-force attacks. Sensitive data stored with LastPass is encrypted using a key that we never have.

- **SOC-2 report**: LastPass has acquired a Service Organization Control 2 (SOC 2) Type I attestation report. As the "gold standard" for software companies that is widely recognized nationwide across industries, completing and maintaining the SOC 2 attestation is just one way we demonstrate our commitment to security and privacy.

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

Table of Contents

Introduction

LastPass is a password manager trusted by millions of consumers and tens of thousands of companies worldwide to safely store their passwords and grant access to the technology and services they rely on. Our core mission at LastPass is to keep customer information secure and provide a reliable service. This document shows how we do this securely.

We help LastPass customers achieve better security in two ways:

1. Building security into the very foundation of the product, with additional layers of protection to safeguard customer data at all steps, and

2. Offering features, settings, and options that allow users and admins to customize LastPass to meet their specific security needs and follow best practices.

By building security and safeguards into the product, we strive to ensure that all LastPass users are protected from threats, both in the cloud and locally on their device.

And by offering configurable, robust security features, we can equip end users and admins alike to eliminate the poor password practices that put their private information at risk. We empower businesses and consumers to strengthen their first line of defense.

We are constantly improving the LastPass software and update our service with the latest technology as new attack vectors and security threats emerge. We work closely with members of the LastPass community and security researchers who help improve the service for the benefit of all users. LastPass fundamentally believes in taking proactive measures to review security reports, address issues, and regularly evaluate new technologies that will strengthen our security model.

Our Privacy Statement is available here (https://lastpass.com/privacy-statement) and our Terms of Service are available here (https://secure.logmein.com/home/policies/terms-and-conditions).

Logging in

The Master Password

When a user creates their LastPass account, they also create a master password. The master password is used to authenticate in to the LastPass account through the browser plug-in or by logging in to www.lastpass.com.

Once logged in, you will be able to access and input the credentials for other websites that have been stored in LastPass. The vault is the space where you can add, view, and manage credentials and other items that have been saved to LastPass. The vault is accessed by successfully entering the correct username and master password.

A strong master password

To ensure the security of their LastPass account, it is essential that users choose a strong master password for their LastPass account. The master password should be long and unique, with a mix of character types; it directly impacts the overall security of the data as other encryption keys are generated from this password.

The master password should never be used as a password for any other website or app. Even a variation of it should never be used for any other account. For example, a breach on another website could put a LastPass account at risk if a user re-uses their master password.

Users should also never share their master password with anyone, including LastPass. No one at LastPass, including our customer care team, ever needs to know the user's master password.

A moderately strong master password also ensures that a brute-force attack is unrealistic.

Protecting the master password

No one at LastPass will ever ask a user for their master password. Any requests to share the master password should be treated as a threat and reported to the team (https://lastpass.com/supportticket.php) immediately.

The encrypted vault data is meaningless to us and to anyone else without the decryption key. The key to the user's data is created from a combination of their username and master password. The master password is never sent to LastPass.

We do not recommend selecting the option to remember master password in the LastPass extension or mobile apps. Though this option is offered due to user demand, selecting the option to remember the master password reduces the security of the master password, and also makes it more likely that a user will forget it. LastPass Enterprise admins can enable a policy that prevents users from selecting remember master password.

New Device Verification

When a user logs in to their LastPass account from a new location and an unrecognized device, LastPass requires the user to complete a verification step to "trust" that new location/device.

LastPass sends a verification link to the email address used for their LastPass account (or their security email address, if one has been added to the account). Once the user clicks the verification link, the new location/device is trusted.

The next time the user logs in from that device/location they will not be asked to complete the verification step.

Multifactor Authentication

LastPass encourages users to enable multifactor authentication to add an additional layer of protection to an account. Multifactor authentication requires another piece of information before access is granted.

Multifactor authentication requires two or more authentication factors, including something the user knows (the master password), in addition to something they have (a code, a key) and/or something they are (a fingerprint). By requiring not only the master password, but also an additional login step (like a one-time password, a fingerprint swipe, a randomly-generated 6-digit code), a user adds another layer of protection against unauthorized access to their account.

If an attacker were to discover a user's Master Password, it's unlikely that they would also have access to a valid multifactor token, therefore minimizing the chance that they would be unable to gain access to the user's account.

LastPass currently supports over a dozen multifactor authentication vendors:

LastPass Authenticator

RSA SecurID


Google Authenticator

SecureAuth


Duo Security

Salesforce Authenticator

Yubico YubiKey

Transakt

Symantec VIP

Toopher


LastPass Grid


LastPass Sesame


Smart Card Authentication


Fingerprint Readers

Learn more about the options LastPass supports here (https://lastpass.com/multifactor-authentication/).

Admins can also mandate multifactor authentication through policies in the admin dashboard, requiring use of any supported multifactor authentication option or requiring use of only specific, company-approved multifactor authentication options.

Encryption Technology

Local-Only Encryption Model

LastPass employs local-only encryption, also known as "host-proof hosting". This type of solution is designed to allow only a LastPass user to decrypt and access their data. We call this "Local-Only Encryption", which means that all sensitive vault data is encrypted and decrypted exclusively on the user's local machine. All of the encryption work is being done locally, on the user's device (such as Chrome, Firefox, iPhone, Android, the Web Vault, etc.), rather than after the data syncs to LastPass' servers.

Only once data is encrypted with the user's unique encryption key is the data synced to LastPass for secure storage. Sensitive data is transmitted to LastPass as base64 encoded data, and it never touches LastPass servers in a way that can be visible to LastPass. LastPass does not have access to nor does it store the master password, which prevents LastPass from having the ability to decrypt a user's sensitive vault data.

This means that LastPass, and the employees who work here, can never access the sensitive data that a user stores in their vault nor can LastPass remotely access a user's device. The data stored in LastPass is decrypted the instant it is needed on the user's device, after the master password is successfully entered, including when the user is accessing their account via the web vault and any of the mobile apps.

Account Lockout

LastPass also protects against brute-force attacks by locking accounts after repeated failed attempts to login. We regularly monitor accounts for signs of irregular or suspicious activity and will suspend accounts automatically when appropriate.

AES 256-bit Encryption

LastPass uses encryption and hashing algorithms of the highest standard to protect user data. Local-only encryption and locally-created, one-way salted hashes provide LastPass users with the best of both worlds: Complete security, with online accessibility, and syncing through the cloud.

LastPass encrypts user data with the trusted algorithm Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode with a 256-bit key generated from each user's master password. The AES 256-bit algorithm is widely-accepted as impenetrable and is the same military-grade encryption used by banks and the US military to secure Top Secret data.

Our best line of defense is simply not having access to sensitive vault data. We believe that if LastPass can't access your data, neither can hackers.

Key Derivation

When a user creates their account, we first do a hash of the LastPass master password using the username as the salt. This is performed on the user's device (client-side).
We use a default of 5,000 rounds of PBKDF2-SHA256 to create the encryption key, on which we perform another single round of hashing, to generate the master password authentication hash (or the "login hash"). This hash is sent to the LastPass server so that we can perform an authentication check as the user is logging in. We then take that value, and use a salt (a random string per user) and do another 100,000 rounds of PBKDF2 hashing, in addition to hashing with scrypt. When the user logs in, we compare this value to what is in our database. This is the value that LastPass stores on its servers to check against when the user next logs in.

The master password and the key are never sent to our servers. Sending either of those pieces of data would give access to the user's vault. And because hashing is a one-way algorithm, LastPass cannot reverse the authentication hash that it receives.

In layman's terms: With a good master password, cracking our algorithms is unrealistic, even for the strongest of computers.

Key Strengthening with PBKDF2

LastPass has implemented AES-256 with thousands of rounds of PBKDF2 SHA-256, a password-strengthening algorithm, to create the user's unique 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.

The standard implementation of PBKDF2 uses SHA-1, a secure hashing algorithm. SHA-1 is fast, but its speed is a weakness in that brute-force attacks can be performed faster.

LastPass has opted to use SHA-256, a slower hashing algorithm that provides more protection against brute-force attacks. LastPass performs x number of rounds of the function (5,000 by default) to create the encryption key, before a single additional round of PBKDF2 is done to create your login hash.

LastPass can increase this number of rounds over time to render brute-forcing the master password nearly impossible even as computers advance. Users also have the ability to 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.

The entire process is conducted client-side. The resulting login hash is what is communicated with LastPass. LastPass uses the hash to verify that you are entering the correct master password when logging in to your account.

LastPass also performs 100,000 rounds of PBKDF2 server-side. This implementation of PBKDF2 client-side and server-side ensures that the two pieces of your data - the part that's stored offline locally and the part that's stored online on LastPass servers - are thoroughly protected.

PBKDF2 can be described as:

Derived Key = PBKDF2(PRF, Password, Salt, Iterations, Key Length)

Where:

PRF is the hash function to be used.

Password is the Master Password.

Salt consists of bits of data unique to each account used to ensure the same Master Password does not produce the same derived key.

Iterations is the desired number of iterations to run the PRF.

Key Length is the desired length of the derived key.

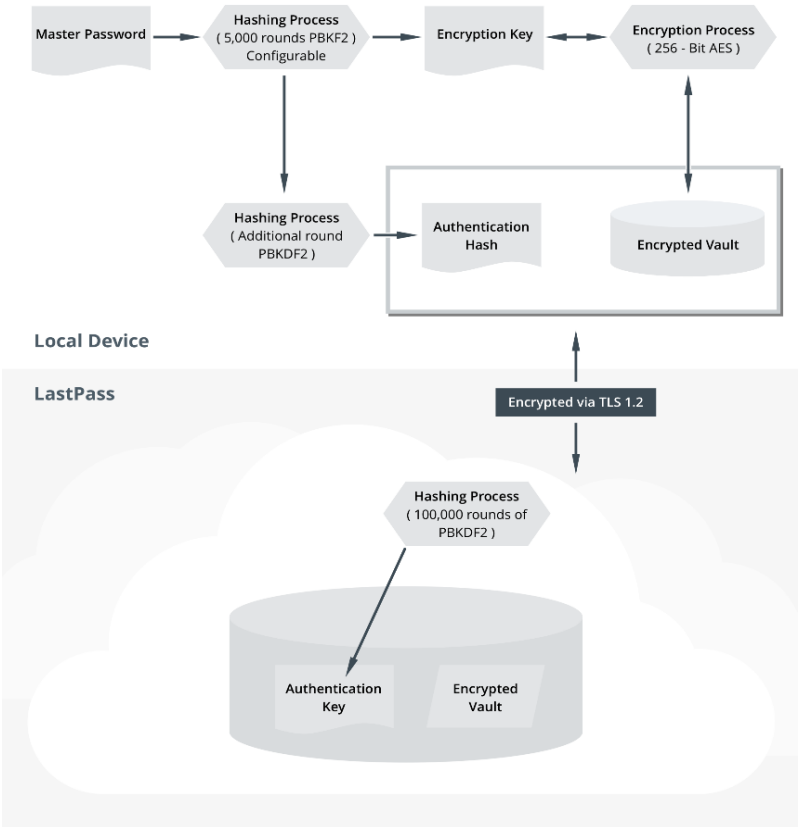
A vault encryption key is calculated with:

PBKDF2(SHA-256, Master Password, Username, 5000, 256)

To create a login hash, an extra level of PBKDF2-SHA256 is run on the user's password using the user's vault encryption key to create another 256-bit hash, thus increasing the number of iterations to 5001.

Login hash = PBKDF2(SHA-256, Master Password, Username, 5001, 256)

This hash value is sent to LastPass and used for account authentication. Additional measures are taken to protect this hash before it is stored by LastPass, as described in Storing the Login Hash section.



5,000 rounds of PBKDF2 strikes a balance between increased security and the inconvenience of longer pauses when logging in to your account. While it's tempting to point to the number of rounds when comparing implementations of PBKDF2 across services, this is essentially an apples-to-oranges comparison, as other services may be using SHA-1, which is less computationally intense than SHA-256. In other words, SHA-256 is a more intensive process than SHA-1, so a lower number of rounds can still be a higher level of security against brute-force attacks.

In terms of usability, the number of PBKDF2 rounds used only affects the process of logging in to your LastPass account. Once you gain access to your account, the implementation of these changes will not affect your browsing experience.

Note: LastPass supports a diverse set of platforms which vary greatly in speed. For the best experience across all of our supported platforms, we recommend you do not exceed 10,000 rounds. A change from 5,000 rounds to 10,000 rounds may not be perceptible to you on most platforms.

However, while we permit users to increase their rounds all the way to 200,000 rounds, you may start to notice problems when logging in via certain browsers or platforms when you go above 5,000 rounds. For example, legacy versions of Internet Explorer will be very slow with such a high number of rounds. Logging into m.lastpass.com on a smart phone (where the rounds are done in JavaScript only) may not work at all.

LastPass Enterprise Controls

LastPass Enterprise offers additional layers of control and protection to companies via the Admin Console. Admins can control the provisioning and de-provisioning of users, mandate the use of security features, and set organization-wide security policies that are customized for the unique needs of their corporate environment. A user kill switch ensures that departing or rogue employees can have access revoked in real-time.

LastPass Enterprise allows you to audit employee password habits and see if employees are reusing passwords, reusing their master password, and putting the organization at risk through their actions.

Companies also benefit from detailed reporting logs for auditing and compliance purposes. In addition to the data encryption and storage benefits, LastPass Enterprise allows companies to create password policies and data breach prevention practices that are manageable and enforceable.
Learn more about LastPass Enterprise here (https://www.lastpass.com/enterprise/).

Shared Folders

Public Key Cryptography

LastPass uses RSA public key cryptography to allow users to share credentials with trusted parties synced through LastPass. Admins and users can create Shared Folders to give appropriate access to individuals or groups, without the need to expose the credentials themselves. And even though it is shared through LastPass, LastPass is unable to decrypt the data.

RSA uses asymmetric key algorithms, where the key used to encrypt a message is different from the key used to decrypt it. Each user has a pair of cryptographic keys, one public, one private. The public key can be shared with anyone and can be used to encrypt data, while the private key is available only to the user and can be used to decrypt data encrypted with their public key.

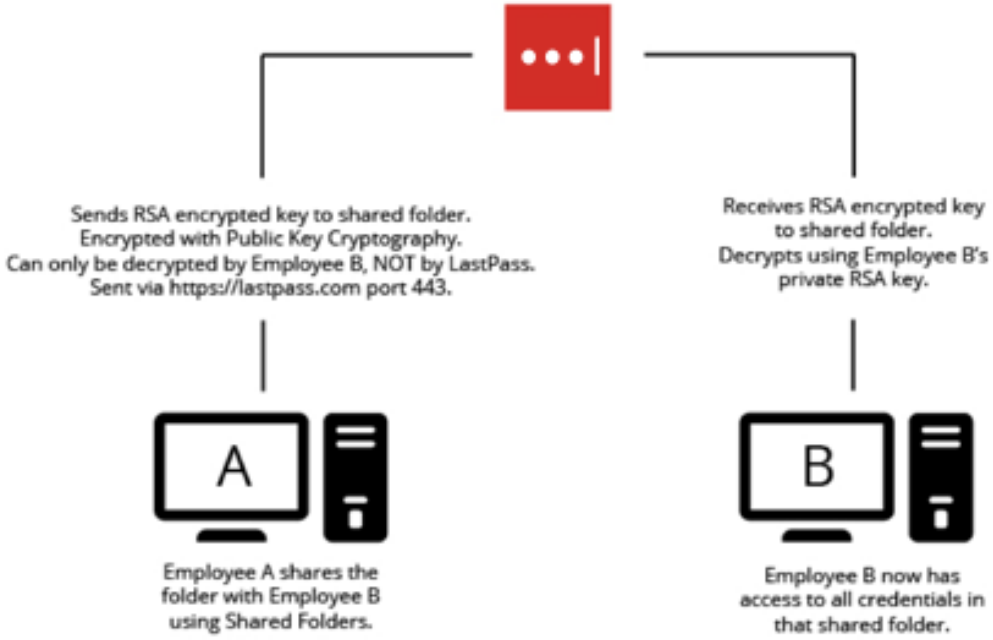
When a Shared Folder is created, a 256-bit encryption key is generated and used to encrypt the data stored in the Shared Folder. This encryption key is further encrypted with the public key of anyone invited to the Shared Folder and can be decrypted only with the invitee's corresponding private key.

All users who share folders generate a 2048-bit RSA key pair locally on their own device. The user's private key is encrypted with their vault encryption key using AES-256-bit encryption then sent to LastPass along with the user's public key. The encrypted private key is sent to LastPass so that it can be attained from other devices in the future. Public keys will be used by other users to encrypt data that can only be decrypted with the original private key.

Securing Shared Credentials

We strongly recommend using the password generator to create a unique, strong password for an account before sharing it.

When you share a credential, whether or not the password is "hidden" from the recipient in LastPass, the recipient can then launch the site that results in the autofill of the credentials. Once a shared credential is auto-filled on a website, it is outside of LastPass' control, and savvy end-users may be able to obtain the password. For example, the recipient may use the browser's developer tools to reveal the password.



Linked Accounts

LastPass users can link a personal account to a LastPass Enterprise account. By linking accounts, the user's personal vault is shared with their enterprise account. This works in much the same way as Shared Folders. The difference is that this user has the Master Password for both vaults.

Account Recovery

Because LastPass does not store the master password, it does not offer the same password reset options users may be accustomed to on other web services. If a user forgets their master password, LastPass cannot look up the master password, reset the master password, or create a new master password for the user.

One Time Passwords (OTP) can be used for account recovery if a user's Master Password is lost. Recovery OTPs are created automatically on a device when logging in.

Recovery

A random recovery key is generated on the user's device at login. This key is used to encrypt the vault encryption key (which is re-generated when logging in) using AES-128 in CBC mode. The encrypted vault key is then sent to LastPass servers while the recovery key is stored locally on the device.

The encrypted vault key is disabled and cannot be fetched from LastPass until account recovery is activated by the user. The encrypted vault key on LastPass' servers is secure because the recovery key is never shared with LastPass.

When Account Recovery is requested, a verification code is emailed or sent via SMS to the user. The user's identity is confirmed via access to the email account or phone number associated with the user's account. After verification, the encrypted vault key is downloaded and decrypted locally on the user's computer using the recovery key. The user specifies a new master password, generates a new vault encryption key, a new login hash, and then encrypts their vault data with the new key. The old encrypted files are wiped from LastPass servers, thus invalidating the old keys.

If for any reason the OTPs are not available, whether because of a software or system upgrade, or because the user does not have access to a previously-used device, then the only recourse is to delete the account to start over. LastPass cannot do anything in this case to recover the encrypted data or reset the master password, because that recovery data is only available client-side rather than server-side. Again, we've designed LastPass this way as a protective measure to reduce the risk of someone maliciously obtaining a user's sensitive data.

Account recovery OTPs can be disabled by the user, or disabled organization-wide with a LastPass Enterprise security policy.

A super admin security policy is available to Teams and Enterprise admins, allowing designated admins to reset the master password of employee accounts.

Login One Time Passwords

Users can generate and print Login One Time Passwords (OTP) on an ad hoc basis for use when logging in to LastPass on an untrusted device. A user can generate OTPs to log in on an untrusted computer in place of the master password, but they expire after first use.

They work the same way as a Recovery OTP but remain enabled until used and are not stored on a local device. Using an OTP can safeguard against keylogging on public or untrusted computers. Learn more here (https://helpdesk.lastpass.com/your-lastpass-icon/loggin-in/one-time-passwords/).

Securing the Client

The LastPass client is typically run as a browser extension that is supported for all major browsers on Windows, Mac and Linux. Native applications are also available for iOS, Android, Windows and OSX.

Communication between the client and LastPass servers uses TLS connections. The TLS configuration uses industry best practices, only allowing TLS 1.x connections with strong cipher suites.

Connections via browser extensions are further protected by browser security controls. HTTP Strict Transport Security (HSTS) forces all connections to TLS, thus mitigating the risks of downgrade attacks and misconfiguration. Content Security Policy headers provide further protection from injection attacks, such as cross site scripting.

LastPass Infrastructure

High-Availability Service

LastPass is built with full redundancy of our data centers, reducing the risk of downtime and single-point-of-failure.

Even if a user does not have internet access, they can still access their account via the LastPass browser extension or app where they have previously logged in. A secure, local copy is stored automatically when a user connects to LastPass that is then available offline.

The status of the LastPass service is currently reported here (https://twitter.com/lastpassstatus).

Service Architecture

LastPass operates in three active-active datacenters in the United States and another pair of active-active datacenters in Europe. This model increases service reliability as each datacenter can handle all user traffic. All datacenters are in world-class hosting facilities that constantly monitor environmental conditions and provide 24-7 physical security.

User vault data are backed up daily and stored offsite at a separate datacenter.

Automated nightly reviews are conducted to ensure the appropriate level of security.

LastPass systems run on a Linux system that updates automatically to maintain the latest available security updates. User data is stored in SQL and NoSQL databases.

Universal Availability

LastPass strives to offer users access to their data on as many platforms as possible, and keeps pace with new technology so that users can always rely on LastPass to securely sync their data where they need it. Information on supported platforms, browsers, and mobile devices can be found here (https://helpdesk.lastpass.com/downloading-and-installing/).

The LastPass web vault is also available at www.LastPass.com on all major browsers and platforms and via m.lastpass.com on mobile platforms. Though downloading the extensions and apps are recommended for the best experience, the web vault ensures secure access on devices where LastPass can't be installed.

Local and Cloud Storage

To ensure that you have consistent access to your data, LastPass creates an encrypted copy of the vault both locally on a user's device and in the cloud on LastPass' servers.

Protecting Data at Rest

When using the LastPass browser extensions or the LastPass mobile apps, LastPass stores a locally-encrypted, cached copy of the vault on that device. If LastPass.com can't be reached because the user has no internet connection or in the unlikely event that LastPass.com is down, the user can log in via the browser extension or the mobile app to access the stored data.

The secure offline cache is only available if the user has successfully logged in to the extension or mobile app at least once before to sync with the LastPass servers.

On Windows devices, Windows Crypto APIs are used to add an extra layer of protection.

Note that offline access can be disabled in the LastPass extension preferences or disabled company-wide with a LastPass Enterprise security policy.

User Data Storage

Sensitive vault data is encrypted client-side, then received and stored by LastPass as encrypted data. Other data, such as a phone number used for SMS account recovery, is encrypted server-side using a Hardware Security Module (HSM). The HSM is a separate device purpose built to securely store cryptographic keys.

Login Hash Storage

LastPass receives the login hash from the user (following the default 5,001 iterations on the user's master password using PBKDF2-SHA26), the login hash is additionally salted with a random 256-bit salt, and an additional 100,000 rounds of PBKDF2-SHA256 are performed. That output is then hashed using scrypt to increase the memory requirements of brute-force attacks. The resulting hash stored by LastPass is the output of 105,001 rounds of SHA256 + scrypt.

LastPass System Data

EncFS is used to encrypt system data needed to run the LastPass service. EncFS is a Filesystem in Userspace (FUSE)-based encrypted filesystem that automatically encrypts all files added to the volume. A system administrator is required to manually enter the password to decrypt the filesystem.

Transport Layer Encryption

LastPass uses TLS exclusively for secure data transfer even though the vast majority of user data is already encrypted with AES-256. This protocol protects the data from any party listening in to the network traffic. TLS ensures that the user is connecting directly to LastPass to protect against man-in-the-middle attacks.

Protecting LastPass Network and Systems

LastPass protects infrastructure and customer data with best practices and regularly-upgraded systems.

Application layer firewalls and filtering

LastPass utilizes a best in class application firewall and DDoS prevention service. Traffic to LastPass services is proxied through this service, which filters and blocks malicious traffic before it reaches LastPass servers.

LastPass runs a local application firewall on its web servers to provide an additional layer of protection against web application attacks. This also actively blocks malicious traffic, such as SQL injection and XSS (cross-site scripting) attacks.

Network layer firewalls and filtering

All LastPass web servers are running host-based firewalls which filter inbound and outbound connections including internal connections between LastPass systems. Only ports 80 and 443 are open to the internet.

Vulnerability Testing

Vulnerability scans are run daily against all LastPass servers, and a detailed internal penetration test is performed quarterly. LastPass also uses tools to search for common mistakes that could result in an XSS or SQL Injection attack.

Third-Party Audits

We're committed to improving LastPass through third-party audits, and LastPass infrastructure is tested by a third party on an annual basis.

Error Reporting

LastPass may also collect anonymized error reports and crash data from users to help us continually improve the service. Though users can opt-out of this when installing LastPass, note that no identifying information is used in these automated error reports, and they are solely used by the LastPass team to improve performance and security.

Code Reviews

All changes to the code base are reviewed by the technical team for security, privacy, and compliance with company policies and procedures.

SOC 2 Attestation

LastPass has acquired a Service Organization Control 2 (SOC 2) Type I attestation report from RSM US LLP. The SOC 2 report provides a rigorous audit of our security and data practices to ensure we meet key criteria. The audit is a detailed review of the controls and processes in place to ensure our products and systems are secure and reliable. This includes ensuring proper confidentiality of the data our systems handle and the availability of those systems. An annual review must be completed to maintain SOC 2 compliance.

As the "gold standard" for software companies that is widely recognized nationwide across industries, completing and maintaining the SOC 2 attestation is just one more way we demonstrate our commitment to security and privacy.

System Hardening

All LastPass systems are hardened, and patched regularly.

All servers run an industry leading Linux Security Module to enforce mandatory access controls to system files and objects. The kernel security module is configured to restrict the capabilities and privileges of running processes to the minimum privilege required, reducing the risk of vulnerabilities from other services. LastPass administrators must explicitly configure access to any files or services that a process requires to run.

Linux kernel security module configuration violations are forwarded to LastPass' centralized logging infrastructure, which helps monitor and detect possible host intrusions.

Access Controls

Access to LastPass infrastructure and systems is protected by multi-layer security and multifactor authentication. Employees are only granted access to LastPass production systems on an as-needed basis and as required by their role.

System access requires administrators to pass multiple identity checks including multifactor authentication. A secure VPN connection is required for access to the LastPass network. SSH is used for console access to servers, requiring password protected SSH keys to login.

Logging and Monitoring

System logs are forwarded to a central log server and reviewed by a log management and analytics tool. Additional tools are used to monitor network bandwidth and the health of LastPass systems, alerting LastPass personnel in the event of any issues.

Security Incidence Reporting

Security is our highest priority at LastPass, including quickly responding to and fixing reports of bugs or vulnerabilities. LastPass is in part able to achieve the highest level of security for our users by looking to our community to challenge our technology.

We appreciate the important work that the security research community provides and appreciate responsible disclosure of issues; we believe that when the security process works as designed, we all benefit.

Bug Bounty Program

LastPass participates in a bug bounty program (https://bugcrowd.com/lastpass) hosted at BugCrowd to facilitate the important work that security researchers do to find and responsibly disclose qualifying security bugs.

Local-Impact vs Broad-Impact Security Concerns

LastPass classifies security reports into two categories: A Local-Impact Security Concern that affects only you or your account, and a Broad-Impact Security Concern, which is an issue that can impact many or all LastPass users.

A local-impact security concern should be reported in a support ticket (https://lastpass.com/supportticket.php) where it will be escalated appropriately.

A broad-impact security concern should be reported through our bug bounty program at https://bugcrowd.com/lastpass.

Reporting Security Issues

When reporting potential issues, please try to be as thorough as possible in providing us enough information so that we can appropriately recreate your findings.

This may include exact steps to reproduce the bug, any links you clicked on, pages you visited, URLs, and any affected account email addresses. Please include a code sample and either images or a video recording that clearly demonstrates the exploit you have found.

If you are using automated tools to find vulnerabilities, please be aware that these tools frequently report false positives.

Responding to Security Concerns

Once you have submitted a security concern, our team will:

1. Promptly take steps to investigate the report and determine its severity.
2. Contact you directly if more information is needed.
3. Otherwise, we'll try to fix the issue, potentially with your assistance. While issues are usually fixed very quickly, deploying the fix to affected customers will be done based on the complexity and severity of the issue.
4. Once the issue is fully resolved to both your and our satisfaction, we'll close the report.