Vendor Report

Vendor Report for LastPass US LP

This report is based on publicly available information and does not consider artefacts such as external assurance reports or contract terms that may only be provided to clients. Refer to the References slide for a list of resources used to generate this report.

July 2024

LastPass US LP – Vendor Summary

LastPass, established in 2008, provides a password management service for individuals and businesses, including secure storage, management of passwords, and other sensitive information across various devices and platforms. The service enables users to create, protect, access, and share credentials. It also provides over 100 customised security policies, dark web monitoring, options for single sign-on, and multi-factor authentication (MFA). While LastPass stores and encrypts this information, end-user master passwords used to access accounts and vaults are never known to, stored or maintained by LastPass.

The pricing model of LastPass for Business includes the Teams and Business versions. The Business option is expandable with add-on features such as single sign-on and MFA. This report focuses on the Business service.

LastPass is accessible online, through a desktop application, and via iOS and Android mobile apps. Business Users must agree to the LastPass Terms of Service for Business Customers. LastPass Families can be enabled on the Business plan so that employees receive a personal LastPass account plus five additional licenses to share with family or friends. The Terms of Service for Personal Use apply. If a business buys LastPass through an authorised partner, the Terms of Service for Partner Sales apply.

LastPass US LP – Vendor Summary

In August 2022, LastPass encountered two security incidents where the threat actor exploited a vulnerability in third-party software, bypassed existing controls, and eventually accessed non-production development and backup storage environments. The threat actor stole both LastPass proprietary data and customer data. As a result, LastPass made a multi-million-dollar allocation to enhance its investment in security across people, processes, and technology.

The LastPass Trust Center and the Compliance Center provide detailed information about the following:

- Security measures and practices.
- Data privacy approach.
- Compliance with global privacy and security laws and regulations.
- System performance information.

LastPass US LP – Key Risk Drivers

- Data Breaches: Users risk their data being exposed if LastPass suffers a breach due to exploited vulnerabilities, insider threats, or operational failures, which could lead to unauthorised access to stored passwords and sensitive information and the compromise of multiple accounts across various platforms.
- Encryption Breakthroughs: If cryptographic standards employed by LastPass are broken, perhaps due to advancements in quantum computing, then the encrypted data stored by users on LastPass could be decrypted by unauthorised parties, leading to a severe loss of privacy and security.
- Third-Party Integration Security: Integrating LastPass with other applications increases the complexity of security management. Each integration point can introduce vulnerabilities, especially if those third-party applications are compromised or poorly secured.
- Availability Issues and Dependencies: Reliance on LastPass for access to multiple services can be problematic if LastPass experiences downtime due to operational or technical issues, which could hinder users from accessing their online accounts, leading to operational delays for businesses. Users are dependent on the continuous availability and security of the cloud platforms hosting LastPass. Any disruptions or compromises of these services could impact their ability to access their data securely and reliably.

LastPass US LP – Key Risk Drivers

- Dependency on a Single Credential: The security of information stored on LastPass heavily relies on users maintaining strong master passwords and handling their recovery options securely. Poor practices, such as using weak passwords or sharing login credentials, can lead to account compromises. If this master password is compromised, potentially through phishing attacks or malware, it could allow attackers access to data stored in numerous web applications.
- Internal Threats: Employees of a LastPass customer with access to the LastPass admin console could misuse their access to sensitive company credentials, especially if internal controls and activity monitoring are poor. For example, a Super Admin could turn policies such as MFA on or off.
- Compliance and Legal Risks: Enterprises must ensure that their use of LastPass complies with data protection laws applicable in their jurisdictions. Failure to manage this could lead to legal penalties and damage to reputation if it is found that sensitive data is mishandled.
- Government Regulation and Scrutiny: Depending on the region, governments may demand access to LastPass's data, posing a privacy and security risk. Compliance with such demands might conflict with the privacy expectations of users and the legal frameworks they operate under and expose organisations to security risks if foreign governments gain access to login credentials and passwords.

Vendor Due Diligence Review – Security & Privacy Facts

Compliance and Information Security Policy & Organisation

- LastPass has several security certifications and attestations, including ISO 27001, SOC2 Type II, SOC3, BSI C5, and TRUSTe.
- LastPass has protocols to address and mitigate security incidents and vulnerabilities and collaborations with security researchers and platforms like BugCrowd.
- Changes to policies and procedures are reviewed and approved by the Chief Information Security Officer (CISO).
- LastPass utilises third-party security firms to conduct routine audits and testing of the LastPass service and infrastructure, including internal penetration tests performed quarterly. Refer to LastPass Security Overview for more details.
- LastPass educates new hires and staff on security policies and ethics at orientation, providing mandatory annual training and ongoing updates through various programs and materials managed by Talent Development and the Security Team.

Vendor Due Diligence Review – Security & Privacy Facts

Infrastructure and Network Security

- Regardless of account type, the vault and account data for new LastPass accounts are stored in the United States by default.
- The vault data of Premium, Families, or Teams accounts is stored in the United States and cannot be moved.
- Business account holders can request that their vault data be stored locally in Europe, Australia, Singapore, or India instead of the United States, with the option to revert to the United States if required.
- LastPass implemented perimeter protection measures to secure its infrastructure, including intrusion detection systems, critical file monitoring, hosted and local application firewalls to block malicious traffic and DDoS attacks, and host-based firewalls on its servers to manage internal and external connections.
- LastPass is powered by the cloud hosting services Amazon Web Services (AWS), Microsoft Azure, and Switch. Some subservice organisation controls are covered in the SOC 3 report.

Vendor Due Diligence Review – Security & Privacy Facts

Infrastructure and Network Security

- Environmental protections in the data centres housing LastPass production servers include heating, ventilation, and air conditioning temperature control, fire suppression systems, uninterruptible power supplies, smoke detectors, and either raised floors or comprehensive cable management, as appropriate for the relevant system.
- LastPass uses multiple monitoring systems such as Security Incident and Event Management (SIEM), platform monitoring for Amazon and Azure, system and performance monitoring, system server logs, error logs, security audit trails, Advanced Endpoint Protection (AEP) technology, and threat intelligence monitoring.
- The network infrastructure employs a standard set of redundant components, including load balancers, advanced firewalls, gateways (NAT, Internet), Virtual Private Clouds (VPCs) with subnets and routing tables, Network Access Control Lists (NACLs) and allowlisting, and a network intrusion detection system.
- Third-party security firms conduct quarterly audits and detailed internal penetration tests to ensure robust security. Additional details on network and data centre security are available in the SOC 3 report.

Vendor Due Diligence Review – Security & Privacy Facts

Access Control and Encryption

- LastPass implemented a physical security program to provide access control to its offices worldwide, encompassing secure entry systems and managing access permissions for new employees and visitors.
- LastPass has strict logical access control measures, including role-based permission assignments, MFA, and access restrictions based on employee responsibilities. Additionally, access permissions are subject to regular review. Refer to the SOC 3 report for more details.
- LastPass supports MFA and passwordless authentication options for customers on specific plans. Refer to the Technical white paper for more details.
- Customer content in transit is first encrypted using AES-256 CBC mode and then again via Transport Layer Security (TLS) protocols when sent over HTTPS. In addition, LastPass uses the latest version of Secure Shell (SSH) with strong cipher suites for specified administrative functions.
- Sensitive vault data is encrypted client-side using a master password to generate a unique encryption key with AES-256 and PBKDF2, ensuring that data remains secure before it is stored on LastPass servers.
- LastPass operates on a zero-knowledge security model, meaning it cannot access users' Master Passwords, vaults, or vault data.

Vendor Due Diligence Review – Security & Privacy Facts

Application and Operational Security

- LastPass notes that its application security program follows the Microsoft Security Development Lifecycle(SDL) to secure product code. The core elements are manual code reviews, threat modelling, static code analysis, dynamic analysis, and system hardening.
- LastPass has a public bug bounty program at BugCrowd.
- Databases are backed up using automated backup strategies to allow multiple copies to be available anytime. Access to stored backup media is restricted to authorised personnel based on job responsibilities.
- LastPass has an Incident Response Plan, change management procedures, business continuity and disaster management plans, and an incident management system.
- The real-time status of the LastPass service, including scheduled maintenance and past incidents, can be monitored through the Status Page.
- LastPass operates in two data centres in the United States and two in Europe, all monitoring environmental conditions and providing 24-7 physical security to safeguard infrastructure and data integrity. Refer to LastPass Security Overview for more details.

Vendor Due Diligence Review – Security & Privacy Facts

Privacy and Data Management

- LastPass notes to adhere to GDPR, CCPA, and other privacy regulations.
- LastPass restricts the storage of sensitive data, such as government-issued IDs, personal health information (PHI), and other legally protected information, unless explicit written permission is obtained due to regulatory and contractual requirements.
- LastPass retains customer content following its internal policies and procedures, applicable legal and regulatory requirements, and any contractual agreements with its customers. Refer to the SOC 3 report for more details.
- LastPass determines an appropriate data destruction approach based on industry standards and internal controls to ensure the irreversibility of data erasure when disposing of electronic data storage devices that are no longer needed, ensuring data destruction is irreversible. When hard drives containing customer content are retired, LastPass employs suitable methods to wipe the data, including rendering discs unreadable and destroying them.

Vendor Due Diligence Review – Security & Privacy Facts

Privacy and Data Management

- LastPass will only disclose customer information when legally required by a valid warrant, subpoena, court order, or similar legal process. They may also challenge or seek to limit requests they consider too broad or unclear. Refer to the Government Request Policy for more details.
- The Privacy Policy explains what personal data LastPass collects from visitors to the LastPass websites and/or properties and how they can use that data as a data controller.
- The Data Processing Addendum (DPA) provides the privacy and data protection terms and conditions that govern LastPass's processing of personal data on customers' behalf as a service provider and data processor.
- Sub-processors are listed on the website.
- LastPass maintains redundancy and backup and recovery processes designed to ensure service availability. For details, refer to Technical and Organisational Measures (TOMs) for LastPass.

References

https://www.lastpass.com/trust-center

https://support.lastpass.com/s/document-item?language=en_US&bundleId=lastpass&topicId=LastPass/lastpass_security_overview.html&_LANG=enus

https://www.lastpass.com/-/media/75DAAA23E6BA46FE9ABBE1B95C841C16.pdf

https://www.lastpass.com/legal-center/privacy-policy

https://www.lastpass.com/legal-center/data-processing-addendum

https://www.lastpass.com/-/media/4a8e0540ad8a44908845d3c34817193f.pdf

https://www.lastpass.com/legal-center/government-request-policy

https://www.lastpass.com/-/media/175854c49fcb489baeaa87e78579e28f.pdf

https://www.lastpass.com/legal-center/terms-of-service/personal

NEED A DETAILED RISK ASSESSMENT OR VENDOR REVIEW?

GET IN TOUCH

Katja Feldtmann

0800 029 237

security@cybershore.co.nz

www.cybershore.co.nz