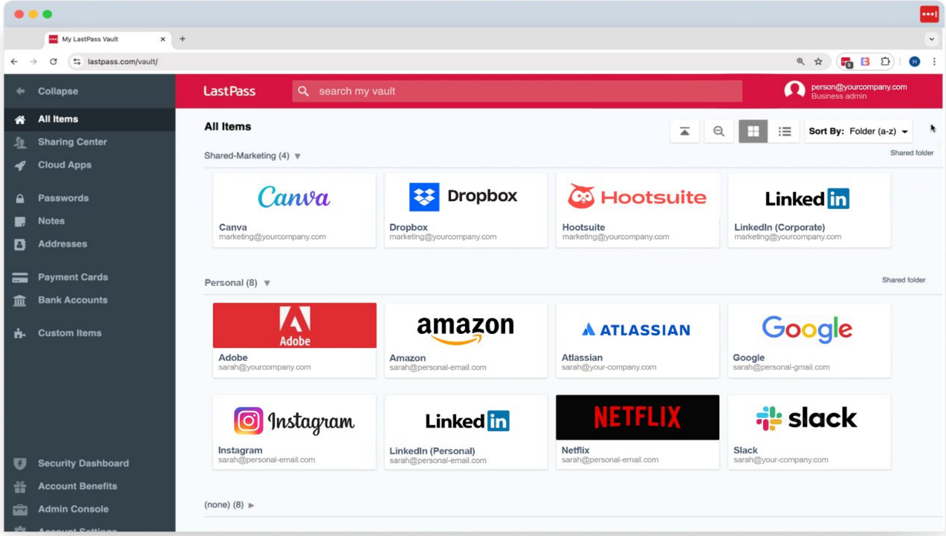
INFO~TECH
RESEARCH GROUP

Securing Digital Identities: Exploring LastPass' Features, Security, and Market Strategy

Carlos E. Rivera

Principal Research Advisor,
Info-Tech Research Group

I was interested in briefing with LastPass, as I had many questions that I wanted to ask that often come up in my member advisory sessions. I should add that I have personally been using the product since before the GoTo acquisition in 2015 and have seen the product significantly transform since their 2022 security incident (more on that later in this article). Let's begin with the company background: LastPass serves nearly 100,000 business customers and approximately 1.6 million paying customers, with thousands more on freemium accounts. The company employs around 860 people globally, with a significant presence in the US, Guatemala, Hungary, the UK, and a growing team in the APAC region. Notably, about two-thirds of their B2B customers are in North America, with Europe, APAC, and South America also being key markets.



Source: LastPass, Analyst Briefing Demo (October 2024)

Market Presence

LastPass has a significant market share, particularly in North America, where two-thirds of their B2B customers reside – mostly in the US, though with a notable presence in Canada and Mexico. The company also has a strong footprint in Europe, especially in the UK, Switzerland, and France. In the Asia-Pacific region, Australia, New Zealand, India, and Japan are key markets, while in South America, Brazil stands out.

Security Incident and LastPass’ Response

The 2022 security incident was a pivotal moment for LastPass, leading to significant changes. The breach in October 2022 led to immediate action toward rebuilding trust and enhancing security protocols. We are at a place in cybersecurity where it’s not a matter of if you have had a security breach, but when you have one and how you respond. LastPass, like a true championship prize fighter, picked themselves back up and used this opportunity to build back stronger than ever. This is evidenced by the immediate changes they made:

- **Christofer Hoff's role:** As the Chief Security and Technology Officer, Hoff has been central to these changes, focusing on a new cloud-native infrastructure.
- **Divestiture from GoTo:** Completed in April 2024, this separation allowed LastPass to concentrate solely on security enhancements.
- **Security enhancements:** Since the incident, LastPass has developed eight security-focused teams and integrated security into the product development lifecycle from the ground up.

It’s important to also call out Lastpass’ commitment to security by way of the security certifications they have achieved since the security incident. These include: SOC2 Type II, ISO 27001, ISO 27701, SOC3, BSI C5, TRUSTe, and an Independent Security Review by Google Play.

Leadership and Security Evolution

Following their 2022 security incident, LastPass underwent a strategic divestiture from GoTo, enhancing their focus on security. Under the leadership of Christofer Hoff, the Chief Security and Technology Officer, LastPass revamped their infrastructure to be cloud-native, emphasizing security by design. This initiative included expanding the security team, with a significant portion of their workforce now dedicated to security roles, reflecting a robust commitment to cybersecurity.

Market Positioning and Competition

In the realm of digital credential management, LastPass competes with entities like Keeper, 1Password, Dashlane, Bitwarden, and NordPass. Its market strategy focuses on small to mid-market enterprises, offering tailored features that align with the needs of businesses without extensive IT infrastructures.

Target Customers

The primary market for LastPass includes very small businesses up to mid-market enterprises (0 to 3,000 employees). These businesses often have limited IT resources, making LastPass' ease of use and security features particularly appealing. Decision-makers in these companies, who might also wear multiple hats including IT, find LastPass' solutions accessible and reliable.

Summary of customer segments:

- **Very small businesses:** Often managed by owners or founders, they rely on recommendations from resellers.
- **Small to mid-sized businesses:** These businesses value straightforward implementation with small IT support.
- **Enterprise customers:** They have more complex needs, often starting with adoption in one business unit before expanding.

Distribution Channels

LastPass' products are distributed through direct e-commerce sales and through partnerships with managed service providers (MSPs) and resellers. This dual-channel approach helps in reaching different segments effectively, with the e-commerce channel being favored for its simplicity. Additionally, there's a notable "flywheel effect," where personal use influences business adoption.

Data Encryption Practices

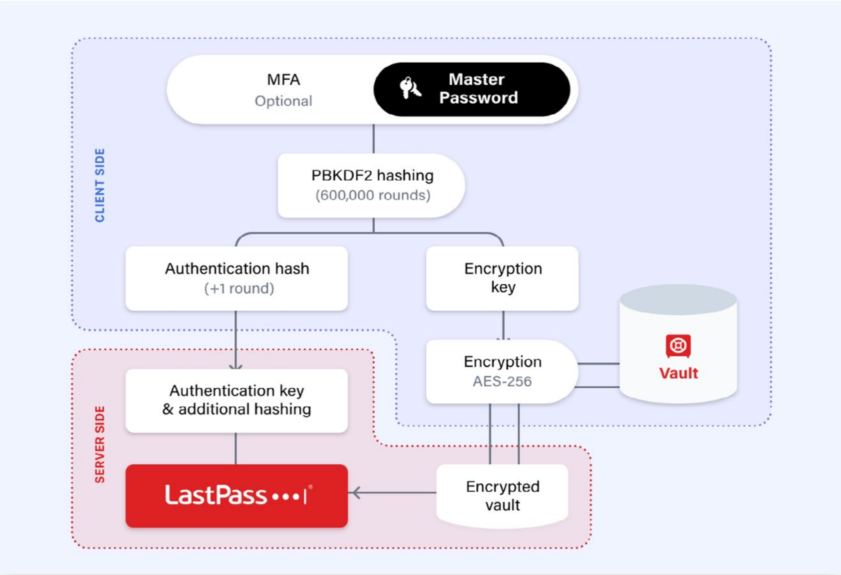
LastPass employs a zero-knowledge security model, ensuring that the company does not have access to users' vault contents. The data within these vaults, including credentials and personal information, are encrypted using password-based key derivation function 2 (PBKDF2). PBKDF2 is a key derivation function that is used to reduce the vulnerability of encryption keys to brute-force attacks by making it computationally expensive to derive the key from the password. I think it's important we understand how it benefits credential vaults:

- **Slow hashing:** PBKDF2 intentionally takes longer to compute. By running the hashing function multiple times, it significantly increases the time required to test each password guess, making brute-force attacks much less feasible.
- **Key stretch:** It stretches the original password into a longer key or a set of keys. This means that even if two users choose the same password, the derived keys can be different due to the use of a salt (a random value added to the password before hashing), which is unique per entry.
- **Salt addition:** As described above, PBKDF2 uses a salt, which adds randomness to the hashing process. This prevents attackers from using precomputed tables (rainbow tables) to crack passwords, as each password hash will be unique even if passwords are the same.
- **Security in storage:** In credential vaults like LastPass:

- **Password protection:** PBKDF2 helps in securely storing passwords. When a user saves a password, it's not stored in plain text but is hashed using PBKDF2, making it difficult for anyone with access to the storage to read the passwords.
- **Key derivation:** The derived key can be used for encrypting other data in the vault or for authentication purposes. This means that even if someone gains access to the encrypted data, without knowing the original password, they can't derive the key needed to decrypt it.

The company is also in the process of encrypting URL fields, aiming to encrypt everything feasible without compromising user experience.

- **Encryption improvements:** LastPass has been enhancing their encryption capabilities, notably by encrypting primary URL fields to prevent credential-URL linkage in breaches.
- **Zero-knowledge encryption:** Using PBKDF2, LastPass ensures that even they cannot access the encrypted data within users' vaults.
- **Field-level encryption:** Each data field within the vault is encrypted, covering not just passwords but also personal details like names and credit card numbers.

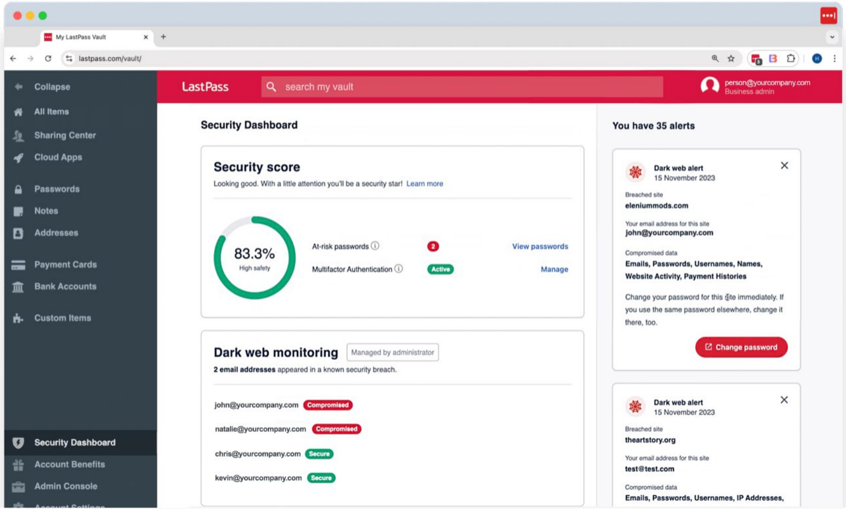


Source: LastPass, Analyst Briefing Demo (October 2024)

Vault Content Protection

The security of LastPass vaults is multifaceted:

- **Secure vaulting:** Encrypted storage for all sensitive data.
- **Multifactor authentication (MFA):** Access to the vault requires an additional security layer.
- **Dark web monitoring:** Alerts users if their data is compromised and publicly exposed.
- **Integration with SIEM platforms:** For enhanced security monitoring and response.
- **SaaS app discovery:** Upcoming features will allow IT admins to monitor and control application access.



Security Dashboard

Security score

Looking good. With a little attention you'll be a security star! Learn more

83.3% High safety

At-risk passwords: 2

Multifactor Authentication: Active

Dark web monitoring (Managed by administrator)

2 email addresses appeared in a known security breach.

john@yourcompany.com Compromised
natalie@yourcompany.com Compromised
chris@yourcompany.com Secure
kevin@yourcompany.com Secure

You have 35 alerts

Dark web alert
15 November 2023
Breached site
eleniummods.com
Your email address for this site
john@yourcompany.com
Compromised data
Emails, Passwords, Usernames, Names, Website Activity, Payment Histories

Change your password for this site immediately. If you use the same password elsewhere, change it there, too.

Dark web alert
15 November 2023
Breached site
theartstory.org
Your email address for this site
test@test.com
Compromised data
Emails, Passwords, Usernames, IP Addresses,

Source: LastPass, Analyst Briefing Demo (October 2024)

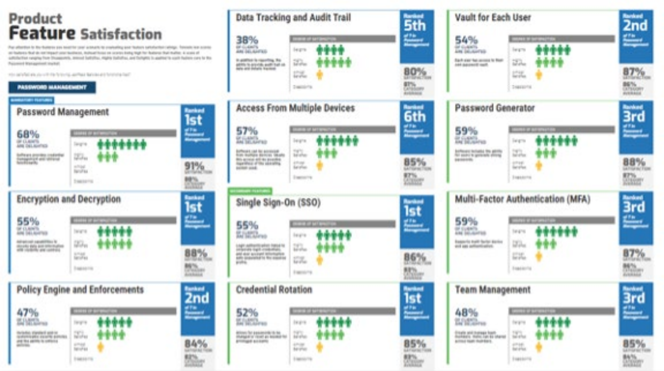
Passkey (FIDO2) Support

Looking forward, LastPass is developing support for passkeys based on FIDO2 standards. Currently in internal beta, the feature is slated for a broader release in mid-2025, starting with consumer-focused applications. This move aims to position LastPass at the forefront of adopting emerging authentication technologies.

Account Recovery and Digital Legacy

For “break-glass” functionality and users facing account access issues, LastPass provides:

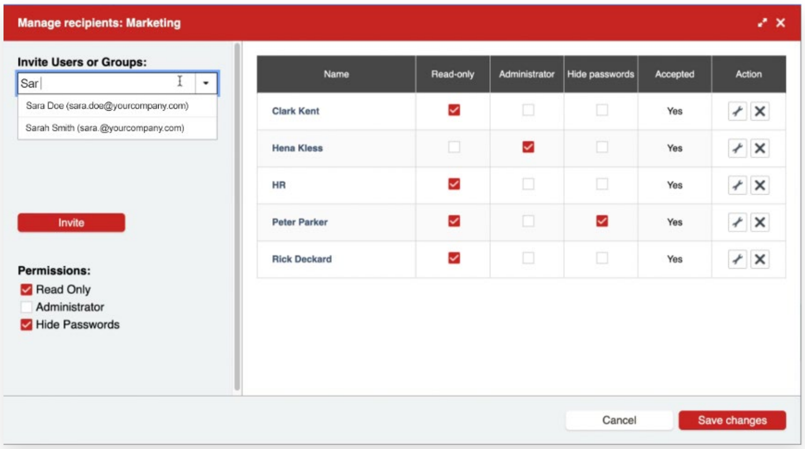
- **Emergency access:** Allows users to designate emergency contacts with vault access.
- **Recovery options:** Users can use recovery codes or seek support for account recovery, ensuring continuity and access in various scenarios.



Source: Software Reviews, LastPass scorecard (2024)

Other Notable Capabilities

- **Dual use:** LastPass provides functionality for users to manage both personal and professional credentials securely.
- **Local caching:** LastPass allows users to securely access their credentials offline on mobile and desktop applications in case there is no internet connection.



Manage recipients: Marketing

Invite Users or Groups:

Sar

Sara Doe (sara.doe@yourcompany.com)

Sarah Smith (sara.@yourcompany.com)

Invite

Permissions:

☑ Read Only
□ Administrator
☑ Hide Passwords

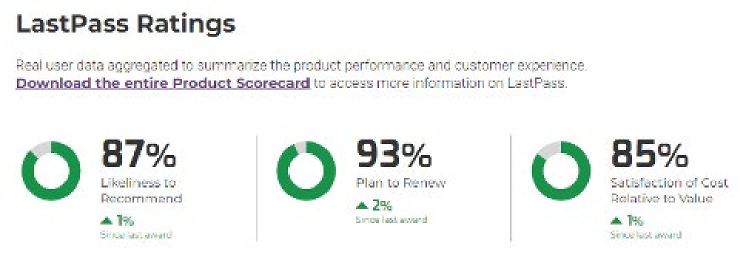
Name	Read-only	Administrator	Hide passwords	Accepted	Action
Clark Kent	☑	□	□	Yes	✎ ✕
Hena Kless	□	☑	□	Yes	✎ ✕
HR	☑	□	□	Yes	✎ ✕
Peter Parker	☑	□	☑	Yes	✎ ✕
Rick Deckard	☑	□	□	Yes	✎ ✕

Cancel | Save changes

Source: LastPass, Analyst Briefing Demo (October 2024)

Our Take

LastPass, through their strategic focus on security, user-friendly design, and robust market presence, continues to be a pivotal player in the password management landscape. The impact of the 2022 security incident is undeniable, but it has fueled their ongoing enhancements in encryption, support for new authentication methods like passkeys, and comprehensive recovery options that underscore their commitment to user security and ease of use. As digital threats evolve, LastPass' proactive security measures will continue to gain momentum and improve their market strategy, positioning them well to serve their diverse clientele effectively.



LastPass Ratings

Real user data aggregated to summarize the product performance and customer experience.
Download the entire Product Scorecard to access more information on LastPass.

87%
Likeliness to Recommend
▲ 1%
Since last award

93%
Plan to Renew
▲ 2%
Since last award

85%
Satisfaction of Cost Relative to Value
▲ 1%
Since last award

Source: Software Reviews (2024)