Reseller Sales Battle Card

Overview

From startups to large enterprises, more than 100,000 businesses and millions of end users worldwide trust LastPass for their cybersecurity needs. With LastPass, customers enjoy an easy way to create, store, manage and share sensitive data across their organizations –from passwords to passkeys (coming soon) and beyond—all without adding burden to their IT teams.

Why Sell LastPass?

Selling LastPass gives resellers the chance to offer a trusted, award-winning solution for simple, secure credential management across businesses of all sizes. LastPass is committed to its partners by offering high margins and strong incentives to help drive profitability, growth, and customer loyalty for resellers. Through our Partner Program, LastPass offers comprehensive support such as marketing and sales resources, promotional campaigns and product training.

Key Benefits for You:

1. Business Growth Opportunity

- Gain new revenue streams.
- Increase your MRR/ARR.
- Boost income and account penetration with add-on solutions.
- Offer customers greater operational efficiency: Adopting a password management solution reduces the number of Help Desk tickets by 25-40 percent.

2. Deliver World-Class Password Security and Improved User Experience

- Enforce password management best practices to increase security.
- With LastPass, customers no longer need to choose between password security and ease of use.
- Each user enjoys a personal vault to store and manage credentials that is secure and easy to use.
- Dark Web Monitoring and Comprehensive Security Dashboards.
- Customers can securely collaborate with teams across their organization, sharing access without sharing passwords. Users can grant and revoke access as needed.
- Store secure content such as product notes and credit cards.
- Securely and easily grant and revoke access to contractors and external vendors.
- Advanced policy management.

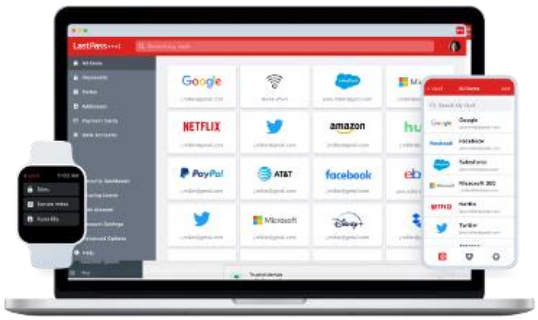
LastPass | Partner Program

LastPass is an award-winning password manager that solves your customer's biggest challenges

LastPass is a cloud-based password manager that works on any device, keeping passwords safe, private, and always within reach. It's easy to set up and simple to use, offering a seamless experience for businesses of all sizes no matter their tech needs. With LastPass, businesses can generate, share, and manage passwords with a single click or tap, putting an end to password headaches. Plus, it helps protect businesses by keeping bad actors away from important data and accounts.

LastPass Business Features

- Password management for an unlimited number of users
- Comprehensive admin console
- 100+ Security policies
- Group user management
- Directory integrations
- Advanced reporting
- Families-as-a-Benefit for all employees
- Advanced SSO and MFA adds-ons available



Compliance Certifications:

- SOC2 Type II & SOC 3
- BSI C5
- ISO 27001
- APEC CBPR and PRP Privacy Certification
- TRUSTe Enterprise Privacy Certification
- IRAP Certified
- FIDO2 Server Certification

Overcoming Objections

1. A client has implemented SSO and feels that is sufficient protection.

- This is a great opportunity to focus on the gap SSO providers leave open for all credential-based accounts. A password manager is an important and complementary solution that closes that gap. Organizations that choose to secure logins only with SSO unprotected those applications that don't integrate with SSO (e.g. corporate credit card accounts and most social accounts, i.e. Facebook).
- LastPass bridges this gap by managing all credential-based accounts not covered by SSO. This helps IT enforce password standards and provides greater visibility into all credentials used.

2. A client is using Google or Azure Vault for free to save their passwords in their browsers. Why should they use LastPass instead?

While browser-based password managers are convenient, they are more often a security liability for businesses. Web browsers may not be compliant with industry standards and may lack scalability or cross-platform functionality.

With LastPass, customers get a comprehensive suite of features designed to make managing passwords effortless and secure, ensuring that the most important credentials are always protected and within reach.

3. A client asks: How secure is the LastPass solution?

Your data is protected by the strength and quality of your master password. Your master password must be strong and unique (minimum of 12 characters, mixture of upper case, lower case, numeric, and special character values and not used anywhere else). Ideally, randomly-generated master passwords are used because their complexity and uniqueness make it significantly harder and more expensive for would-be thieves to brute force guess into the account.

LastPass offers cryptographic libraries in specific areas and has encrypted all production databases that contain customer data. LastPass has released new functionality to enforce stronger master passwords. This significantly strengthens security, privacy, user experience and operational security.

Resources

Library of Case Studies

Market POV: LastPass is rated number one in the overall grid reports for password managers by G2 for several seasons in a row, with over 70 badges awarded. Learn more here.

Partner POV: EpiOn: *"We wanted to partner with a multi-tenanted and robust tool, and LastPass was the clear front runner"* Full case study here.

Customer POV: HOLT CAT: *"I tried other password managers, but I always go back to using LastPass purely because their functionality supersedes their competitors"* Full case study here.

How LastPass Stands Out

• Innovative authentication and enhanced user security.
• Advanced threat protection and security transparency.
• Superior admin controls and support.
• Worldwide confidence and trust.