MSP Sales Battle Card

Overview

From startups to large enterprises, more than 100,000 business users 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 MSPs 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. LastPass offers an award-winning admin console purpose-built for MSPs, making it easy to grow revenues with a centralized way to manage many accounts while streamlining overhead. Our Partner Program for MSPs offers comprehensive support, such as marketing and sales resources, ready-to-go campaigns-in-a-box, and product training.

Value Drivers (What's in it for the MSP)

1. Business Growth Opportunities with the Flexibility You Need

- Introduce new revenue streams, increasing your MRR/ARR
- Continued growth opportunities with add-on solutions
- Free up your time by decreasing the number of Help Desk tickets by 25-40%
- Monthly Billing to ensure you are charged only for the seats you use
- Flexibility to add/remove clients from the admin console

2. Deliver Password Management Solution to Increase Security to Your Clients

Organization-wide password management coverage ensures that you have the appropriate volume of licenses to secure the entire business. That means all your clients can create and store passwords, secure notes, credit cards and more, but can also securely collaborate between internal teams and external vendors, partners, contractors, etc., granting and revoking access to accounts as needed.

3. LastPass Solution is Built for MSPs

The LastPass multi-tenant platform is built for seamless deployment and management, reducing the complexity of supporting multiple managed clients' accounts with varying needs all in one central dashboard. With features that protect sensitive data, simplify onboarding, automate password management and integrate with complementary security and identity access management platforms, LastPass improves operational efficiency and is readily available in eight languages.

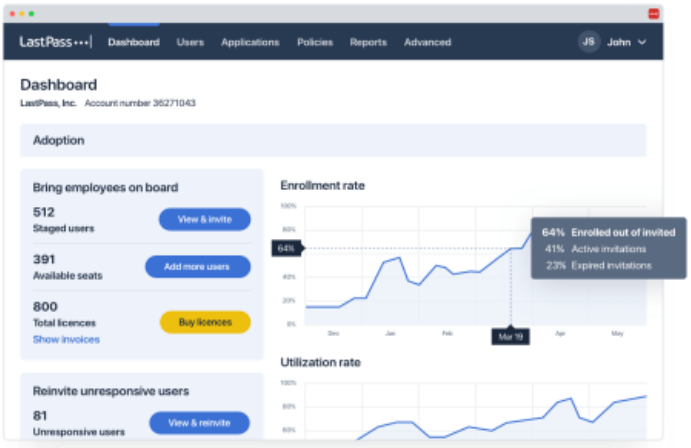
LastPass | Partner Program

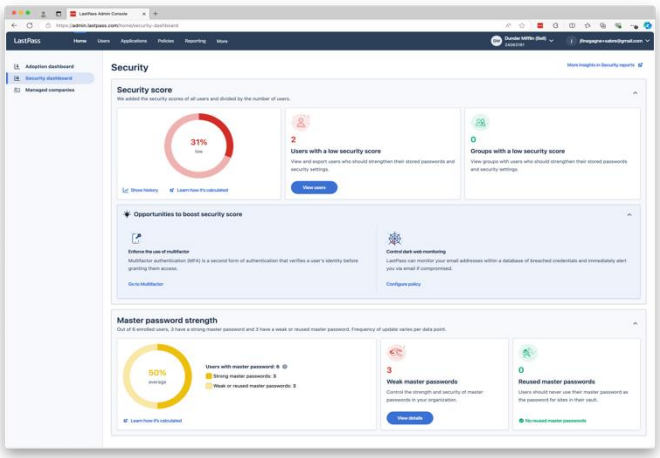
LastPass MSP Solution

Multi-tenant Centralized Password Management

LastPass Admin accounts (e.g. MSP technicians) can manage multiple independent tenants or company accounts for LastPass all from one single user account.

Managed Companies have all the features and functionality available to a LastPass account, including various multifactor authentication options, directory integrations, federated login, 120+ customizable policies, single sign-on capabilities, and much more.





Actionable Insights for Admins

- Access security reports
- Review audit reports
- Dark web monitoring
- Gain employee insights
- Role-based access control
- Company Templates to accelerate deployment <15mins.

Compliance Certifications:

- SOC2 Type II & SOC 3
- BSI C5
- ISO 27001 and 27701
- APEC CBPR and PRP Privacy Certification
- TRUSTe Enterprise Privacy Certification
- IRAP Certified
- FIDO2 Server Certification

Overcoming Objections

1. A client has SSO implemented to manage passwords.

- SaaS sprawl has become a big issue in today's enterprises of all sizes. Shadow IT, user preferences and sometimes acquisitions and mergers all contribute to the fact that there are often more apps in the ecosystem than are properly covered by IT's governance—and that includes those protected by Single Sign-On and MFA.
- An enterprise is only as safe as its weakest link. Not all applications are integrated with SSO; each user on an unprotected app is a potential attack surface. With LastPass focused on the user, every app they use must be password-protected through their Vault.
- Apps used for personal use on work computers is a huge vulnerability. Public sites like LinkedIn, Facebook and X may be left open on corporate computers and will automatically compromise the user's SSO access.
- With just SSO, IT lacks visibility into employee's password practices. This means they cannot enforce complex password rules or ensure that users are not re-using passwords across various systems and applications.

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. 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 revert to LastPass purely because their functionality supersedes their competitors"* Full case study here.

How LastPass Stands out
- Innovative authentication and enhanced security
- Advanced threat protection
- Superior admin controls and support
- Cost transparency
- Customizable controls with 120+ policies
- Greater passwordless capability
- Seamless migration from previous vaults
- Integration with PSA Tools
- Role-based security controls
- Collaboration among teams

Dedicated LastPass Strategic Partner Rep: <insert contact info>