

JANUARY 2025

An Underappreciated MSP Opportunity: Password Management

Todd Thiemann, Senior Analyst

Abstract: Managed service providers (MSPs) require better tools to support their customers’ increasingly diverse and complex password and access management needs more efficiently, cost-effectively, and securely. Solutions like LastPass enable MSPs to support key identity security requirements around password and SaaS application management, while complementing their existing service offerings. This increases value for services, while increasing the service “stickiness” with effective password management for all client users.

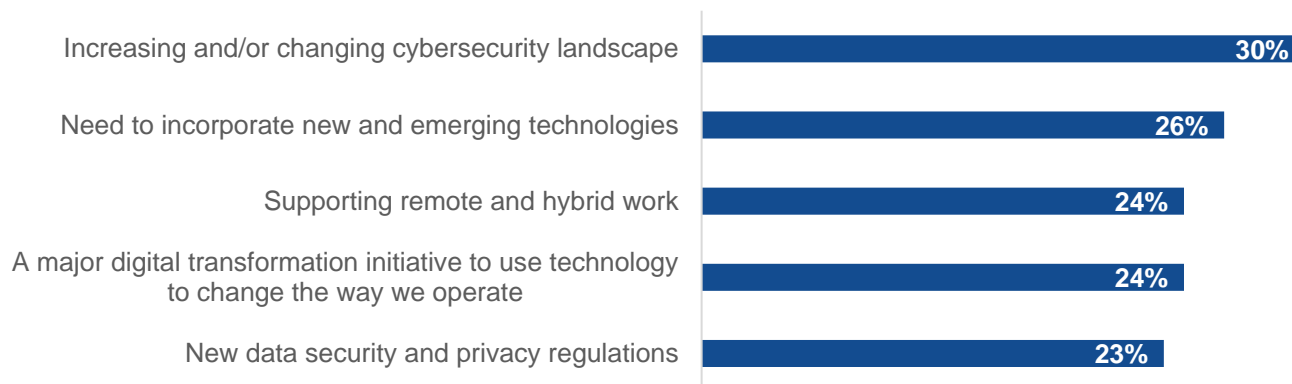
The Small and Midmarket Enterprise Complexity Conundrum

As midmarket enterprises utilize innovative technologies to increase productivity, their IT environments become increasingly complex. These enterprises have a combination of modern and legacy assets, multiple clouds, branch offices, and remote sites that increase risk with an expanded attack surface and increasing volume of accounts and applications that contain sensitive business data that can easily be lost or go unprotected.

While the expansion of IT environments has enabled organizations to conduct IT-driven activities from virtually anywhere and at any time, it also has come with challenges. As businesses evolve, operations typically become more complex. At the top of the list is a far greater degree of IT complexity. In research from TechTarget’s Enterprise Strategy Group, 30% of respondents attributed the increasing complexity of their organization’s IT environment to the changing cybersecurity landscape (see Figure 1).¹

Figure 1. Top Five Biggest Reasons Enterprise IT Environments Are Increasingly Complex

What do you believe are the biggest reasons your organization’s IT environment has become more complex over the past two years? (Percent of respondents, N=715, five responses accepted)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

¹ Source: Enterprise Strategy Group Complete Survey Results, [2024 Technology Spending Intentions Survey](#), February 2024.

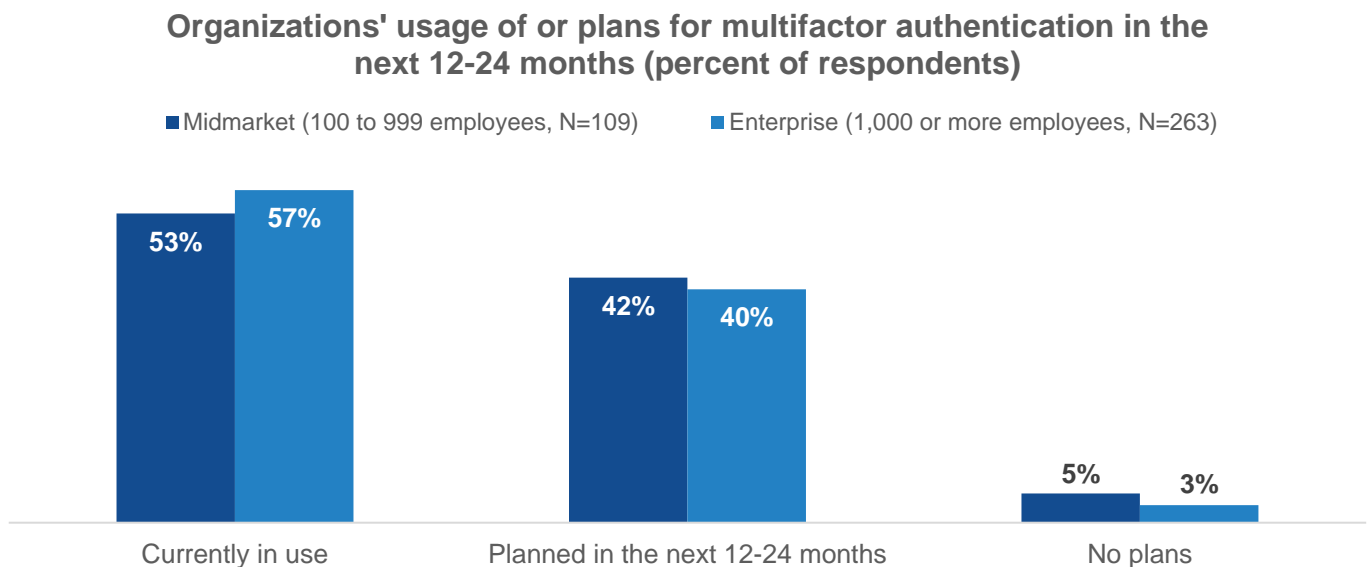
This Enterprise Strategy Group Showcase was commissioned by LastPass and is distributed under license from TechTarget, Inc.

New technologies and applications result in an increasing volume of new accounts and credentials, which creates a security challenge. Password management issues are not just about having weak or reused passwords anymore; with more apps and people working from home, things like logging in, sharing passwords, and managing who gets access to what is getting trickier and more complex. Consequently, password management has become a large vulnerability for businesses of all sizes. Compromised credentials are equivalent to the master key to a lock holding the most critical assets of an organization.

Password management poses the problem of balancing security and convenience. Organizations need to ensure security with the frequent use of single sign-on (SSO) and multifactor authentication (MFA) for access management. However, they also need to ensure convenience and avoid imposing unnecessary security “friction” on users.

While businesses have improved their password infrastructure and hygiene, much remains to be done. A simple, centralized password management tool can swiftly and effectively reduce the security workload. According to Enterprise Strategy Group research, there is room for improvement in the use of MFA, as just 53% of midmarket organizations use or plan to use MFA in the next 12-24 months, leaving 47% of the market dealing with potentially inconsistent or nonexistent password management (see Figure 2).² This is a significant security risk, given the degree to which ransomware affects small and medium-sized organizations.

Figure 2. Midmarket Organizations Are Behind in MFA Adoption



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

To better service their customers, MSPs should consider investing in enterprise password management solutions that deliver the following benefits:

- Solving a universal security issue while reducing solution portfolio complexity and management.** Password management is a prominent, painful problem experienced by every organization. The password management opportunity for MSPs contrasts with some narrow, specialized solutions that can decrease business focus. MSPs need a solution that can solve broad problems with bespoke support, flexible billing, and enablement tools to help drive adoption.

² Source: Enterprise Strategy Group Research Report, [The State of Identity Security: Opening Doors for the Right Entities and Locking Out the Bad Actors](#), July 2024.

- **Increasing value opportunities while improving MSP team efficiency.** MSPs must continually look for ways to expand offerings and attract new customers. Any new solution needs to fit into the existing portfolio, have rapid deployment, require minimal support, and prove to be effective across a broad array of customers. Margins are important, but MSPs can also increase business and revenue with streams across the maximum number of users, not simply a subset that might be active users of a niche solution.
- **Differentiation.** MSP customers have multiple options, and MSPs can struggle to provide relevant differentiation. When it comes to credential management, organizations are striving to make a solid technical choice that they can sustain for a long period of time rather than a “whitebox” offering that might offer subpar technology. They want to know that the credential management solution is technologically sound and battle-tested and that it can deliver increasing value over time.

MSPs that deliver these benefits to their clients can help them overcome their challenges around password management and improve their security posture, while at the same time growing their MSP businesses more quickly and profitably.

The LastPass Approach to Password Management

MSPs looking to better serve their SMB and midmarket customers' diverse and often-confusing environments need an easy-to-adopt, consistent, and powerful tool to manage passwords and access across the environment. LastPass has developed a solution that works for companies of all sizes and technical requirements.

LastPass has devoted considerable energies to being a trusted, reliable, and easy-to-work-with password partner for the channel. The LastPass Partner Program includes training and resources to enhance the skills and expertise of partner sales and technical teams so they can effectively sell and support LastPass solutions.

The LastPass solution is specifically designed to meet the requirements of MSPs with functionality, including multitenancy and a centralized admin console. This approach brings together essential tools, information, and assets in one place so that MSPs can better manage the different needs of a varied portfolio of customers.

LastPass differentiates its solution across the following dimensions:

- **Convenience and ease of use.** LastPass provides ease of use to facilitate productivity for all employees across all their devices. LastPass simplifies managing passwords with intuitive password features like auto-generate, auto-save, one-click autofill, and passwordless login, available on any system or device.
- **Improving collaboration.** Advantage flows to the organization that can collaborate more effectively, delivering both efficiency and resiliency. LastPass facilitates sharing and teamwork through effortless credential and folder sharing across internal and external teams, streamlined user management, and native SSO integrations with top SaaS apps.
- **Comprehensive security.** LastPass protects passwords for all users and can be deployed across all devices. The solution enforces strong and unique passwords that are stored in an encrypted vault for optimal protection. The battle-tested solution helps to protect against unauthorized access, account takeover, and data breaches.
- **Demonstrating compliance and insurability.** Organizations frequently have internal governance and external compliance requirements as well as the need to obtain cyber insurance. Being proactive about security measures can improve cyber insurability (i.e., qualifying for coverage) and contribute to lower premiums. Demonstrating compliance through password management can help an organization save time and resources through adherence to government and industry standards, frameworks, and regulations, as well as fulfilling the most common cyber insurance and customer security requirements.

Conclusion

Organizations of all sizes continue to struggle in solving the password management challenge. They want a password management solution that delivers security while improving efficiency and productivity. MSPs bringing the right technology solution to bear can benefit from bigger deal sizes, higher win rates, and shortened sales cycles, becoming more trusted partners to their customers resulting in increased and “stickier” revenue. LastPass is well suited to solving the password management problem while providing a path of least resistance for MSPs to obtain enhanced sales and margins.

©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for BrightTALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.

About Enterprise Strategy Group

TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

 contact@esg-global.com

 www.esg-global.com