



**LastPass Business**

# Reviews, tips, and advice from real users



Powered by  **PeerSpot**

# Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 8

Other Solutions Considered..... 9 - 11

ROI..... 12

Use Case..... 13 - 14

Setup..... 15 - 17

Customer Service and Support..... 18 - 21

Other Advice..... 22 - 25

Trends..... 26 - 27

About PeerSpot..... 28 - 29

# Product Recap



LastPass Business

# LastPass Business Recap

LastPass Business enhances enterprise security with features like password sharing, user deactivation, and login control. Integrated with Active Directory, it ensures password management through a security dashboard, multifactor authentication, and YubiKey support.

LastPass Business provides comprehensive password management by supporting secure storage, shared folders, and master passwords for streamlined access. With an enterprise admin console and robust reporting tools, it efficiently manages credentials. It supports secure storage for procedures and notes, crucial for IT departments. Improvement areas include group inheritance, admin capabilities, and automated password rotation. Issues like URL recognition, plugin stability, and user access reporting need addressing. Enhancements in mobile app navigation and technical support are also needed, alongside increased customization and authentication options.

## What are the key features of LastPass Business?

- Password Sharing: Allows secure credential sharing among team members.
- User Deactivation: Easily manage and deactivate user access.
- Multifactor Authentication: Enhances security with additional authentication methods.
- Security Dashboard: Provides insights into password health and security scores.
- Integration with Active Directory: Facilitates user management and credential syncing.
- Enterprise Admin Console: Centralizes admin controls for credential management.

## What benefits should users expect when evaluating LastPass Business?

- Enhanced Security: Multifactor authentication and secure storage protect sensitive data.
- Improved Access Management: Streamlines login processes and improves control.
- Efficient Credential Management: Simplifies admin tasks with reporting tools.
- Collaboration Support: Securely shares credentials among employees and contractors.
- Reduced Security Risks: Encourages complex password adoption and reduces simple password reliance.

In specific industries, LastPass Business is implemented as a vital tool for storing and synchronizing encrypted credentials, supporting robust password policies, and facilitating secure access control management. Organizations benefit from storing shared accounts and managing core enterprise admin passwords, promoting higher security standards across users and applications.

# Valuable Features

Excerpts from real customer reviews on PeerSpot:



“One feature that is really important to us is the ability to create secure notes.”



**Mike Klaus**

Senior Systems Analyst/Administrator at a agriculture with 1-10 employees



“It is easy to use.”



**Verified user**

Identity & access specialist at a consumer goods company with 5,001-10,000 employees



“The most valuable feature for me is being able to pair applications and user permissions.”



**Verified user**

Operations Engineer at a tech services company with 1,001-5,000 employees



“It's improved security; we don't have to worry about people storing password loosely and secure them.”



**Verified user**

Assistant Director of Technology Support at a university with 1,001-5,000 employees



“The most valuable feature is the liberty of keeping encrypted passwords and elevated information in a sealed vault.”



**Verified user**

Engineering at a comms service provider with 10,001+ employees



“The initial setup for this process is straightforward and extremely easy. It just works.”



**Verified user**

CEO at a legal firm with 1-10 employees



“Until now, I haven't found anything like the dashboard. It gives you a security score. I find that to be really great. The Sharing Center is really great as well. And the Security Challenge is really great too.”



**Luis Enrique**

Network Engineer at a tech services company with 1-10 employees

## What users had to say about valuable features:

“There are some alerting features in it that are quite good, like multifactor authentication. In general, it's a good product. It's rich in features and it does the job. You can invite contractors in and share it both internally and externally with set groups..”

**Mark Wight**

ICT Manager at Onefortyone

[Read full review](#) 

---

“The shared folders is an important feature. It's the primary feature we use. Also, the ability for LastPass to autofill and hide the passwords, so we don't have to keep changing passwords every time a person leaves, is valuable. .”

**Verified user**

Co-Founder at a consultancy with 51-200 employees

[Read full review](#) 

---

“I found the most valuable feature the support of the YubiKey. The capability of utilizing this hardware key was what led me to choose this product over anything else. This ensures that even if my LastPass password is compromised, nobody has access to my password vault. This gives me peace of mind..”

**Verified user**

CEO at a legal firm with 1-10 employees

[Read full review](#) 

“The most valuable feature is being able to use a single master password to access all of your other passwords.

One feature that is really important to us is the ability to create secure notes. In our scenario, these are notes such as how to get some of our devices on the network. They are processes and procedures that we don't want anybody else to see, especially within the IT department. It's a small department and we have very many processes that we use, but not on a daily basis, so we aren't going to remember them. By using LastPass and secure notes, we can go back to those notes in a secure fashion and remind ourselves how to do certain things. For instance, how to create a test database for accounting, which is something that we do once a year. We don't want that to be out in a non-secure fashion, where somebody in the public can see it..”

**Mike Klaus**

Senior Systems Analyst/Administrator at a agriculture with 1-10 employees

[Read full review](#) 



## Other Solutions Considered

“We were looking at Symantec. We are a Symantec client, that's why we are looking at them, but we felt LastPass offered more significant value for the money.”

### Verified user

Assistant Director of Technology Support at a university with 1,001-5,000 employees

---

[Read full review](#) 

“I tried another product, albeit a long time ago, and I was not pleased with it. LastPass is more intuitive when it comes to entering data and adding items. We are also able to edit data, which is easier than with our previous solution. It just seemed like it was a little more clunky, and not as cognitive..”

### Mike Klaus

Senior Systems Analyst/Administrator at a agriculture with 1-10 employees

---

[Read full review](#) 

“Prior to LastPass we used the KeePass Password Safe, which came bundled with our antivirus security solution. We switched because of the security key. I wanted that feature more than the two-factor authentication because it is an extremely strong, physical device that is used to lock down LastPass..”

**Verified user**

[Read full review](#) 


CEO at a legal firm with 1-10 employees

---

“We looked at a few products that were industry-specific, such as SCADA software, although these were not necessarily security products.

There was a security product that we reviewed, based on Active Directory, but for what it gave us, it was not a good value..”

**Mike Klaus**

[Read full review](#) 

Senior Systems Analyst/Administrator at a agriculture with 1-10 employees

---

“We have password security throughout the organization. A small group of people used infected apps. Everyone was using it differently. Some people weren't using anything to store and secure their data, which is very vulnerable. We used a variety of things, Symantec was one of the big ones that people use as far as a single use application on iPhones to better store passwords..”

**Verified user**

[Read full review](#) 

Assistant Director of Technology Support at a university with 1,001-5,000 employees

---

“I have evaluated several password managers including Norton Password Manager, KeePass Password Safe, Dashlane, and OneLogin. The LastPass solution is the best one that I have tried.

The OneLogin solution comes to mind, as it has been hacked in the past. Because we cannot review or audit their code, we need to trust that they will make changes and update their product accordingly. There is always a worry, however, that something could go wrong. I am most comfortable with LastPass because of the support for the hardware security key.

Dashlane is a good solution, but I do not like the way it looks..”

**Verified user**

[Read full review](#) 

CEO at a legal firm with 1-10 employees

# ROI

Real user quotes about their ROI:

“ROI is a hard thing to quantify. It definitely saves us a lot of time. I know for sure that it's worth the value of the license price we are currently paying, but that's why we have to reevaluate it with the price doubling..”

## Verified user

Co-Founder at a consultancy with 51-200 employees

[Read full review](#) 

---

“It's always hard to put a value on return on investment. You avoid one breach and it's paid for a million times over. We got a penetration test company internally, just to see how secure our network is, and there happened to be one bit of software that had been overlooked by an external company that managed it. It hadn't been upgraded so that managed to get them into the network. They would've been able to access through the test thing a file that we had previously. If that was a real-life scenario they would have been able to get into our network and get full access to our organization's passwords. If they did get in, they would have gotten access to the cloud. The ROI we see is that we are completely secured compared to what we had previously where there was a vulnerability..”

## Mark Wight

ICT Manager at Onefortyone

[Read full review](#) 

# Use Case

“My primary use case is related to the sharing of passwords with other members of the team. This includes the secure notes feature for very sensitive encryption information, as well as passwords for logging in..”

**Verified user**

CEO at a legal firm with 1-10 employees

[Read full review](#) 

---

“The primary use case of this solution is to manage the access control for our users.

We have twelve hundred users and two thousand applications and I manage all access to the applications..”

**Verified user**

Operations Engineer at a tech services company with 1,001-5,000 employees

[Read full review](#) 

“Our primary use case for this solution is to store the encrypted credentials, passwords, and login information for our administrative accounts. We have a lot of elevated accounts in our organization, and we needed a way to consolidate all of our user's passwords, encryption keys, etc..”

**Verified user**

[Read full review](#) 

Engineering at a comms service provider with 10,001+ employees

---

“Our main use case is a vault for passwords, but as a segue into that, we also are encouraging users to develop more secure passwords. By using this product, they won't have to have simple passwords that they can remember. They can just use the product, have it create secure passwords, and then auto-populate as they go to the various sites that they're normally going to. By doing that, we're going to create a more secure environment here..”

**Mike Klaus**

[Read full review](#) 

Senior Systems Analyst/Administrator at a agriculture with 1-10 employees

# Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

“The initial setup was straightforward. It was pretty much "plug and play," easy to pick up. I think we only had one or two training sessions for our staff..”

## Verified user

[Read full review](#) 

Assistant Director of Technology Support at a university with 1,001-5,000 employees

---

“The initial setup for this process is straightforward and extremely easy. It just works. As an example, the importing of passwords from Google Chrome works very well..”

## Verified user

[Read full review](#) 

CEO at a legal firm with 1-10 employees

---

“Overall, the initial setup is pretty straightforward. I struggled just a little bit with the browser extension at first, but after you go through it a couple of times, there is no trouble. I probably shouldn't have struggled but may have been nervous at that point. As it is now, we're able to navigate and get what we need from it..”

**Mike Klaus**

[Read full review](#) 

Senior Systems Analyst/Administrator at a agriculture with 1-10 employees

---

“The installation was not at all straightforward. Naming is hard, URL recognition is painful, and auto-fill is freaking people out. Imagine you have 100 different logins for Google (Adwords, Analytics, personal, merchant), and LastPass always fills out the first match, based on the URL..”

**Verified user**

[Read full review](#) 

System Administrator at a tech services company with 51-200 employees

---



“It was one of the easiest for implementing passwords. You can sync it with Active Directory. There were certain sites that I couldn't sync it with and I needed to input a password manually but it was really straightforward. Their interface is really easy to understand. It's not too difficult.

It took less than one day to get everybody onboard, the five people using it. It was really easy. The only thing they needed to do was import some passwords that they had and change some passwords..”

**Luis Enrique**

[Read full review](#) 

Network Engineer at a tech services company with 1-10 employees

---

“The initial setup was quite simple. It meets requirements and it was quite easy to put in. The structure is quite easy to understand and the way the security works. You could do it in a couple of hours if you really wanted to. The majority of our time was really working out how we wanted to do the security and coming to an agreement on that, which made it take longer.

It doesn't require much maintenance. Once you've got it set up it just pretty much self manages itself..”

**Mark Wight**

[Read full review](#) 

ICT Manager at Onefortytone

# Customer Service and Support

“The technical support is just okay, medium, I would say. I have had a lot of contact with them and they know that I am an experienced user, so I normally only get a manual page back.

I am not always satisfied with their solution..”

## Verified user

Operations Engineer at a tech services company with 1,001-5,000 employees

[Read full review](#) 

---

“Their technical support was very good. They generally respond via email, or they log into their service desk, and they generally post stuff up there that comes in the email to say there's been an update to a certain request. You log in and you see what the update is and you respond. I think they're overseas, so it generally does take a couple of hours to respond, and that's generally in the early hours of the morning. It would be better if they were in Australia and we got a response in the middle of the day. We deal with all different service providers and their response is more than adequate for what our requirements are..”

## Mark Wight

ICT Manager at Onefortyone

[Read full review](#) 

“We've only had to contact technical support a couple of times and my personal experience was very good.

There are some products where the support is very poor and there are some products where the support has been good. I was pleased with the speed of response and the completeness of the response that I received from LastPass so to me, that is good.

I would rate their support a ten out of ten..”

**Mike Klaus**

[Read full review](#) 

Senior Systems Analyst/Administrator at a agriculture with 1-10 employees

---

“Support answers quickly when enterprise customers call/write. Solutions are sometimes poor and un-reproducible. For example, they ask if you can logoff, login, or restart your computer which have no effect on the error reported. As well there are problems with shared credentials not available to allowed shared users and also available to not allowed users. After filing a ticket, magically it is solved without any feedback from support why this happened. This makes it really dangerous if you trust this software and by accident recognize on a client machine that the user has access to credentials which shouldnt be in the vault of the user..”

**Verified user**

[Read full review](#) 

System Administrator at a tech services company with 51-200 employees

---

“LastPass has been bounced around a bit. They are now owned by LogMeIn, so we have had a little bit of a challenge keeping track of who our account manager has been. We have found this to be confusing sometimes. You pick up the phone not knowing if you are looking for LogMeIn or LastPass. At one point, we had LogMeIn services here, so I was contacting the wrong account rep, and it took about a week to figure out who the right account rep was. So, that's a little wonky. It would be nice if they could consolidate their systems, so their customers have one view of the overarching company.

Tech support has been good. We haven't needed it much, because it is not a complex application. There is not that much you have to do with it. .”

**Verified user**

[Read full review](#) 

Senior Manager, Global Service Desk at a tech vendor with 1,001-5,000 employees

---

“My only concern up until now is the communication, especially since this is for work. They do respond but sometimes, if you want to get in contact with somebody, it's really difficult when it comes to LastPass.

For example, I started LastPass Enterprise and I tried to contact sales or a contact person. For me to actually get in touch with somebody was really difficult. I even tried to give my name and email and they told me they would get back in contact with me. At first, I thought it may be something with my email domain, that maybe something about LastPass was dropping my emails. Then I started using my live domain email. Even so, I didn't receive any contact. So, my experience with LastPass is that it's a great solution, but when it comes to communication and support, it has been tough.

When it comes to opening a ticket, they do respond within one day. But, for immediate contact, no. It was crazy, especially in the beginning because I was so enthusiastic, I wanted to start right away. I tried for three weeks to a month to contact sales because I had many questions. It got so crazy that for me to actually get in contact with LastPass I even called LogMeIn to see if they could find a way to transfer me to LastPass.

LastPass is a great solution, but, because of the communication, I didn't actually start it as a solution for our enterprise business. That's why it has been only for four to five users..”

**Luis Enrique**

Network Engineer at a tech services company with 1-10 employees

[Read full review](#) 

# Other Advice

“On a scale of one to ten, I would rate LastPass either an eight or a nine because it's beneficial for us and it checked all the security audit boxes. We are talking about substantial organizations here. If you're tiny, then you can get away with a more straightforward setup..”

## Verified user

Assistant Director of Technology Support at a university with 1,001-5,000 employees

---

[Read full review](#) 

“I would recommend this product to a colleague or a coworker, either within the company or at a different company. This is based on how easy it is to use, and that the subscription is a fair price.

I would rate this solution a seven out of ten..”

## Verified user

Engineering at a comms service provider with 10,001+ employees

---

[Read full review](#) 

“I am satisfied with all aspects of LastPass expect that the changes are not immediately synced to the users.

If you are over one thousand employees, I am not sure if you should use LastPass.

If you have less then I would recommend this solution.

I would rate this solution an eight out of ten..”

---

**Verified user**

Operations Engineer at a tech services company with 1,001-5,000 employees

[Read full review](#) 

“I have known LastPass for so long that it feels natural. That said, I have some advice with respect to using it.

First, it has to be secured with a security key. Next, ensure that you master the password sharing features. Finally, I suggest disabling the form fields because it tends to over-interpret what it should be doing. I prefer to have more control than that.

The secure notes feature is very important, so be sure to familiarize yourself with it.

I would rate this product eight and a half out of ten..”

---

**Verified user**

CEO at a legal firm with 1-10 employees

[Read full review](#) 

“LastPass gives us the ability to provide granular role permissions, although it isn't particularly important to do so in our environment. We definitely don't want everybody to have wide-open access to everything, so we do have a tiered structure in place, as far as access is concerned.

At this point, we have not integrated LastPass with other applications. We use it for websites but not for applications per se. There are some that we would like to experiment with but we haven't done it yet.

My advice to anybody who is looking to implement LastPass is that there are a lot of password vault environments on the market, so you should do your research and read the reviews. That said, this is a premium product that is easy to implement and easy to use. It doesn't seem to be hard on resources and I believe that the value is there, in terms of cost versus performance.

I would rate this solution a nine out of ten..”

**Mike Klaus**

Senior Systems Analyst/Administrator at a agriculture with 1-10 employees

[Read full review](#) 

---

“If you're looking for a password management solution that can hold your passwords and share passwords among employees, one that is cloud-based – and even without the internet you can still access passwords – and if you need a solution that that has the best price for the best product, LastPass is the one. But if you're a person who works in IT who wants to put passwords in privileged accounts and manage them with automation and everything that an enterprise password manager is required to do, LastPass is not the solution for you. You have to search for something else.

In our organization, the roles of the LastPass users are just below executive level. Their decisions, and what they do, can influence the company. They manage



LastPass themselves. In the Sharing Center is the Shared folder. If somebody is going to change a password, they need permission to do so. In our case, they all have permission to change a password. If a password is changed, it's changed. That's it. I don't really see the need for a person to maintain LastPass.

The two main reasons my company cannot move to LastPass are because of the synchronization issue and the poor communication.

I rate LastPass at eight out of ten. It offers everything you need for a password management solution. The con that makes it less than a ten is the communication with support and sales. Normally, you just contact sales at a company and you can reach them easily, to start gathering information, to talk with them about your plan and, sometimes, to get a demo, based on your plan. I didn't have that with LastPass..”

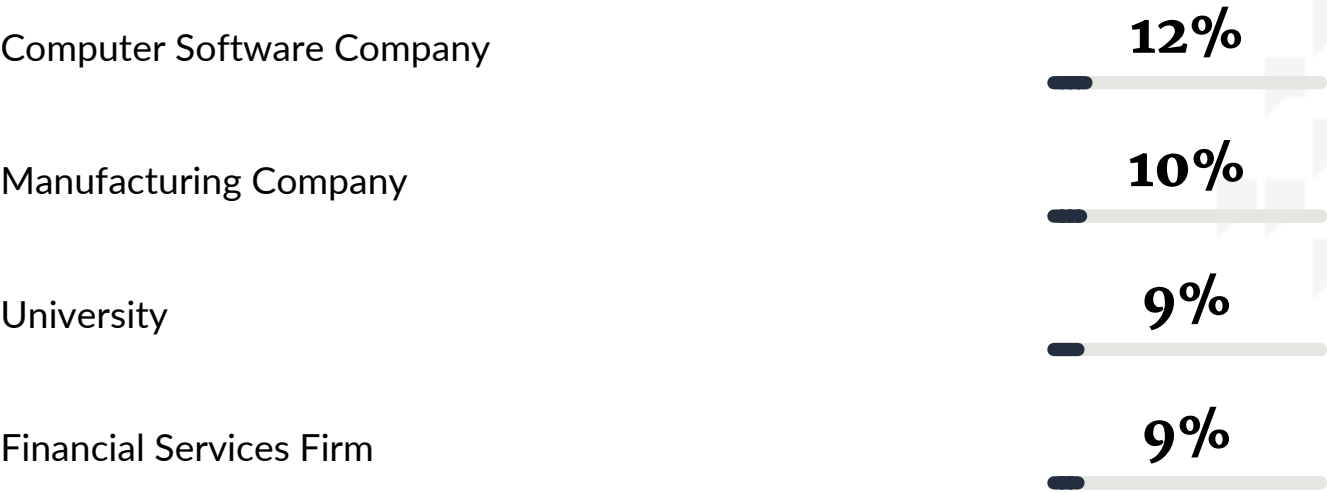
**Luis Enrique**

Network Engineer at a tech services company with 1-10 employees

[Read full review](#) 

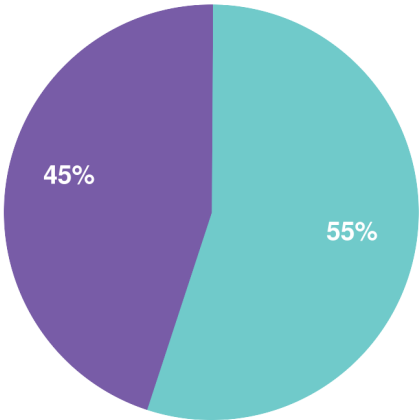
# Top Industries

by visitors reading reviews

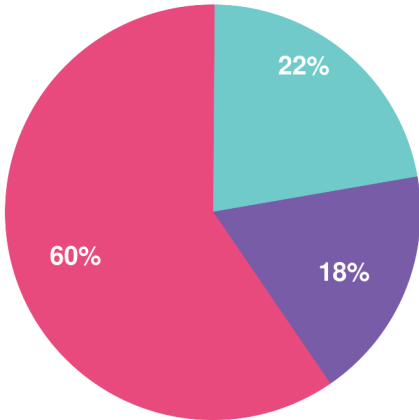


# Company Size

by reviewers



by visitors reading reviews



 Large Enterprise

 Midsized Enterprise

 Small Business

# About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

## Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a [customized report](#) of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.

[Get your personalized report here](#)

# About PeerSpot

PeerSpot is the leading review site for software running on AWS and other platforms. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: [www.peerspot.com](http://www.peerspot.com)

## PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

[reports@peerspot.com](mailto:reports@peerspot.com)

+1 646.328.1944