LastPass •••|
by LogMeIn

FINDING AN IDENTITY SOLUTION FOR YOUR BUSINESS

A Guide to Evaluating
and Comparing Options

Your trial will expire on October 14, 2016
BUY LICENSES
CONTACT US
5
reusing Master Passwords
VIEW USERS
3
invited but not yet activated
REINVITE ALL
0
with a weak security challenge score
90%
Average password strength
291 site logins this week
VIEW REPORT
52

IDENTITY IS FOUNDATIONAL TO A SECURE, PRODUCTIVE BUSINESS.

Your organization faces more complexity than ever. There are more devices, applications, networks, even users in your business ecosystem. Being able to connect users to the right technology, at the right time, in a way that is secure, is fundamental to helping everyone work effectively and efficiently. No matter where they are or when they need access, you need to connect users to the right resources – apps, services, data, and more – without exposing the business to risk.

Using unique data points to build an "identity" for every user in your environment allows you to accurately identify who your users are and facilitate secure access to what they need, every time. From the user's behavior and devices to the services they use and their personal attributes, the most successful approach to managing identities accounts for a wide variety of use cases and authentication scenarios.

> *The key, of course, is to find the right balance between security and ease of use, so that employees can work productively while minimizing cyberthreats.*

IDENTITY BRINGS ACCESS AND AUTHENTICATION TOGETHER.

In this guide, we specifically focus on evaluating and comparing identity solutions that combine Access technologies like Single Sign-On (SSO) and Enterprise Password Management (EPM) with Authentication technologies like Multifactor Authentication (MFA). When these technologies are combined into one solution, you can address many pressing identity challenges across the business.

In this guide, we'll explore:

- **Challenges an identity solution will help you resolve**
- **Benefits to expect from an identity solution**
- **A comprehensive set of criteria for evaluating solutions**
- **Why SSO, EPM, and MFA are better together**

STRUGGLING WITH THE FOLLOWING? AN IDENTITY SOLUTION CAN HELP.

Lack of insight into Shadow IT. 77% of employees use a 3rd-party cloud app without the approval or knowledge of IT. How can you put parameters around Shadow IT so that employees aren't putting the business at risk?

More security at the expense of usability. More isn't always better. Frequent password rotations, clunky two-factor authentication experiences, multiple work portals – end users know security is important, but they just want fast and convenient.

Risky password hygiene. 80% of data breaches are attributed to weak, reused, and stolen passwords. That's why you should be eliminating passwords where possible, strengthening the ones that remain, and requiring additional steps to authenticate users.

Lack of integration across solutions. How can you gain a comprehensive view of users across the business if your security solutions don't talk to each other? Better integration creates better visibility – and control.

An IT team lacking time – and expertise. Whether you're a team of 50 or a one-man department, IT admins juggle competing priorities daily. Eliminating time wasted on password resets, account lockouts, onboarding, and offboarding means IT can focus on more value-add projects. Plus, with a shortage of admins skilled in cybersecurity, in-house expertise is hard to come by.

Not sure where to start with MFA. Standard two-factor authentication may be what most businesses choose, but adaptive authentication offers many added benefits. No two users are the same, and different authentication scenarios demand different requirements.

BENEFITS YOU CAN EXPECT FROM THE RIGHT IDENTITY SOLUTION.

Visibility: Track user activities, generate reports on those activities, and gain a detailed understanding of what users are accessing and how they're behaving.

Control: Enforce policies that align with the business' security goals and government regulations, and ensure access is appropriate to each user's role.

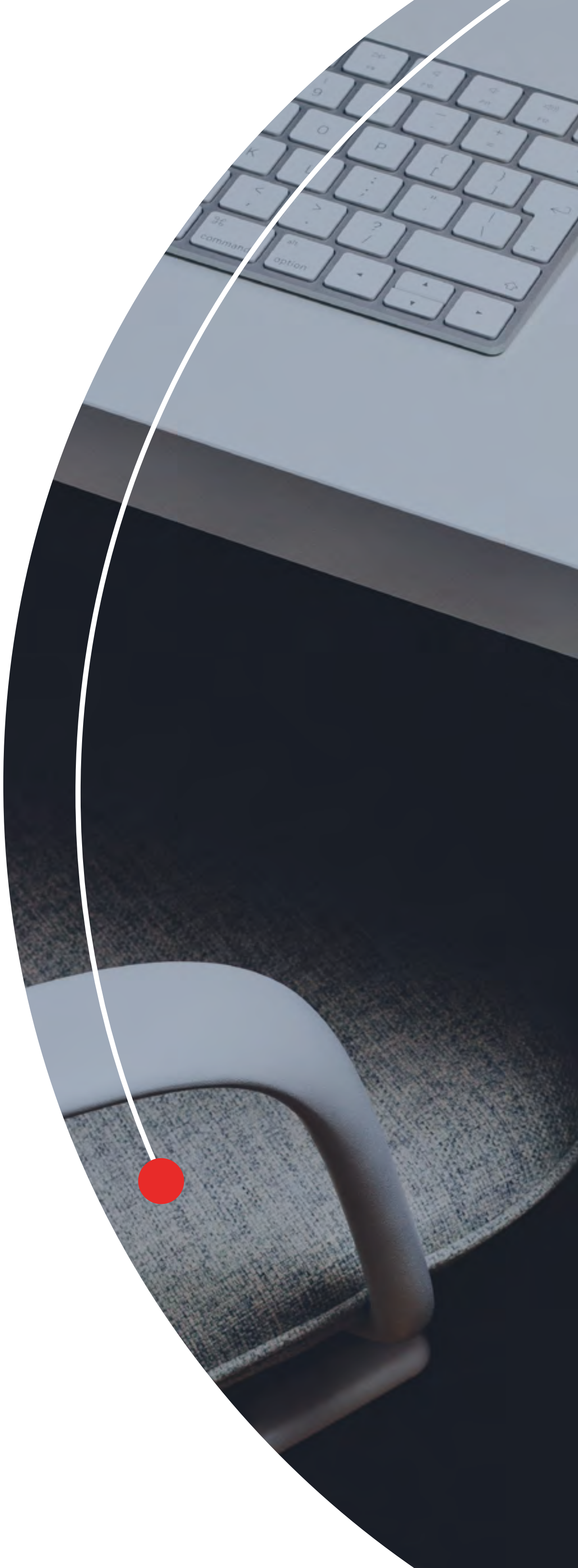
Automation: Integrate with existing technologies and infrastructure to speed up deployment, simplify day-to-day management, and standardize user offboarding.

Unification: Bring access and authentication together in one solution that offers a complete view of every access point and user action.

Security: Impose role-based permissions so every user has the least-privileged access needed to do their job. Eliminate passwords, strengthen those that remain, and add protection with more authentication factors.

Productivity: Remove password-related obstacles and give users a simplified, frictionless way to access the tools they need to do their work.

Savings: Reduce time spent on password resets, account lockouts, and day-to-day user management. Minimize or eliminate the overhead of outdated, resource-intensive on-premise solutions, and the in-house expertise required to manage them. Savings in time, money, resources, and talent add up.



WHY SSO, EPM, AND MFA ARE BETTER TOGETHER.

Single Sign-On, Enterprise Password Management, and Multifactor Authentication solutions each provide important security and productivity benefits to an organization. Managing multiple solutions, however, can be challenging. The solutions may not integrate with each other, more tools create more complexity, and employees face more hurdles just to do their work.

When combined in one solution, though, your organization will achieve unified visibility and control across every access point. And given that SMBs tend to have more limited budgets and resources than large enterprises, we agree that a holistic, all-in-one solution will maximize your IAM investment.

In summary, an all-in-one identity solution should give IT the oversight they need to increase security across the organization, while also removing access-related obstacles for users. A solution that is easy to learn and use, and that simplifies day-to-day management for busy IT admins, is the most likely to lead to a successful implementation. With unified visibility into user access and authentication across the business, you can reap the rewards of balancing user experience and increased security.

CRITERIA FOR EVALUATING IDENTITY SOLUTIONS.

So you've decided your business could benefit from an identity solution. Now what? Finding the right solution means understanding your needs as well as what you expect an identity solution to do for you, and then finding the product that best delivers on those needs and expectations.

Key areas when comparing solutions include:

- **Central, unified admin control**
- **Breadth and variety of integrations**
- **Frictionless employee experience**
- **Custom, granular controls**
- **Universal access management**
- **Flexible multifactor authentication**
- **Security by design**
- **Self-service implementation**
- **Reasonable cost of ownership**

Let's dive in.

CENTRAL, UNIFIED ADMIN CONTROL

When it comes to identity, one of the biggest challenges for IT admins is gaining visibility into – and control over – user access and authentication across the business. What apps are employees using? When and where are they accessing resources? Are the right access controls in place? Are authentication requirements strong enough to stop attacks? Are employees practicing good password hygiene? The right identity solution will give admins insight into all these elements, and more.

Look for:

- **One admin dashboard to manage SSO, EPM, and MFA capabilities**
- **At-a-glance insights into users, including their activity, permissions, and assigned apps**
- **Organization-wide measurements on security, password hygiene, and threats**
- **Detailed reporting logs for auditing and compliance**
- **Automatic revocation of access when employees leave**

PRO TIP

The admin dashboard is your command central when deploying and managing an identity solution. Understand available metrics on the dashboard so you know how to track progress over time.

BREADTH AND VARIETY OF INTEGRATIONS

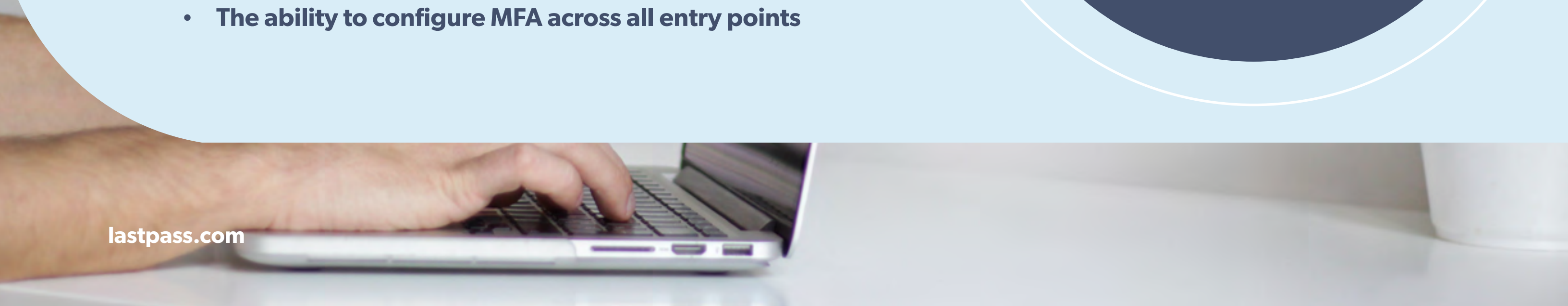
For busy IT admins, automation is key to reducing time spent on manual, repetitive tasks and simplifying day-to-day management of an identity solution. The more you can leverage existing infrastructure, the smoother and faster your deployment will be. The ideal identity solution should offer extensive integrations so that employees are up and running quickly. When your identity solution integrates with your existing technology ecosystem, admins enjoy greater flexibility and control while reducing costly and time-intensive overhead.

Look for:

- **Deep integration with popular directories for onboarding, offboarding, and management**
- **Importing groups from directories for assigning privileges and policies**
- **A large SSO catalog with a broad range of pre-integrated apps**
- **The option for federation with services like Microsoft ADFS or Azure AD**
- **Support for all use cases – including cloud, mobile, and legacy on-premise apps**
- **The ability to configure MFA across all entry points**

PRO TIP

Using a test environment during your trial will allow you to fully explore available integrations and configuration options, without worrying about impacting your production environment.



FRICTIONLESS EMPLOYEE EXPERIENCE

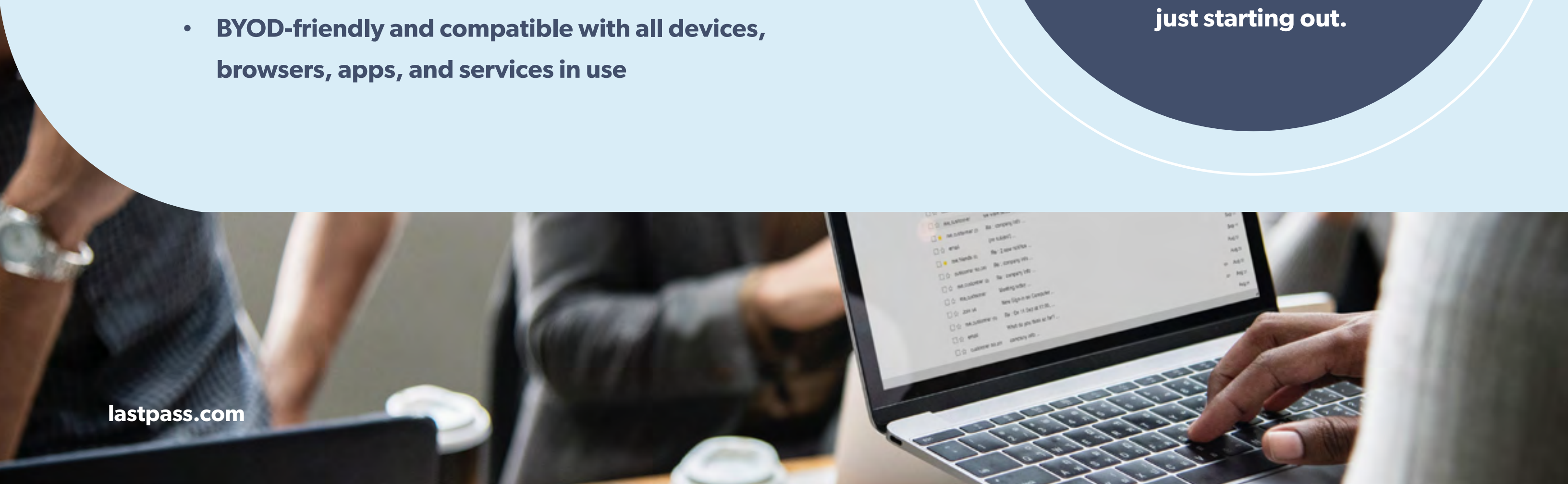
An identity solution must meet the needs of admins – and users. If employees don't readily adopt and use available features, you're less likely to see security and productivity gains. Any identity solution you invest in should remove obstacles for the employee – like eliminating lockouts and resets – and save them time as they go about their daily routine.

Look for:

- **Little setup work required of the user**
- **One password to unlock access to all work tools**
- **One portal to view and launch any app via SSO or EPM**
- **Auto-capture and auto-store of passwords**
- **Flexible MFA that adds steps only when suspicious activity is detected**
- **Secure password sharing that syncs updates behind-the-scenes**
- **BYOD-friendly and compatible with all devices, browsers, apps, and services in use**

PRO TIP

A proof of concept with a group of users from all areas of the organization – not just IT – will give you insight into how the product works and how intuitive it is when just starting out.



CUSTOM, GRANULAR CONTROLS

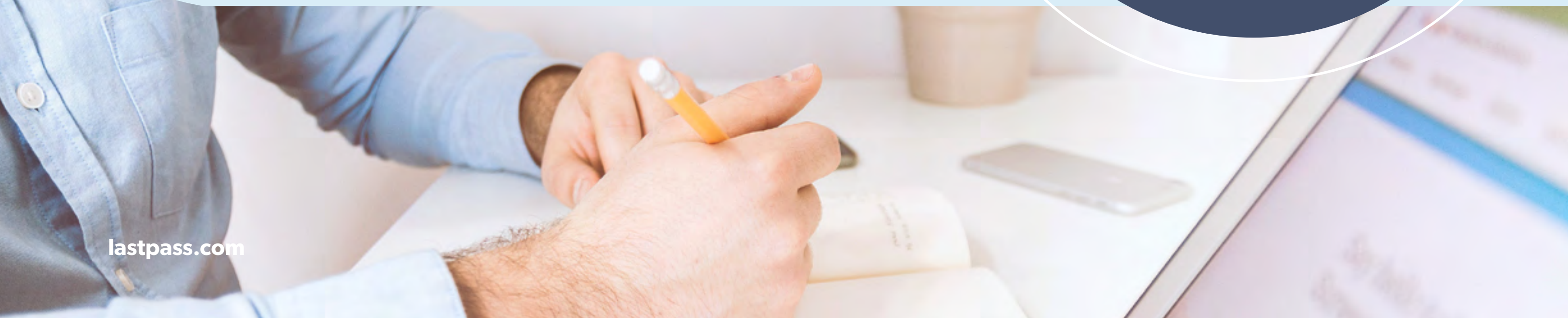
One of the primary aims of an identity solution is to improve your organization's security. From reducing passwords in use to improving the strength of remaining passwords to adding intelligent layers of protection, an identity solution should boost cybersecurity hygiene across all employees and eliminate common threat vectors. When admins can enforce flexible policies across the organization – or even by individual or group – businesses can strike the right balance between security and usability.

Look for:

- **Extensive policies to control access, authentication, feature usage, and more**
- **One centralized dashboard to manage all policies across Identity**
- **Assigning policies at the user, group, or organizational level**
- **Consistency of policies across MFA, SSO, and EPM**
- **Role-based permissions that give just the right level of access**

PRO TIP

Understand the context in which you'll be using policies. What do you want to control in your environment? What rules and restrictions do you need to put in place to meet your organization's security requirements?



UNIVERSAL ACCESS MANAGEMENT

With the rise of BYO-everything in the workplace, IT is challenged to support more devices and apps than ever before. As businesses migrate to the cloud, they may find themselves managing a hybrid environment of newer cloud and mobile apps alongside legacy on-premise tools. An identity solution should seamlessly support all these use cases and allow businesses the flexibility to evolve and add more over time.

Look for:

- **Support for legacy on-premise tools, cloud apps, and mobile apps**
- **Auto-capture and auto-fill of form-based web logins**
- **Discoverability of apps and services in use**
- **Security reports for all apps and passwords in use**

PRO TIP

By combining SSO and EPM features, you can reduce Shadow IT in the organization by "seeing" everything in use, whether an IT-managed app or a website an employee saves to their portal.

FLEXIBLE MULTIFACTOR AUTHENTICATION

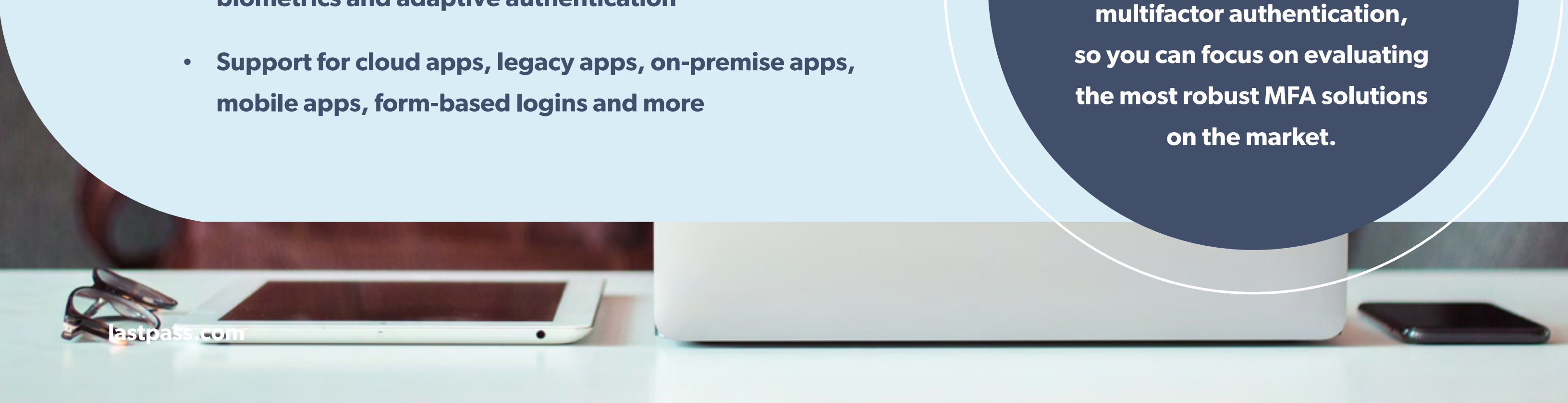
Many businesses implemented two-factor authentication (or started to) years ago but haven't kept up with the latest advances in authentication. A lot has changed – from the way MFA leverages devices like smartphones to the user experience to the admin controls. Today's best MFA solutions go beyond standard two-factor authentication to ensure the right users are accessing the right data at the right time, with requirements that adapt to the risk of any given login event.

Look for:

- **Option to use personal smartphones for end user convenience**
- **Use of "hidden factors" like geolocation, device ID, and IP address**
- **"Human factors" like fingerprint scans and Face ID**
- **Adaptive authentication that leverages biometric and contextual factors**
- **Security by design that encrypts biometric data at the device level**
- **Combination of methods in use, such as push notification, biometrics and adaptive authentication**
- **Support for cloud apps, legacy apps, on-premise apps, mobile apps, form-based logins and more**

PRO TIP

Understand the difference between two-factor authentication and true multifactor authentication, so you can focus on evaluating the most robust MFA solutions on the market.



SECURITY BY DESIGN

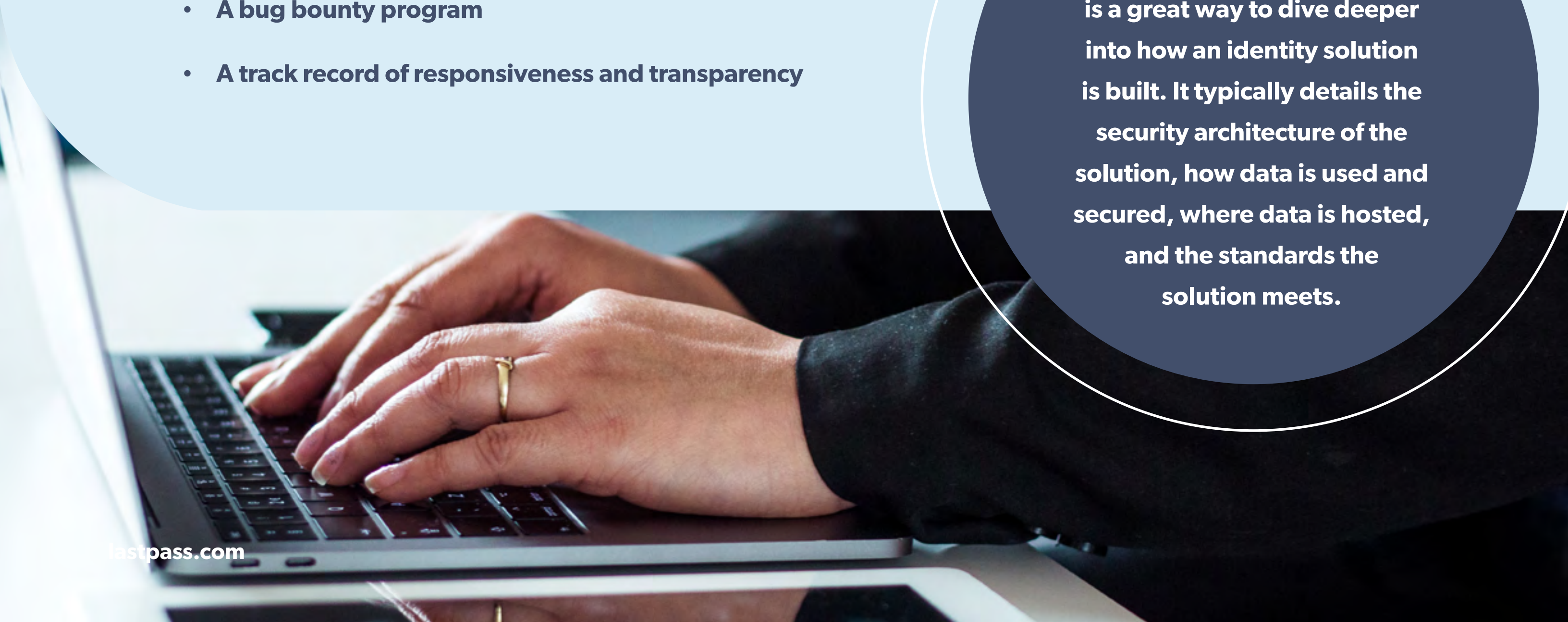
An identity solution should be safe and reliable, while providing you the features and capabilities to achieve your security goals and enforce stronger policies organization-wide. Ensure the solution aligns with and reinforces the policies you have in place and compliance requirements you need to meet.

Look for:

- **Best practices for securing data in transit and at rest**
- **Local-only encryption of any stored passwords**
- **Extensive admin policies and controls across SSO, MFA, and EPM**
- **Regular audits and industry certifications like SOC-2**
- **A bug bounty program**
- **A track record of responsiveness and transparency**

PRO TIP

A technical whitepaper is a great way to dive deeper into how an identity solution is built. It typically details the security architecture of the solution, how data is used and secured, where data is hosted, and the standards the solution meets.



SELF-SERVICE SOLUTION

Identity solutions can vary greatly when it comes to the expertise they require for implementation and the add-on professional services that may be encouraged. For SMBs who may not have the resources or budget of large enterprises, it's important to look for a solution that doesn't require specialized knowledge or extensive training. A self-service solution will save time, money, and arguably leads to greater ROI.

Look for:

- **Out-of-the-box setup for admins**
- **Directory integrations that automate onboarding and offboarding**
- **An app catalog for simple configuration of company tools**
- **A step-by-step implementation guide**
- **Pre-packaged training resources like handouts, videos, and presentations**

PRO TIP

Advanced planning can ensure you take full advantage of your trial and maximize the success of your rollout. Use available guides for your proof-of-concept and implementation to ensure you're following best practices and using the solution to its full potential.

REASONABLE COST OF OWNERSHIP

There's no denying that cost is an important factor, especially if you're an SMB with a tighter budget. While you want to keep costs reasonable, remember that you need to find a solution that successfully addresses your organization's challenges when it comes to access and authentication. An all-in-one solution that combines many products in one bundle will reduce the need to invest in multiple IAM solutions and lowers administrative overhead.

Look for:

- **One solution that combines core functionality like SSO, EPM, and MFA**
- **Budget-friendly solutions that don't sacrifice functionality or security**
- **Flexible purchasing options**
- **Self-service resources that admins can leverage for internal training**
- **Optional professional services for installation and deployment**

PRO TIP

During your trial, familiarize yourself with available documentation and other self-service training materials. What resources – from webinars to tutorials to documentation – are available for admins and users? If your business requires extensive support or training needs, understand options and added costs.

MAXIMIZING YOUR FREE TRIAL

A trial is a valuable opportunity to learn more about the service. You can try key features, see how the service can be customized to your organization's unique needs, and even gather feedback from employees. By the end of your trial, you should have a clear idea of the security and efficiency benefits that the identity solution will bring to your organization.

To make the most of your trial:

1. **Organize your trial task force.**

   Before you get started, be sure to clarify who will be testing the service, and what will be expected of them during the testing period. We recommend recruiting employees outside of IT, to get well-rounded feedback of the end user experience.

2. **Explore apps and integrations.**

   Use the app catalog to look for your organization's most-used services, whether cloud, mobile, on-premise or legacy. Look into options for adding custom SAML-based apps. Also, look at available integrations with directories and other technologies that can help speed up deployment and simplify day-to-day management. A test environment is an ideal way to test directory sync during your trial.

3. **Set up Single Sign-On and Multifactor Authentication.**

   Select 5 apps to test. Follow the configuration steps to enable SSO for them. Turn on MFA for the apps as well, and practice launching the apps from the dashboard. Test across different devices and common use cases for your business.

4. **Configure policies.**

   Familiarize yourself with available policies that apply to Single Sign-On, Multifactor Authentication, and credential management. Configure policies that control how, where, and when apps function, or MFA is required. Apply them to the entire organization or specific groups, users or apps. Once you enable a few policies, put them to the test to see what users will experience, and what reporting you'll see from the admin dashboard.

5. **Assign users to test apps.**

   The best identity solution is one that employees will readily adopt and find easy-to-use. Select apps that are used by other departments and recruit employees outside IT to help test the login experience during your trial. They can be a valuable source of feedback as you evaluate your trial. Early testers can also become helpful internal advocates once you select and deploy an identity solution.

6. **Try password management features.**

   When it comes to form-based logins, be sure to test storing, filling, generating, updating, and managing credentials. Explore password sharing capabilities, including sharing single items or folders of items with others. Test on any devices that will be used throughout the organization, including desktop, iOS, and Android.

LEARN MORE ABOUT LASTPASS IDENTITY

LastPass Identity provides simple control and unified visibility across every entry point to your business, with an intuitive access and multifactor authentication experience that works on everything from cloud and mobile apps to legacy on-premise tools. From single sign-on and password management to adaptive authentication, LastPass Identity gives superior control to IT and frictionless access to users.

We'd love to hear more about your business needs, so please reach out to us when you are ready to take a closer look: www.lastpass.com/lastpass-identity-contact-sales

Central admin control

1,200+ single sign-on applications

Industry-leading enterprise password manager

100+ access security policies

Advanced reporting

Secure password sharing

User directory integrations

Adaptive multifactor authentication

One solution

LastPass •••|

by LogMeIn

www.lastpass.com/products/identity