LastPass ••• | by LogMeIn

FINDING AN ACCESS SOLUTION FOR YOUR BUSINESS

A Guide to Evaluating and Comparing Options

SECURITY STARTS WITH THE BASICS.

Today's business is digital. Without connectivity, work doesn't get done. But an always-on, always-connected world equals more pressure to keep your business secure. There are more devices, applications, networks, even users in your business ecosystem, which means managing and protecting user access is more complex than ever. Staying on top of all possible threats can be overwhelming. What you need is a comprehensive solution that grants users the right access to the right technology at the right time, while reducing friction throughout the workday.

80% OF BREACHES
ARE DUE TO POOR PASSWORDS.[1]

50% OF THE WORKFORCE

is millennials aged 18-24 years old[3] – and turnover is common as more than half have already had 3 or more jobs.[4]

76% OF EMPLOYEES

experience regular password problems.[2]

59% OF EMPLOYEES

reuse the same password.[5]

43% OF ALL CYBERATTACKS

target small businesses.[6]

93% OF CYBER INCIDENTS

can be prevented with the right tools.[7]

69% OF EMPLOYEES

say they would use a password solution if it were offered to them.[8]

IAM, IDAAS, SSO, EPM: ACRONYMS EXPLAINED, AND WHY IDENTITY MATTERS.

At its core, identity and access management (IAM) refers to a combination of technology and policies that ensures people in a business have the right level of access to organizational resources for their role.

An IAM ecosystem helps IT securely manage employee identities so that when someone tries to access a resource, the solution confirms that the user is authorized to access said resource before successfully authenticating. Equally important is the ability to deprovision – or remove access – when an employee leaves the organization or changes roles.

For businesses embracing the cloud, identity-as-a-service (IDaaS) is a type of IAM offering that uses single sign-on (SSO), enterprise password management (EPM), authentication factors and access controls to securely connect employees to the tools

needed to do their work. Single sign-on only requires employees to remember one set of credentials, while replacing the rest with a behind-the-scenes protocol called SAML 2.0. A password manager helps a user store, manage and protect any passwords that can't be replaced with SSO. Users only remember one master password that grants access to the portal that connects them to all their apps and services.

BUT IT'S NOT JUST ABOUT SECURITY.

Passwords are a source of frustration, decreased efficiency and loss of productivity. Access solutions provide a simplified, frictionless experience without sacrificing security or control.

IN THIS GUIDE, WE'LL FOCUS ON ACCESS SOLUTIONS AND EXPLORE:

- Core components of an effective access solution
- Key problems an access solution should address
- A comprehensive set of criteria for evaluating solutions
- Best practices for implementing an access solution

We'd love to hear more about your business needs, so please reach out to us when you're ready to take a closer look:

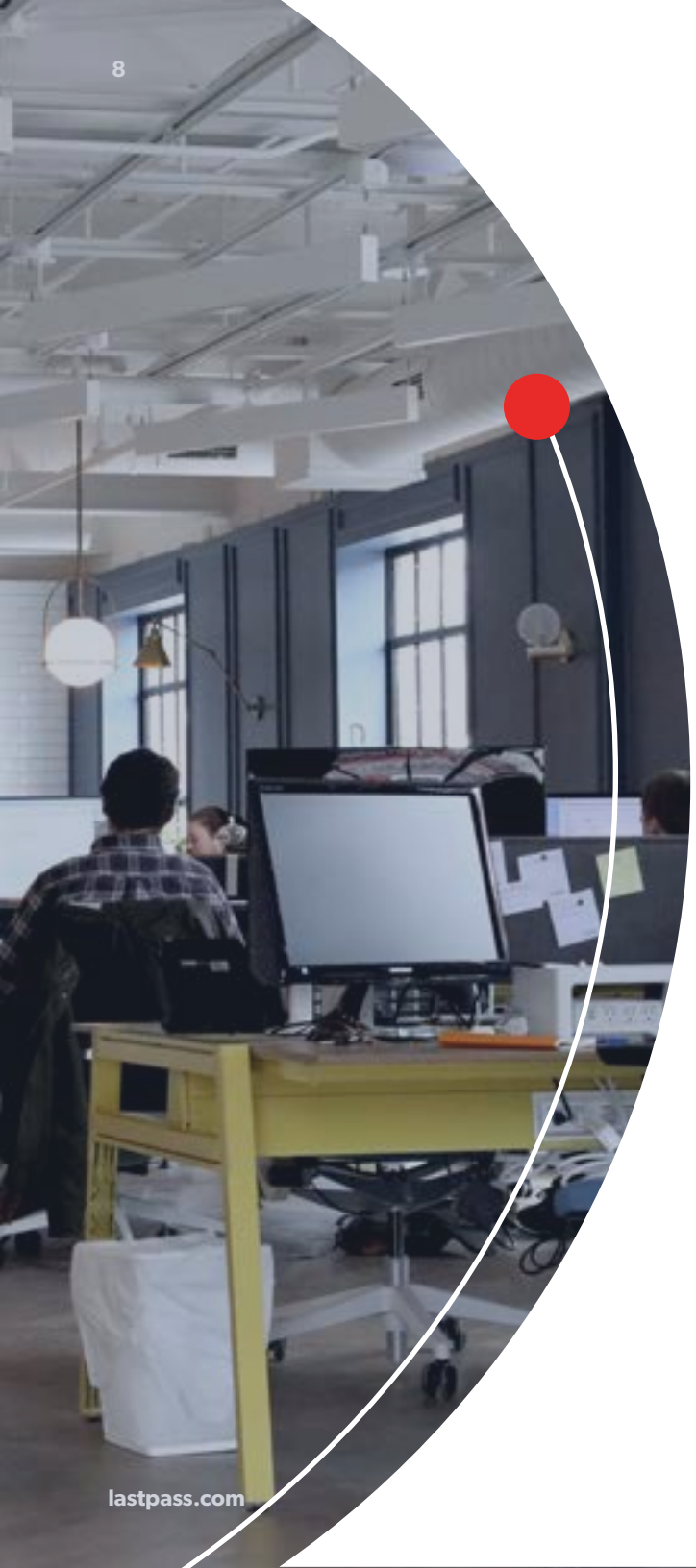
www.lastpass.com/lastpass-enterprise-contact-sales

WHY CONSIDER AN ACCESS SOLUTION?

The last decade has seen a massive change in the workplace. With the rise of the cloud and the rapid adoption of personal computers and smartphones, it's not just easy to work from anywhere – employees expect it. They try new apps, often without IT approval. They job hop frequently. They want their technology to be fast, convenient and easy to use.

Not only are employees introducing more risk, cyberattacks are more prevalent and sophisticated. And it's not just major consumer brands that are targeted – some two-thirds of cyberattacks are directed at small and midsized companies.[9] To maintain customer privacy and combat cybercrime, governments are introducing more cyber security regulations, dictating how user data must be accessed, stored and protected.

It's no wonder that IT is more challenged than ever to manage employees inside and outside the four walls of the office, ensuring users have appropriate access and company data is secure without becoming a blocker to workforce productivity.



WE'RE STILL STUCK WITH PASSWORDS, TOO.

Despite all the talk about the "death of the password," we don't yet live in a post-password world. Over 50% of the most popular cloud services do not have out-of-the-box support for SSO,[10] which leaves employees with too many passwords to remember and manage. As a result, the security of your business suffers from:

- Inaccurate password tracking
- Disconnected password solutions
- Weak, reused passwords
- Lack of oversight for shared passwords
- Lockouts and productivity loss

Even when a business is using SSO, protecting the data of employees, customers and partners requires that all password-protected entry points to the business are handled appropriately.

WHEN IT COMES TO SECURING USER ACCESS, ACHIEVING BEST PRACTICES MEANS:

- Combining SSO and password management in one easy-to-use solution
- Making it fast and easy for employees to do their work
- Integrating and automating with existing technology, like user directories
- Supporting all use cases, from cloud to mobile to legacy apps and beyond
- Applying role-based permissions to employee identities
- Decommissioning employee access after they leave or change roles
- Adding protection with multifactor authentication wherever possible

An access solution that combines SSO and password management is the most comprehensive way to protect every access point across the entire organization.

AN EFFECTIVE ACCESS SOLUTION SHOULD:

Centralize reporting and IT insights.
Leverage detailed access and security reports to get granular, customizable visibility across the business.

Enforce policies organization-wide.
Standardize policies across SSO and password management at the user, group or organizational level.

Simplify employee access.
Whether access is secured with a password or SSO, make everything accessible from one secure portal.

Rescind employee access when they leave.
Equip IT to audit user access, change permissions and rotate passwords instantly.

Share access to accounts, without sharing passwords.
Maintain accountability and oversight of shared accounts, internally and externally.

Integrate with existing infrastructure.
Accelerate and automate workflows with an extensive app catalog and support for existing directories.

Reduce access risks.
Gain visibility into poor password hygiene and measure improvements.

CRITERIA FOR EVALUATING SOLUTIONS:

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

KEY AREAS WHEN COMPARING SOLUTIONS:

A centralized admin experience:
What does it take to deploy the solution, and how does it automate the management of ongoing tasks?

Comprehensive security controls:
Are admins given the right amount of oversight and visibility?

A breadth and variety of integrations:
How many pre-integrated apps are available?
How does the solution integrate with existing technology?

An effortless, secure experience:
How easy is it to use, and does it address the access challenges employees are facing?

A self-service solution with appropriate cost of ownership:
What budget does the solution require upfront, and what are the costs (monetary or otherwise) in the longer term? Is rollout self-service?

A focus on security:
Is the solution safe and reliable, and does it help you achieve your security goals?

A CENTRALIZED ADMIN EXPERIENCE.

To scale an access solution, admins need a centralized way to deploy, manage and maintain the service as well as report on security across the business.

LOOK FOR:

- One admin portal for both SSO and password management
- Flexible admin privileges for managing and securing the deployment
- A self-service solution that requires little day-to-day management
- Provisioning tools that facilitate the lifecycle of an employee's digital identity
- Extensive policies and actionable security alerts

QUESTIONS TO ASK:

- What admin roles and privileges are offered?
- What skills or knowledge are required for deployment?
- What ongoing maintenance is required?
- How do I configure policies, at the user, group and organization level?

ACTION ITEMS:

Explore the admin dashboard. Look for key features like an SSO app catalog, user and group management, shared credential management, customizable policies and actionable security reports.

Configure access and security policies. Review available policies and understand how they align with your business' security posture.

COMPREHENSIVE SECURITY CONTROLS.

With increased regulations and the threat of cyberattacks, it's not enough to deploy a few cloud apps for employees to access. The true power lies in capturing data about the organization's security and facilitating appropriate action.

LOOK FOR:

- At-a-glance insights into users, their connected apps and user activity
- Credential sharing that tracks actions to individuals
- Organization-wide measurements on access security
- Detailed reporting logs for auditing and compliance
- Access deprovisioning or secure account recovery when employees leave

QUESTIONS TO ASK:

- Is there an audit trail, and what details do the reports capture?
- How is security hygiene measured, at the global and individual level?
- How do you terminate or reclaim a user's account when they leave?
- What can reporting tools tell us about shadow IT within the organization?

ACTION ITEMS:

Review reporting logs. Take note of what actions and events are recorded for both users and admins, how granular the logs are and how long they are available.

Ask questions about a range of scenarios. You want to see actionable overviews of your security profile that will help you proactively protect against threats.

A BREADTH AND VARIETY OF INTEGRATIONS.

IT teams want solutions that save them time and require minimal resources. An access solution should plug in to the business' existing technology ecosystem, while offering out-of-the-box integrations that require little setup and maintenance.

LOOK FOR:

- A catalog of pre-integrated cloud apps for easy-to-deploy single sign-on
- Directory services that can sync identity information already in use
- API integrations for streamlined user management
- Built-in support for all use cases, from mobile to legacy and beyond
- Federation with leading identity providers (IdPs)

QUESTIONS TO ASK:

- Are single sign-on capabilities supported, with an app catalog?
- What apps are available in the app catalog?
- Can Microsoft Active Directory or other user directories automate user management?

ACTION ITEMS:

Test your core cloud apps. Explore the app catalog and try deploying several of your most-used apps. Evaluate the experience from the admin and user perspective.

Leverage user directories. Automate user onboarding and offboarding, apply policies and assign shared credentials.

AN EFFORTLESS, SECURE EXPERIENCE.

An access solution is only effective if employees embrace it. IT must communicate how the solution will benefit users. The solution should be simple to set up and fit naturally within an employee's everyday workflow.

LOOK FOR:

- Minimal setup work required of the user
- One portal that unlocks access to everything
- Auto-capture and auto-fill of passwords
- Built-in password generator
- Personalized security reports for the user
- Simple, up-to-date password sharing

QUESTIONS TO ASK:

- What steps are required to get started and use it?
- Does the user have one portal for SSO and password management?
- Does it reduce daily friction for the user?
- How does password sharing work?
- Are passwords auto-captured for the user?

ACTION ITEMS:

Try it yourself. A proof of concept with a group of users will give you insight into how the product works and how intuitive it is when just starting out.

Inventory devices in use. Ensure that any solution you adopt is compatible with those devices and use cases.

Look for third-party validation. Customer references, case studies, SOC 2 reports, audits and detailed white papers build trust in the security model and validation of the customer experience.

A SELF-SERVICE SOLUTION WITH APPROPRIATE COST OF OWNERSHIP.

Cost is important, but like any other software purchasing decision, it shouldn't be the sole driving factor. Find a solution that is within your budget but that provides the critical functionality required to successfully address access challenges. This is especially important when considering that many businesses must invest in multiple tools to address their IAM needs – the fewer tools needed, the lower your costs and administrative overhead.

LOOK FOR:

- Budget-friendly solutions that don't sacrifice functionality or security
- Combined core functionality like SSO and password management in one solution
- Self-service resources that admins can leverage for internal training
- Optional professional services for installation and deployment

QUESTIONS TO ASK:

- What is the per-user cost?
- Are there add-on costs for additional functionality or services (such as SSO and password management together)?
- What time and resources are required to deploy and maintain the solution?
- What resources – from webinars to tutorials to documentation – are available for admins and users?
- Can licenses be purchased and/or renewed online or is it managed by a sales representative?

ACTION ITEMS:

Confirm your budget. Understand the total allocated budget and whether your first-choice solution fits within it.

Determine what resources are available. Look through documentation and other self-service training materials. If your business requires extensive support or training needs, understand options and added costs.

Walk through implementation scenarios. Ask about how routine tasks are performed – like adding or removing users, deploying cloud apps, adjusting policies and rotating passwords.

A FOCUS ON SECURITY.

When adopting an access solution, there are two things to consider:

1. Whether the service itself is safe and reliable.
2. Whether the service helps achieve your security goals and enforce better policies.

LOOK FOR:

- Local-only encryption that keeps the master password private
- Best practices for securing data in transit and at rest
- Advanced admin policies and controls across SSO and password management
- Support for multifactor authentication
- A track record of responsiveness and transparency

QUESTIONS TO ASK:

- How is data secured locally, and server-side?
- What policies and security settings are available?
- What controls are available on a global, group and per-user basis?
- What multifactor authentication options are available?

ACTION ITEMS:

Review internal security policies. Ensure the solution aligns with and reinforces the policies you have in place and compliance requirements you need to meet.

Read the technical white paper. Take note of how data is secured, and how the encryption key is protected (ideally, it's never shared with the service provider).

Evaluate the full list of policies and controls. Look for a granular level of control, allowing custom requirements around account access, password hygiene and feature usage.

ENSURING SUCCESSFUL IMPLEMENTATION:

DEFINE THE PROJECT AND GOALS.

By using the previous evaluation criteria to select the best access solution for your business, you have laid the groundwork for a successful implementation. However, several steps are key to getting it into the hands of your employees and ensuring it becomes a valuable asset:

Set clear objectives for implementing an access solution.

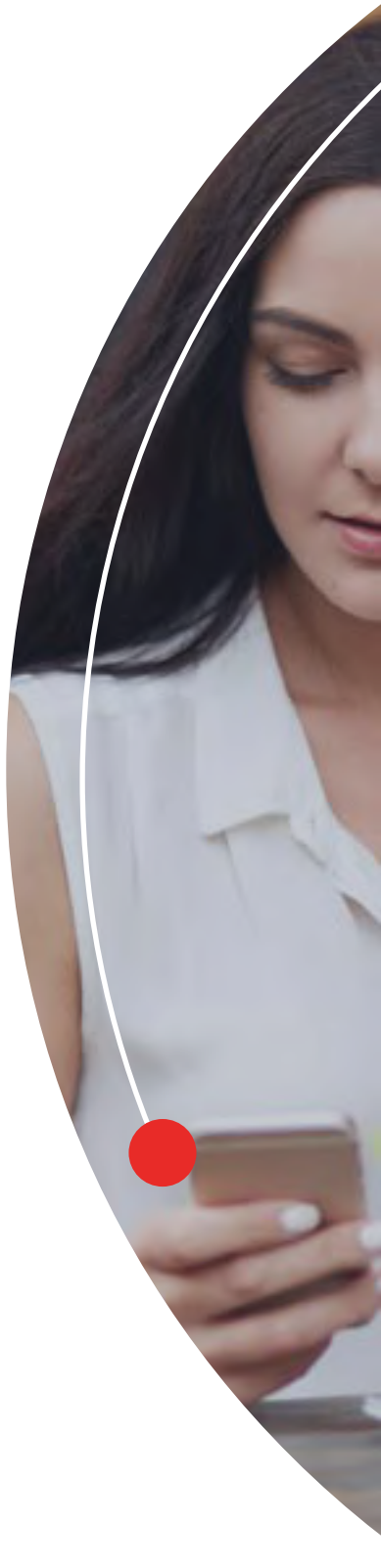
Understand where it fits in the larger security strategy.

Assign ownership of the project, including evaluation, comparison, selection and implementation.

Inventory the technology in use. Are you a BYOD work environment? What apps have you adopted company-wide? What other IAM solutions are used? How do you want them to integrate with your new solution, or will you be replacing existing tools?

Ensure alignment on security goals and how an access solution will help.

Confirm how you will show successful adoption and ROI for the implementation.



REVIEW AND TURN ON POLICIES AND SECURITY CONTROLS.

Default options provide out-of-the-box security, but your business may have unique requirements. Whether it's restricting employees' access, disabling features or requiring security settings, it's important to familiarize yourself with available options. Ensure appropriate permissions and restrictions are in place before employees use the service.

Define your security level. Is your business locked down or lax?

Review all available security policies and settings in the admin dashboard.

Decide which controls should apply globally, to groups or individually.

Enable the policies and settings that are appropriate for your security model.

Require additional means of authentication like multifactor authentication.

GET THE SOLUTION IN THE HANDS OF USERS.

The true value lies in user adoption. To achieve a successful deployment, streamline the onboarding process and plan for users who fail to sign up.

Evaluate onboarding options and choose the one that best suits your environment.

Sync with existing directories to automate onboarding.

Prepare employees by raising awareness and providing training.

Communicate policies and best practices to all employees.

Schedule follow-up reminders for those who fail to sign up or have subpar product usage.

ORGANIZE TRAINING FOR ADMINS AND EMPLOYEES.

Whether you offer brown-bag training sessions over lunch or open office hours, training for both admins and users will drive adoption.

Schedule employee training to cover core SSO and password management features.

Leverage internal onboarding toolkits such as handouts, presentations or webinars.

Facilitate Q&A sessions with staff, either during training or in separate office hours.

Make training part of the onboarding processes, so any new employees are automatically trained to use the service.

Understand adoption rates and security scores.

SECURE EVERY ACCESS POINT WITH LASTPASS ENTERPRISE.

For more than 58,000 businesses of all sizes, LastPass Enterprise reduces friction for employees while increasing control and visibility for IT with an access solution that's easy to manage and effortless to use. With single sign-on for IT's top-priority apps, and password management to capture and secure everything else, LastPass Enterprise protects every access point and conveniently connects employees to their work.

LASTPASS ENTERPRISE PROVIDES:

- Centralized, secure access with an integrated SSO and password manager solution
- A frictionless employee experience with one place to store and access every tool
- An admin dashboard with comprehensive security controls and company-wide visibility
- Plug-and-play integrations for IT teams
- Convenient, secure password sharing
- Self-guided resources to facilitate high adoption
- A strong, zero-knowledge security model

Sources:

1 Verizon, 2019. "Data Breach Investigations Report (DBIR)"
2 Ovum, 2017. "Closing the Password Security Gap"
3 Dynamic Signal, 2018. "Key Statistics About Millennials in the Workplace"
4 Forbes, 2018. "Why Your Millennials Are Leaving (And How to Keep Them)"
5 LastPass, 2018. "The Psychology of Passwords: Neglect Is Helping Hackers Win"
6 SCORE, 2018.
7 Online Trust Alliance, 2018. "Cyber Incident & Breach Trends Report"
8 Ovum, 2017. "Closing the Password Security Gap"
9 TechRepublic.
10 LastPass, 2017. "Password Exposé"

LastPass ••• | by LogMeIn

LEARN MORE AT LASTPASS.COM/BUSINESS

05.27.19/PDF/ LMI0638C