LastPass ••• | by LogMeIn

IDENTITY 101 FOR SMBs

A Guide to the Benefits and Features of Identity Solutions

Mike Terry
2082218573 | miketerry@outlook.com

TODAY'S BUSINESS ENVIRONMENT IS ANYTHING BUT SIMPLE.

Employee expectations are high. An always-connected, on-the-go workforce demands more flexibility in working wherever, whenever, from any device.

Today's employees also don't hesitate to try new apps. The average employee actively uses **36** cloud services at work.[1] They want technology to be fast, convenient, and easy to use, and they'll seek it out themselves if it isn't already available. **77%** of employees use a 3rd-party cloud app without the approval or knowledge of IT.[2]

The average employee also might not stick around for long. Job hopping is the new norm – **50%** of the workforce is millennials aged 18-24 years old, and **more than half** have already had 3 or more jobs.[3]

In short, you are faced with managing and connecting more devices, applications, networks, and users, in a business that is constantly evolving.

It's no wonder that facilitating employee access to business systems and data is more challenging than ever.

INCREASED CYBER THREATS JUST COMPLICATE THINGS MORE.

Managing today's hybrid work environment may be challenging, but securing that environment is equally important – and difficult.

Something as simple as the password continues to be an obstacle for employees, a productivity drain for IT, and a threat to the security of the business.

80% of known data breaches are due to weak, reused, or stolen credentials.[4] When **59%** of people mostly or always use the same password,[5] it's not surprising that one phished password can lead to a breach. The average employee struggles to manage **over 100** credentials, with **76%** experiencing regular password problems.

80%

of known data breaches are due to week, reused, or stolen credentials.

76%

of employees experience regular password problems.

Incorrect access controls just compound the problem. When employees have unrestricted access to data and resources, misuse and loss of data are inevitable. It also becomes easier for attackers to abuse privileged access to critical systems.

On average, IT security teams spend **4 hours** per week on password management-related issues alone and receive **96** password-related requests per month.[6] Some IT teams receive over **25** forgotten password requests in **a day**![7]

When **43%** of cyberattacks affect small businesses[8] and **53%** of midmarket companies have experienced a breach,[9] doing security basics right is no longer an option. But there's hope: **93%** of cyber incidents can be prevented with the right tools.

4 hours

spent per week on password management issues by IT security teams.

96

password-related requests are being sent to IT security teams every month.

MANAGING IDENTITY AND ACCESS REDUCES RISKS AND REMOVES OBSTACLES.

Ultimately, you need to connect your users – employees, contractors, partners – to the right technology at the right time, in a way that is secure. Being able to work effectively and efficiently requires that users have access to what they need, when they need it, wherever they are, without putting the business at risk.

To know that you're giving the right people access to something, you first need to have a way to know who they are. Building a unique "identity" for each user in your environment allows you to facilitate secure access and reliably prove it's the right user, every time.

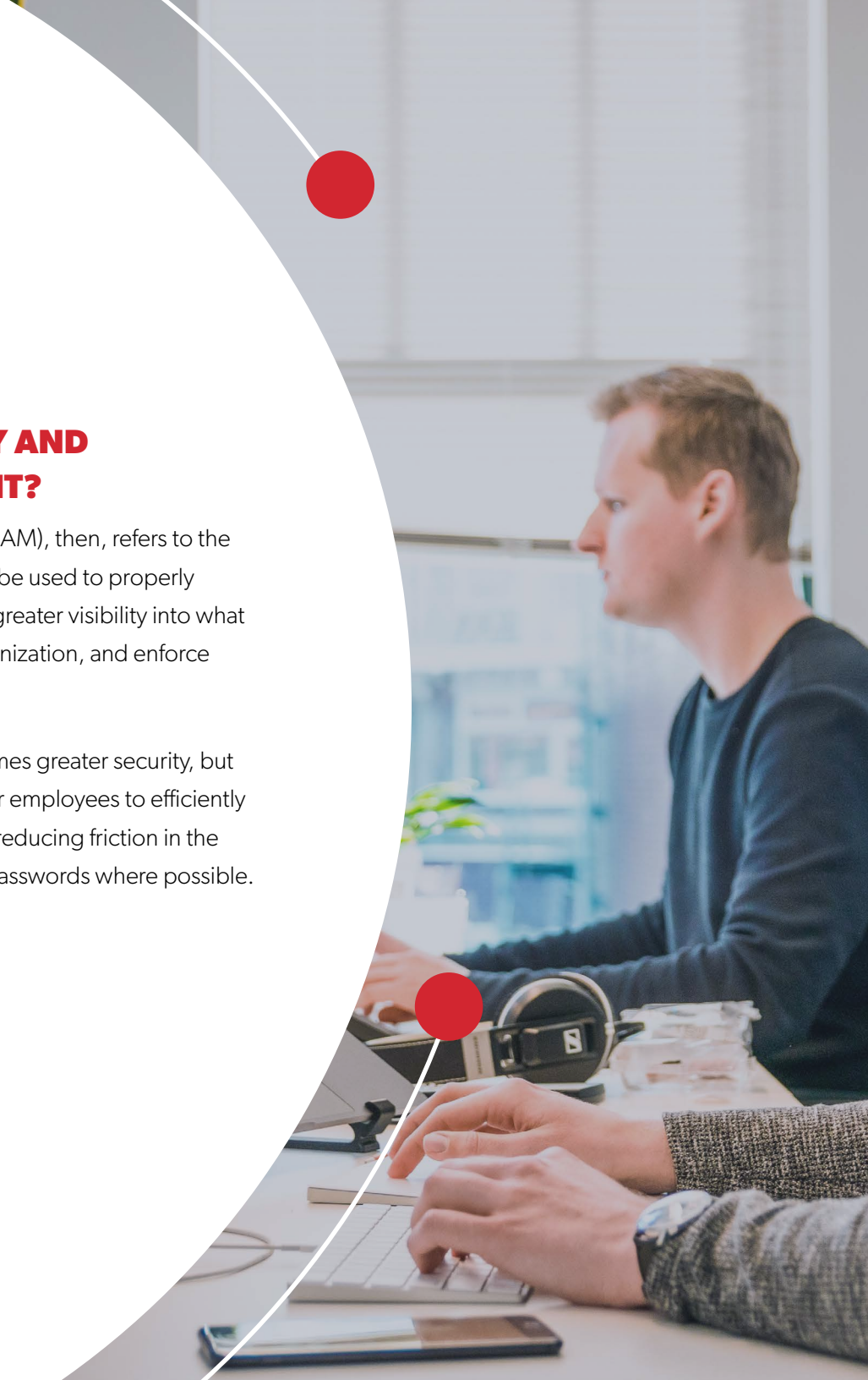
Several data points can be leveraged to build an identity, from the user's behavior and devices to the services they use and personal attributes. No two users are the same, so any approach to managing identities should account for a wide variety of use cases and authentication scenarios.

Of course, too much security can hurt employee productivity, but not enough can pose risks to the business. The key is to find the right balance between the two.

SO, WHAT IS IDENTITY AND ACCESS MANAGEMENT?

Identity and Access Management (IAM), then, refers to the technologies and policies that can be used to properly manage every user's identity, gain greater visibility into what users are accessing across the organization, and enforce stronger control over that access.

With more visibility and control comes greater security, but IAM solutions also make it easier for employees to efficiently go about their day-to-day work by reducing friction in the login experience and eliminating passwords where possible.



AN IDENTITY SOLUTION HAS FAR-REACHING BENEFITS.

IAM solutions focus on defining user roles, managing privileges, and deciding when employees are granted or denied access, but they also have significant benefits for the organization overall.

THE IDEAL IDENTITY SOLUTION WILL GIVE YOU:

Visibility: Track user activities, generate reports on those activities, and gain a detailed understanding of what users are accessing and their security behaviors.

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.

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

SSO, EPM, MFA: IDENTITY TECHNOLOGIES EXPLAINED, AND WHY THEY SHOULD BE USED TOGETHER.

There are many technologies that fall under the IAM umbrella. In this guide, we focus on a few key technologies that, especially when used together, can help your business build or modernize your identity program.

Access

Access solutions focus on connecting users to the right apps and services via passwords and other protocols. Key technologies include Single Sign-On (SSO) and Enterprise Password Management (EPM).

Authentication

Authentication solutions focus on successfully verifying and securely authorizing users as they request access to something. Key technologies include Multifactor Authentication. Options include SMS codes, hardware keys, biometrics, contextual methods, and more.

Identity

Identity solutions combine multiple Access and Authentication technologies to holistically address IAM needs across the business.

Identity technologies can be on-premise (managed on-site and in-house) or cloud-based (built and operated by a third-party provider). Using a cloud-based solution has many advantages: It costs less, requires fewer internal resources, demands less in-house expertise, and outsources security to industry experts serving thousands of organizations. For that reason, a cloud-based solution is our top recommendation for SMBs looking to create or modernize their identity program.

HOW ACCESS SOLUTIONS REDUCE PASSWORDS AND SECURE EVERY ACCESS POINT.

An Access solution helps your business achieve two goals: Eliminate login-related obstacles for employees and increase IT's visibility and control over every access point in the business. After all, anything that requires a password is an entry point to your business and needs to be managed accordingly.

There are two key Access technologies: Single Sign-On (SSO) and Enterprise Password Management (EPM).

SSO + EPM

Though they can be used separately, they are most effective when used together to offer complete coverage of all access points in the business.

SINGLE SIGN-ON CONNECTS EMPLOYEES TO CRITICAL BUSINESS TOOLS.

With Single Sign-On, employees only remember one set of credentials. All other passwords are replaced with a behind-the-scenes protocol like SAML 2.0. Once an employee authenticates to their SSO portal, they can launch and connect to any of their assigned business apps while bypassing any passwords or login pages.

KEY FEATURES OF SSO SOLUTIONS INCLUDE:

- **A single password** that unlocks access to all apps
- **One portal** where employees can view and launch apps
- **Elimination of passwords** by using SAML 2.0
- **A catalog of pre-integrated apps** for easy admin deployment
- **Support** for cloud, legacy, mobile, and on-premise apps
- **Integrations** with directories and other technologies to automate and simplify management
- **Policies** to enforce security standards and access controls

IT teams leverage SSO for the highest-priority apps in use across the organization. However, **over 50%** of the most popular cloud services do not have out-of-the-box support for SSO[10], and **77%** of employees use a 3rd-party cloud app without the approval or knowledge of IT.[11] That's why pairing SSO with a password manager is the most effective way to secure every access point.

over 50%

of the most popular cloud services do not have out-of-the-box support for SSO.

77%

of employees use a 3rd-party cloud app without the approval or knowledge of IT.

ENTERPRISE PASSWORD MANAGEMENT CAPTURES, STORES, AND FILLS EVERYTHING ELSE.

With Enterprise Password Management (EPM), employees again only have one password to remember. All other passwords are captured and stored in the password manager, which fills them in when an employee needs to log in to something. A password manager also facilitates other password-related tasks, like generating passwords, sharing credentials, and updating old passwords.

KEY FEATURES OF EPM SOLUTIONS INCLUDE:

- **A single password** that unlocks access to all credentials
- **One vault** to store, view, manage, edit, and launch logins
- **Automatic capture and filling** of any form-based login (including those unknown to IT)
- **Encrypted password sharing**
- **A password generator** that creates long, unique passwords
- **Centralized admin dashboard** with policies, reporting, and integrations to give IT visibility, automation, and control

EPM can significantly improve an organization's security posture by identifying and eliminating weak and reused passwords. IT gains greater visibility into all apps and services in use, and ensures strong passwords are protecting access to hidden services (Shadow IT).

HOW AUTHENTICATION SOLUTIONS ADD INTELLIGENT SECURITY AT EVERY ACCESS POINT.

When someone wants to access a system or resource, it's essential to prove that 1) the person is who they claim to be, and 2) they should be allowed access to said system or resource. An Authentication solution does just that, by verifying a user's identity based on unique data points, and then securely authorizing their access after checking their privileges.

Passwords may be the first line of defense for most organizations, but nearly 80% of breaches caused by hacking feature the use of stolen credentials.[12] Once a password is stolen, if nothing else is in place to detect and stop unauthorized access, a breach is inevitable. Relying on passwords alone – a form of single-factor authentication – isn't enough.

That's why businesses need Multifactor Authentication.

MULTIFACTOR AUTHENTICATION THWARTS ATTACKERS WITHOUT SLOWING DOWN EMPLOYEES.

With Multifactor Authentication (MFA), two or more pieces of information (factors) are required to prove a user's identity and connect them to the technology they use to do their job.

THOSE FACTORS MAY INCLUDE A COMBINATION OF:

1 Something you know

(a knowledge factor) like a password, PIN, or security question

2 Something you are or do

(an inherence factor) like a fingerprint, face scan, retinal scan, or voice

3 Something you have

(a possession factor) like an ID card, hardware token, or software token

Many businesses are familiar with two-factor authentication (2FA), which combines two factors – typically your password (knowledge) and a code generated by an app on a smartphone (possession).

However, the drawbacks of standard 2FA include lack of support for a wide range of use cases (across legacy, mobile, on-premise, and cloud apps), and an inability to adapt to unique scenarios (the same factors are required no matter the situation). That's why an MFA solution that leverages several available datapoints and accounts for different behaviors, personal devices, levels of access and attributes, is far more effective.

KEY FEATURES OF MFA SOLUTIONS INCLUDE:

- **Biometric authentication** with human factors like face, fingerprint ID, voice, and iris
- **Contextual authentication** with hidden factors like phone location, IP address, or device ID
- **Adaptive authentication** that leverages biometric and contextual intelligence to adapt login requirements to specific users and scenarios
- **The option** to replace passwords with MFA
- **Protection for every access point,** including legacy, cloud, mobile, and on-premise apps
- **Centralized, granular control** from an easy-to-use admin dashboard
- **Integration with directories** and other technology for simple deployment and management
- **Proper encryption** of biometric data to ensure privacy and security

MFA goes beyond the one-size-fits-all approach of 2FA to offer organizations a smarter way to add protection to every entry point. But rather than slow employees down with cumbersome prompts and codes, the best MFA solutions leverage hidden and human factors to identify and authenticate users with a frictionless login experience.

ADMINS VS USERS: SECURITY WITHOUT SACRIFICING USABILITY.

For an Identity solution to be a success in your business, you need to address the needs of both IT admins and end users. Skimping on features or ease of use for either will cause resistance and dissatisfaction.

WHEN IT COMES TO IT ADMINS, THEY NEED:

- **One place to manage** all users and access points
- **Policies that allow control across** the organization, at the group and individual user level
- **Out-of-the-box setup** that can plug into existing infrastructure
- **Coverage of all use cases** across the business
- **Compatibility with single sign-on**, enterprise password management and other IAM solutions
- **A variety of MFA methods,** whether biometric, push notification or adaptive, that can be offered at the user or group level

WHEN IT COMES TO END USERS, THEY WANT:

- Minimal setup steps required
- Little to no training needed
- A frictionless login experience that quickly becomes invisible
- Privacy of their data

WHY SMBS NEED A HOLISTIC, ALL-IN-ONE IDENTITY SOLUTION.

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.

A COMPREHENSIVE IDENTITY SOLUTION SHOULD INCLUDE:

- A single, easy-to-use admin dashboard
- Automation and minimal day-to-day IT management
- Custom, granular policies across SSO, EPM, and MFA
- One portal to unlock access to all apps and credentials
- Flexible MFA with support for many authentication methods
- Adaptive authentication that combines biometrics and contextual factors
- A frictionless experience for users
- Security by design

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.

LEARN MORE ABOUT LASTPASS BUSINESS

LastPass protects your business, without compromising ease of use and employee productivity. As an all-in-one access and authentication solution, LastPass empowers employees to generate, secure, and share credentials seamlessly, while providing simplified access and authentication to cloud and legacy apps, VPNs, and workstations. With LastPass password management, SSO, and MFA, your business can maintain visibility and control into your security while ensuring protection through LastPass' zero-knowledge security infrastructure.

- **Secure password sharing**
- **Dark web monitoring**
- **Basic single sign-on**
- **Central admin console**
- **100+ security policies**
- **Detailed security reports**
- **User directory integrations**
- **Universal password management**
- **Basic multi-factor authentication**

Mike Terry | 2082218573 | miketerry@outlook.com

Sources:

1. McAfee's CASB: MVISION Cloud
2. NTT Com Shadow IT Survey, 2016.
3. Forbes, 2018. "Why Your Millennials Are Leaving (And How to Keep Them)"
4. Verizon Data Breach Investigations Report (DBIR), 2019.
5. LastPass, "The Psychology of Passwords: Neglect is Helping Hackers Win", 2017.
6. LastPass and Vanson Bourne, "The SMB's Guide to Modern Identity: Bridging the Gap from Passwords to Identity", 2019.
7. LastPass and Vanson Bourne, "The SMB's Guide to Modern Identity: Bridging the Gap from Passwords to Identity", 2019.
8. SCORE, 2018
9. Cisco's, "Small and Mighty: How Small and Midmarket Businesses Can Fortify Their Defenses Against Today's Threats", 2018.
10. LastPass 2017 "Password Expose"
11. NTT Com Shadow IT Survey, 2016.
12. Verizon's 2019 Data Breach Investigations Report (DBIR)

03.23.21/PDF/ LMI1893dd