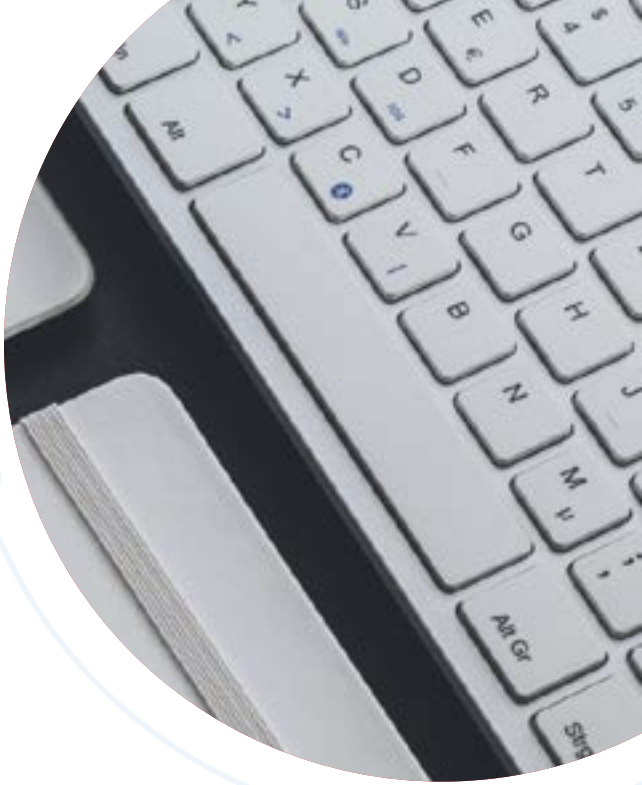
LastPass ••• | by LogMeIn

THE SMBs GUIDE TO MODERN IDENTITY

Bridging the Gap from Passwords to Identity

INTRODUCTION

As an IT and security professional at an SMB, you likely manage more responsibilities than ever. You may be juggling many competing priorities, from the helpdesk to network maintenance to managing user access and securing employee identities. But what exactly is an identity, and what do you need to know to maximize security and productivity with Identity and Access Management (IAM) solutions? Especially when your organization may not have resources of a large enterprise.



LastPass commissioned the market research firm Vanson Bourne to offer insights into the state of identity for SMBs. We surveyed 700 IT and security professionals at organizations ranging from 250 to 2,999 employees, across a variety of industries in North America, Europe and Asia-Pacific. Survey respondents held a range of IT security roles, with 37% at the C-level, 40% at the management level and 23% at the administrator level.

In this report, we've combined Vanson Bourne's findings with what we've learned from our customers' experiences. In the following pages, we offer SMBs a definition of identity, an understanding of different identity technologies, a look at how SMBs are approaching identity and an exploration of the unique challenges SMBs face.

Our goal is to give you clarity around IAM and actionable steps for applying this knowledge to further improve your organization's IAM program.

TABLE OF CONTENTS

1. WHAT IS IDENTITY?

Identity is **you**. It is the behavior, devices, access, and attributes that are unique to you as an individual. Your identity allows you to prove that you are who you say you are. In the workplace, your identity connects you to the right resources from the right devices at the right time, so you can work securely and efficiently.

But identity is complex. Around the clock, employees use many applications – both approved and not – from a variety of devices, networks and locations. Threats are ever-present and evolving. Every employee has their own identity, so every identity needs to be properly managed. Otherwise, the wrong users can access the wrong apps and resources, leading to security vulnerabilities and organizational inefficiencies.

Technology may be adding to the complexity of identity, but it's also the key to efficiently managing it. As we'll lay out in the coming sections, different solutions can be used to give you greater visibility into what users are accessing across the organization, and stronger control over that access.

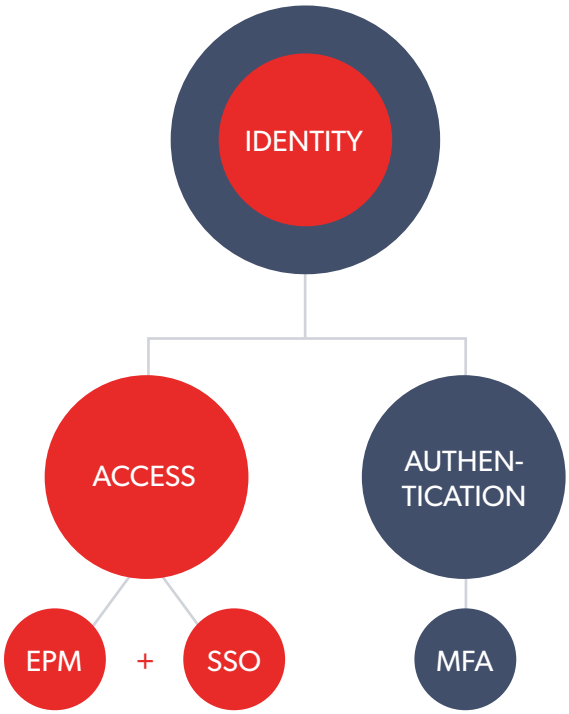
2. THE MODERN IDENTITY TECHNOLOGY STACK

Identity technologies aim to securely manage user identities to connect people to the technology they need to get their work done.

The identity technologies discussed throughout this report are:

- **Multifactor Authentication (MFA):** Combines two or more factors – something you are (inherence), something you know (knowledge) and something you have (possession) – to verify a user before granting access to an account or authorizing an action.
- **Single Sign-On (SSO):** Connects employees to applications with one set of login credentials, eliminating passwords for key services.
- **Enterprise Password Management (EPM):** Captures, stores and fills passwords for all form-based web logins and facilitates secure password sharing.
- **Privileged Access Management (PAM):** Secures, controls, manages and monitors access to critical accounts and systems.
- **Lifecycle Management:** Automates the provisioning, deprovisioning and management of user identities.

Used individually, each technology brings unique security and productivity benefits to a business. When brought together, businesses have complete security and visibility into every user and access point.



With more limited resources, it's particularly important for SMBs to look for all-in-one solutions that combine the key components and maximize an investment in identity technology.

3. UPGRADING IDENTITY CAPABILITIES IS A TOP PRIORITY FOR SMBs IN THE COMING YEAR

When it comes to security, an IT professional's job is never done. Whether it's upgrading old technology, keeping up with the latest threats or finding ways to more effectively train employees, IT teams have their work cut out for them.

Almost all IT professionals surveyed **(98%)** see room for improvement in the general security behavior of their employees (creating strong passwords, secure sharing and collaboration), and more than half **(53%)** cited large improvements needed in security behavior. Very few IT professionals **(< 5%)** believe all users in their organization operate in a completely secure manner. It's clear that very few businesses believe they're at the finish line when it comes to security, which isn't surprising given how rapidly threats and cyber security solutions are evolving.

98%

of respondents see room for improvement in the security behavior of their employees

53%

cite large improvements needed in the security behavior of their employees

<5%

believe all their employees operate in a completely secure manner

Due to competing priorities, IT teams are struggling to address their security needs. The average organization has at least four IT security objectives coming in the next year, including securing data **(75%)**, securing new technologies as they're adopted **(68%)** and reducing risk **(66%)**. **65%** agree that upgrading their IAM capabilities is also a primary objective, which can in part help IT teams achieve the first three objectives. Keeping the lights on ranked the lowest **(26%)**, which makes it clear that when it comes to security, complacency is the last option.

TOP 4 IT SECURITY OBJECTIVES

75% securing data

68% securing new technologies as they are adopted

68% reducing risk

65% upgrading IAM capabilities

4. MOST SMBs ARE CHALLENGED TO BALANCE EASE OF USE AND SECURITY WHEN IMPLEMENTING AN IDENTITY SOLUTION

Given that security is a high priority for most SMBs, it's no surprise that many are investing in identity solutions. **Less than 1% (0.29%)** of IT professionals believe that managing user access is unimportant to the overall security of the organization.

Unfortunately, **92%** of organizations also say they are experiencing at least one challenge when it comes to identity. The average organization struggles with three identity-related challenges: **47%** of respondents said balancing ease of use with increased security was a hurdle, **40%** cite the general security of their solutions and **37%** are facing demands from employees for a solution that's easy to use.

92%

of organizations experience at least one identity challenge

47%

Balancing ease of use with security

40%

General security of their solutions

37%

Employee demands for greater ease of use

The challenges also differ by country. Balancing ease of use with increased security ranks as the top priority in France **(56%)**, UK **(49%)** and US **(47%)** while the security of IAM solutions tops the list in Germany **(50%)** and Australia **(49%)**.

BALANCING EASE OF USE IS THE BIGGEST CHALLENGE

56% FRANCE **49%** UK **47%** USA

SECURITY OF IAM SOLUTIONS IS THE BIGGEST CHALLENGE

50% GERMANY **49%** AUSTRALIA

Even while IT teams recognize that identity technology will significantly increase the security of the organization, it's clearly a challenge to find solutions that employees are willing to use. Any technology that is tedious to use or slows down a user's workflow will be a hindrance, and adoption will suffer. That's why it's critical that SMBs choose identity solutions that are easy for employees to use and adopt, while still increasing the overall security of the organization.

5. IT PROS AGREE THAT POOR IDENTITY PRACTICES HAVE EXPOSED THEIR BUSINESS TO RISKS

IT teams are likely motivated to prioritize security and invest in identity because they've seen the consequences of failing to do so. **82%** of respondents say their business has been exposed to a risk as a result of poor IAM practices, including incorrect access controls **(41%)**, loss of employee data **(36%)**, loss of customer data **(33%)**, financial losses **(26%)** and exposure of their cloud environment **(32%)**. The risk of incorrect access controls was ranked highest in every country except Australia, who ranked the exposure of their cloud environment the highest **(40%)**.

82%

say their business has been exposed to a risk due to poor IAM

41%	36%	33%	32%	26%
Incorrect access controls	Loss of employee data	Loss of customer data	Exposure of their cloud environment	Financial loss

Not surprisingly, organizations that require huge improvements to the general security behavior of their employees are the most likely to have experienced most of these risks, primarily incorrect access controls **(46%)** and loss of customer data **(46%)**.

POOR SECURITY BEHAVIOR INCREASES RISKS

Average organizations*:
- Incorrect access controls — **41%**
- Loss of customer data — **36%**

Organizations with poor security*:
- Incorrect access controls — **46%**
- Loss of customer data — **46%**

Given the risks they've experienced, and potential threats, **81%** of IT professionals agree that if their organization does not implement a better approach to identity, then they are exposing themselves to a wide range of security risks. It's no surprise then that **94%** also agree that IAM should be a higher priority for their organization than it currently is. IT professionals are aligned that removing risky employee behavior from the equation with identity technologies is an effective way to reduce threats to the organization.

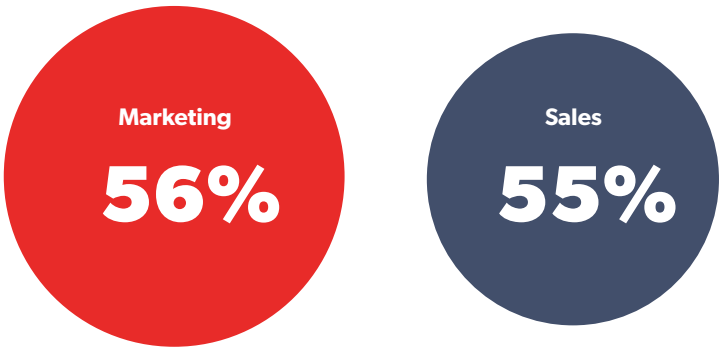
* *The average response across all 700 respondents.*

* *The average response from respondents who noted huge improvements to the general security behavior of their employees are required.*

6. MARKETING AND SALES TEAMS ARE THOUGHT TO POSE THE MOST RISK TO AN ORGANIZATION

Who's putting the business at risk? **56%** of IT security professionals rank marketing among the two departments that are most likely to operate in an insecure manner, with the sales team ranked close behind by **55%**. Why? It could be that these teams, particularly marketing, are more likely to work with outside contractors or agencies and may not always follow protocol when doing so. They may also be more likely to try new cloud services – without IT approval – for the data insights and productivity benefits they may offer.

DEPARTMENTS MOST LIKELY TO ACT INSECURELY



DEPARTMENT LEAST LIKELY TO ACT INSECURELY

Finance

31%

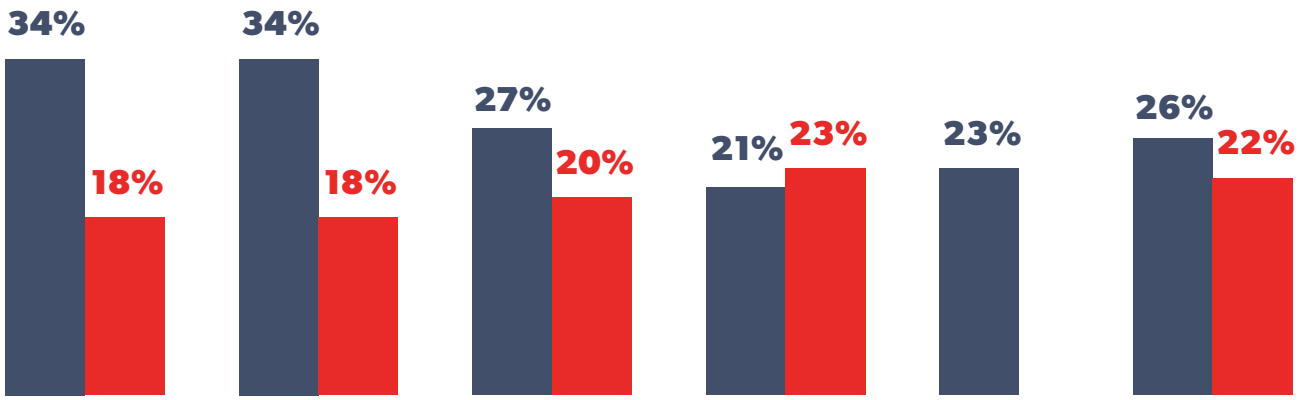
Finance was least likely **(31%)** to be considered among the riskiest departments; we can assume it's because more rules are in place to regulate their behavior due to the sensitive data they handle on a regular basis.

Given that employees at all levels, across all departments, can pose a risk to the organization, it's important that IT teams implement easy-to-use identity technologies that can be deployed to all employees. Identity solutions can minimize or eliminate risky behaviors, like reusing weak passwords or sharing account access without administrative oversight.

7. PASSWORDS CONTINUE TO CAUSE FRUSTRATION – AND RISK

Unfortunately, IT teams continue to spend valuable time and resources dealing with tickets for password-related problems and security concerns.

MOST IT TEAMS RECEIVE TICKETS FOR:



Lost or stolen credentials monthly or a couple of times a month (18%)

Compromised credentials monthly, though 18% admitted they don't know how often compromised credentials are reported

Accidental sharing of credentials with the wrong person monthly or a couple of times a month (20%)

Forgotten passwords daily or a couple of times a week (23%)

Unprompted password updates monthly

Issues with prompted password updates monthly or even weekly (22%)

On average, IT security teams spend **4 hours per week** on password management-related issues alone and receive **96 password-related requests per month**. Some IT teams receive over 25 forgotten password requests in a day. One organization even reported that their IT team spends up to 30 hours a week on password management!

Given the ongoing resource drain that passwords pose to organizations, it's unsurprising that almost all **(95%)** of IT security professionals report that their organization should place more emphasis on the importance of strong password behavior. This attitude is seen most prevalently in Germany at **98%**.

Large proportions of respondents from organizations that have invested in an EPM solution, or plan to invest in an EPM solution, agree that this solution would deliver greater organizational security **(54%)**, simplified management of user profiles and credentials **(47%)** and increased employee productivity **(43%)**.

From the above data, it's clear that many businesses have not completely addressed all password-related obstacles and security risks within their organization. Interestingly, **90%** of respondents who believe that huge improvements are required to the general security behavior of their organization's employees report that they have an enterprise-level solution in place, suggesting that EPM is just the starting point in managing identity.

4 hours

spent a week on password management issues

95%

of IT security professionals believe their company should better emphasize strong password behavior

93%

of IT professionals claim to have a good or complete understanding of EPM solutions

8. SINGLE SIGN-ON SERVES A CRUCIAL ROLE – BUT LEAVES CRITICAL GAPS WHEN USED IN ISOLATION

Most IT professionals agree that managing user access is crucial. In fact, **90%** say that managing user access is either critically or very important to the overall security of the organization. This attitude is highest among respondents from the UK **(93%)**. Given the risks and resource drain associated with passwords, single sign-on (SSO) solutions offer the benefit of eliminating passwords for IT-supported apps and simplifying the login process for employees accessing key apps in the cloud and behind the firewall.

Most organizations have invested in some form of SSO, with **74%** of respondents indicating they have an SSO solution in place. It's no surprise, then, that many IT professionals cite a high level of familiarity with SSO solutions, with **54%** claiming a complete understanding and **40%** a good understanding. Familiarity is highest in the US with **63%** of respondents indicating a complete understanding, and lowest in Australia with only **39%** indicating the same.

Around half of IT security professionals **(49%)** from organizations that have invested in or plan to invest in an SSO solution agree that this would deliver simplified management of user profiles and credentials **(49%)**, greater organizational security **(48%)** and increased employee productivity.

Though SSO delivers the benefit of reducing the risk of employee password behaviors by eliminating passwords, many IT professionals recognize SSO as simplifying the employee login process with only one password to remember. Also note that visibility is not an expected benefit (**only 31%**), which means many IT professionals acknowledge that SSO solutions on their own do not offer comprehensive insight into user access across the business.

Unfortunately, SSO is not a panacea, and **38%** of IT professionals surveyed indicate that, of the technologies covered in this report, SSO is the worst approach to managing identity on its own. Many apps aren't integrated into an SSO solution – whether because they don't support SSO, they're not high enough priority for IT to configure SSO or IT doesn't even know they're being used. That's why **80%** of IT professionals agree that relying on SSO alone will leave a variety of cloud apps and privileged accounts unsecured. Pairing SSO technologies with an EPM solution ensures that every access point is secured, while removing most, if not all, access-related obstacles faced by employees.

49%

of organizations with SSO agree that it simplifies user and credential management

80%

agree relying on SSO alone will leave a variety of cloud apps and privileged accounts unsecured

38%

of IT professionals indicate that SSO is the worst approach for managing identity on its own

9. STRENGTHENING USER AUTHENTICATION WITH MFA IS A HIGH PRIORITY FOR SMBS

Multifactor authentication (MFA) has gained in popularity over the past few years as organizations recognize the inability of passwords alone to protect their business. Most organizations have invested in MFA solutions, with **73%** indicating they have MFA technology in place, while **19%** expect their organizations to invest in MFA in the coming year. By requiring additional factors to prove a user's identity before access is granted, MFA protects businesses from the risks of weak and compromised passwords.

73%

of organizations indicate they have MFA technology in place

19%

expect to invest in MFA within one year

59% of IT professionals agree that strengthening user authentication is critical and cite it as among their key priorities for improving their identity capabilities. MFA is prioritized the most in Germany, with **63%** of IT professionals agreeing it's among their key IAM objectives. It's no surprise, then, a third of all respondents **(35%)** say MFA is the best approach for getting started with identity.

Most IT professionals cite a good **(45%)** or complete **(48%)** understanding of MFA. However, only **35%** of professionals in France and Australia cite a complete understanding of MFA, so additional education is likely needed to increase confidence in using and deploying MFA solutions.

Implementing biometrics is a priority for **36%** of respondents' organizations, which is a specific functionality of MFA. Prioritization for biometrics is seen highest in Germany at **39%**. We expect to see use of biometrics in SMBs continue to increase in the coming years, as biometrics become more readily available via smartphones and employees become increasingly comfortable with authentication options like fingerprint, voice and facial recognition. SMBs looking to deploy MFA solutions with biometrics should understand how the data is used and stored and ensure compatibility with all use cases in the organization.

59%

of IT professionals agree that strengthening user authentication is critical

93%

of IT professionals claim to have a good or complete understanding of MFA

36%

of respondents' organizations see implementing biometrics as a priority

IT security professionals from organizations that have invested in or plan to invest in MFA see the most likely benefits as greater organizational security **(60%)**, fewer instances of incorrect access to confidential information **(48%)** and decreased risk of credential/password theft **(47%)**. Again, visibility is not an expected benefit of MFA (only **33%**), so a solution that offers greater insight into authentication across the business would hold great value when coupled with MFA.

With only **1%** of respondents saying that MFA would not provide any benefit, most IT and security professionals agree that MFA is a valuable and necessary technology. It significantly increases the security of an organization by requiring users to provide additional factors before they can gain access to systems. Key features like biometrics and adaptive authentication can provide IT teams with more flexibility and greater security, though SMBs will want to look for solutions that still provide reasonable cost of ownership and minimal ongoing management.

60%

see greater organizational security as one of the most likely benefits in MFA solutions

1%

of respondents say that MFA would not provide any benefit

10. AUTOMATING IDENTITY MANAGEMENT IS ON THE RISE

Automating tasks related to identity management can save SMBs time and resources. On average, **40%** of all respondents prioritize automating identity processes as a key objective, with almost half in Germany **(47%)** and Australia **(46%)** focused on improving automation.

We expect to see the role of automation increase moving forward as more SMBs deploy identity programs across their organization. Lifecycle management solutions can automate the provisioning and deprovisioning of identities to automatically provide users with the access required for their role and simply remove the account when the user leaves the organization or changes roles.

40%

of all respondents prioritize automating identity processes as a key objective

Focused on improving automation

Germany **47%** Australia **46%**

11. IT PROFESSIONALS AT SMBs RECOGNIZE PRIVILEGED ACCESS MANAGEMENT'S SECURITY BENEFITS

More than half **(60%)** of SMBs have invested in privileged access management (PAM). **51%** of respondents overall cite a complete understanding of PAM, with Germany citing the least familiarity with only **40%** indicating a complete understanding. An additional **38%** of professionals cite a good understanding. Overall, additional education around PAM would be valuable for IT professionals globally.

51% **of IT professionals with PAM experience agree that it provides greater organizational security**

IT professionals from organizations that have invested in or plan to invest in PAM agree that the primary benefits of PAM solutions are greater organizational security **(51%)**, fewer instances of incorrect access to confidential information **(45%)** and increased employee productivity **(42%)**. Additionally, **26%** of SMBs plan to invest in a PAM solution in the coming year.

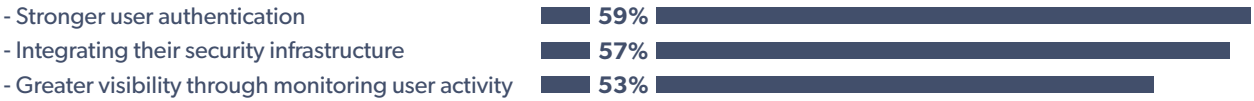
12. SMBs NEED A HOLISTIC SOLUTION THAT IS EASY TO IMPLEMENT AND READILY ADOPTED BY USERS

As we consider the data we've highlighted throughout the report, one thing is clear: While IT says they understand the need for managing identity, they've yet to bring a full identity solution to their organization. But rather than investing in piecemeal solutions, **93%** of IT professionals agree that bringing the various aspects of identity and access management under one solution would greatly benefit the overall security of the organization. Given their resource constraints, we agree that SMBs need an all-in-one identity solution.

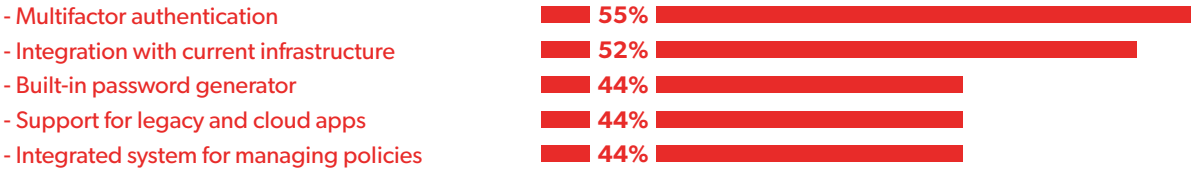
The minority of respondents **(23% - 38%)** have yet to complete their investment in all aspects of identity. Only **24%** of IT professionals surveyed cited budget as a challenge for IAM, so perhaps it's a matter of finding the right solution for your business.

OF ORGANIZATIONS AGREE A UNIFIED IAM SOLUTION WOULD BENEFIT THEIR ORGANIZATION

When evaluating their current identity capabilities, IT professionals see room for improvement with:



Our respondents also indicated several features for their ideal identity solution:



In other words, the ideal IAM solution would support a wide range of use cases, integrate and support the existing technology ecosystem in the business, specifically address password hygiene and allow admins flexibility in customizing the solution to meet their organization's unique security requirements.

Putting these ideal features into practice, IT professionals report on average that their organization has four key priorities regarding improving their IAM capabilities moving forward; strengthening user authentication **(59%)**, integrating security infrastructure **(57%)**, monitoring user activity **(53%)** and simplifying user access **(44%)** topped the list. For the most part, these priorities mirror the main challenges that SMBs are currently experiencing. For example, strengthening user authentication and integrating the security infrastructure are aimed at tackling the challenge of securing identity solutions, while simplifying user access will help address the demand from users for an easy-to-use solution.

As we've seen throughout the report, identity technologies are expected to offer both security and productivity benefits. In fact, most respondents **(93%)** agree that implementing a better approach to IAM could increase employee efficiency. To realize those benefits, it's crucial for SMBs to invest in a holistic solution that balances user experience with security.

13. WHERE TO GO FROM HERE: WHAT SMBs NEED TO KNOW TO TAKE NEXT STEPS IN MANAGING IDENTITY.

As an IT professional at an SMB, you may find yourself in any number of different positions with regards to your identity program. Perhaps you've invested in one IAM technology and are wondering how to add others. Perhaps your organization has long used all of them but are finding your existing solutions no longer support the business. Or, perhaps your business has no identity program in place, and you're wondering where to start.

FIRST, WE RECOMMEND UNDERSTANDING:

- **The problems you're trying to solve:** Is managing user access a hurdle? Are employees securely managing passwords? Is too much security impacting employee productivity?
- **Your requirements for solving those problems:** What type of identity solution meets the challenge you're facing? Is there a unified solution that can meet all of those challenges in one?
- **The technologies you currently use to meet those requirements:** Are you using password management? Single sign-on? Multifactor authentication?
- **Current gaps in the technologies you're using:** Are you using specific IAM technologies in isolation?
- **Additional technologies that may help address those gaps:** How can you complement your existing IAM solutions to securely manage user identity?

By clarifying your current identity position, you can research and evaluate identity technologies with greater focus and intent. Careful planning and decision-making can ensure that an investment in IAM solutions brings the maximum productivity and security benefits.

A holistic solution that brings the benefits of each IAM technology together is the best option for SMBs. An all-in-one solution that offers unified visibility and control across every access point, with an end user experience that is easy to learn and use, 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.

MANAGE USER IDENTITY WITH A SINGLE SOLUTION

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.

- 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

Unify access and authentication:

www.lastpass.com/products/identity

06.26.19/PDF/ LMI0638C