LastPass •••|
by LogMeIn

How Identity and Access Management Empowers Businesses to

SECURELY WORK FROM ANYWHERE

INTRODUCTION

Organizations have rapidly shifted their businesses to operate remotely, and the benefits of doing so are significant. However, with remote work also comes risks.

Remote work isn't a trend, but rather the new normal. We have now entered the work from anywhere era. This means seamless, secure access for employees and security for the business, no matter where employees are working from. The reality of work from anywhere means IT has to facilitate secure access for employees from many locations, from many devices for many applications – which complicates the process of ensuring employees are who they say they are.

In the work from anywhere era, it's critical organizations develop an identity and access management (IAM) strategy that authenticates and authorizes every employee so that they gain access to the business resources they need to stay productive.

By determining an IAM strategy that secures the business no matter where employees are working from, organizations can ensure only the employees gain the right access to the right resources at the right time, while IT maintains complete visibility and control over every login – no matter where the team is working.

TABLE OF CONTENTS

THE CHALLENGES OF SECURING A REMOTE WORKFORCE

While there are significant benefits remote work, there are also some risks to consider.

Cybercrime and phishing attacks are on the rise; some organizations have seen phishing schemes targeting remote workers rise by up to 40%. And organizations are not prepared. Cybercriminals know organizations are not prepared, and are taking the opportunity to spot and exploit vulnerabilities.

Allowing remote access to the network widens the surface of attack for cyber criminals. It also adds complexity to the IT environment, and these complex networks are getting harder to secure. This poses challenges to a company's IT network, as well as their employees.

Employees are working from more locations than ever before

IT needs to ensure every login is secure – no matter where employees are

Cybercriminals spot and exploit vulnerabilities

up to **40%**

increased phishing schemes targeting remote workers

From an IT perspective...

For IT teams, the biggest change is the loss of control. As more workers gain remote access, managing **where** and **how** people access business resources becomes the main challenge.

Some of the associated risks include:

- **Incorrect access controls:** With increased remote work comes a higher risk of employees having access to data they don't need for their role.
- **Data breach:** When the IT parameters of a corporate office no longer exist and employees are working from anywhere, there is a greater risk of a data breach.

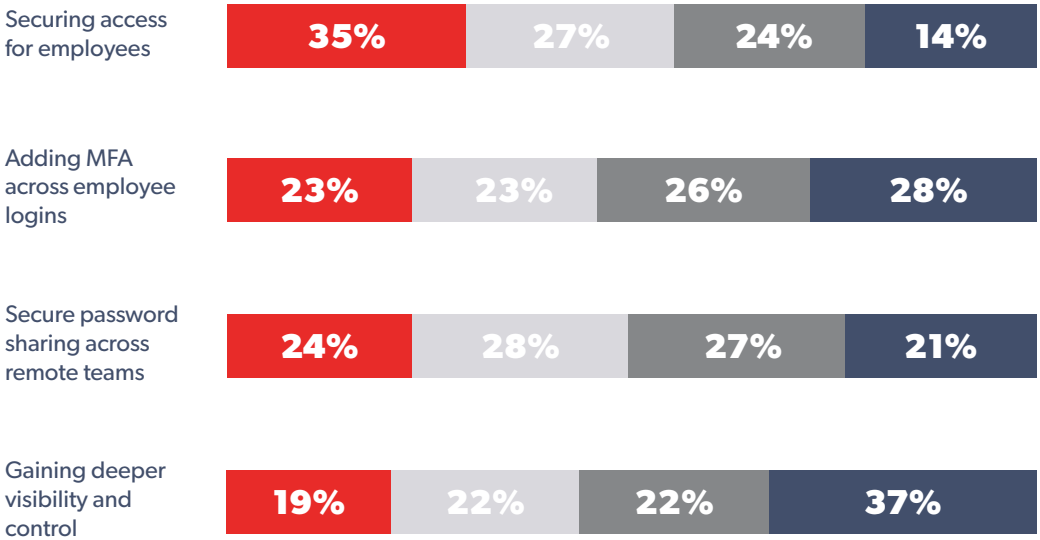
From an employee perspective...

If IT teams don't have a secure way to delegate access to employees, remote workers will be unable to securely access their work. This can lead to employees insecurely accessing what they need which puts the business at risk, or simply unable to access anything which damages productivity.

According to our recent IDG study, secure access for employees is ranked as the top IAM priority for remote work, which means decision makers should be considering a single sign-on (SSO) solution, which securely connects employees to their work to tackle this challenge.

REMOTE WORK PRIORITIES

Ranked from 1 to 4 with 1 being "Most critical".



IAM IS CRITICAL TO SECURING A REMOTE WORKFORCE

Remote working is the now normal and businesses need a long-term, robust IAM strategy to secure their remote workforce. The associated risks and challenges mean that a remote work IAM strategy is a critical priority.

According to our recent remote work research in partnership with IDG, 96% of organizations have seen their IAM strategies impacted as a result of remote working and 98% of IT decision makers consider IAM critical to securing the remote workforce. Management and long-term considerations of IAM need to be modified to in order to provide adequate security and the small percentage of those not doing so pose great risk to their business-critical functions.

96%

of organizations have adjusted their IAM strategy as a result of remote work.

98%

agree IAM is critical to securing a remote workforce.

How IAM can improve security for a remote workforce:

- **Single sign-on (SSO):** SSO allows you to maintain control over access, no matter where your team members are logging in from. Whether they're in the office, working from home or another remote location, they can access multiple apps with one single password. A secure connection is created, enabling employees to tap into the necessary resources with a seamless authentication process. This provides IT with added control over employee logins through security management, enabling easier access for a remote workforce, while also improving the user experience and boosting productivity. With secure access for employees being ranked as the top IAM priority for remote work, it's likely that SSO will become a must-have technology for organizations in the work from anywhere era.

- **Password management:** Remote working can only be efficient when there are easy and secure ways to share data and sensitive information. Even something as simple as sharing a login password poses a risk when you're not in the same physical office. In a typical business environment, a password may need to be shared with a variety of colleagues. And in the absence of a dedicated password management tool, people will always choose the fastest (and often insecure) way to do so. A password manager can enable easy password sharing in a few clicks without compromising your security.

- **Multifactor authentication (MFA):** MFA is another technology to consider when looking at identity management for your organization, and is considered to be one of the most effective ways to secure remote workers. It requires employees to authenticate with two or more factors during the login process.

62%

of IT decision makers believe MFA to be the most effective way to secure their remote workforce

With 80% of all data breaches caused by passwords alone, this makes MFA more important than ever. Phishing scams are on the rise and MFA helps to add an extra layer of security. It can also minimize threats such as spear phishing, keyloggers, credential stuffing, brute force attacks and more. The added benefit of MFA is that it's seamless for employees to use. The additional layer of security for every login via biometrics is easy for employees to authenticate with; it's a win for IT and a win for employees.

BUILDING YOUR REMOTE WORK IAM STRATEGY

As well as maximizing security controls, IT teams must also minimize complications for employees. Usability is key so choosing solutions that facilitate collaboration and quick access to documents should be a priority. With the right IAM strategy in place, IT can secure remote workers and employees can seamlessly access what they need; everyone's happy.

In order to secure your network and ensure ease of use for remote workers, it's important to leverage SSO, password management and MFA for a combined approach. Our data tells us that SSO is important to the overall security for 90% of businesses, while 59% business rank MFA as a top area for improvement. Additionally, 95% of companies see a need to emphasize strong password behavior in their teams. So, it's clear that all three technologies play a major role in security.

On their own, these technologies play a vital role in preventing breaches and improving usability. Utilized simultaneously, they provide a seamless, holistic identity solution.

The benefits of a combined IAM approach:

- **Access controls are fully managed:** Your IT teams will be able to give or revoke access in real-time to different users. Single sign-on uses a strong authentication protocol that removes the need for remembering multiple passwords, all under the control of IT. For instance, a team member can access the network from their mobile, laptop or tablet, all with one easy login.
- **Easy access from anywhere:** You can facilitate remote working and digital transformation with easy, secure access from any location. This means that your teams can collaborate effectively even with different physical locations and time zones – all while improving user experience and security.
- **Reduce IT costs:** By automating and standardizing many aspects of identity, you can better allocate your IT resource. IAM also creates day-to-day efficiencies that lead to significant cost savings in the long run.
- **Simplify auditing and reporting:** Consolidating identities and passwords with SSO makes it easier for IT departments to audit user credentials and create detailed reports. Instead of having to look at a huge number of devices to figure out who is accessing the network, one single identity and login provides instant identification.

59%

Strongly agree increasing security for their remote workforce is a top priority over the next 12 months.

#1

Securing access for employees is ranked as the #1 IAM priority for remote work

SECURITY FOR THE NEW NORMAL

Work-from-anywhere is the new normal, and organizations that are slow to adopt this new format will inevitably get left behind. Digital transformation is the only way to futureproof your business, and in the long run it can help you retain staff, attract new talent, and facilitate efficient processes.

While security risks are only going to increase as your remote capabilities expand, that doesn't mean your business has to be at risk. By putting the right IAM technologies and policies in place, IT can protect against risks in a remote working environment. As more companies shift to remote business models, it's critical for organizations to consider how they are managing identities and access to their network.

In light of recent events, major brands like Twitter have announced their employees will be allowed to work from home indefinitely. Businesses of all sizes are planning on being more flexible with their workforce, and many are being forced to review outdated systems to support these new, digital ways of working.

As we move into the future, IAM will continue to increase in importance. It's very simple – a network is much easier to secure when you know who's connected to it. By choosing IAM solutions that consolidate identities and logins, IT can regain control of users and their access levels based on preset protocols.

With the right IAM strategy in place, you can fully manage employee access, add layers of silent security, and make it easy for workers to collaborate with one another. Having this sort of flexible environment benefits everyone, including employees who will have a better work/life balance. Through a holistic IAM strategy, you can achieve all of this while reducing the risk of cyberattack on your company and securely enabling your employees to work from anywhere.

08.06.20/PDF/ LMI1526