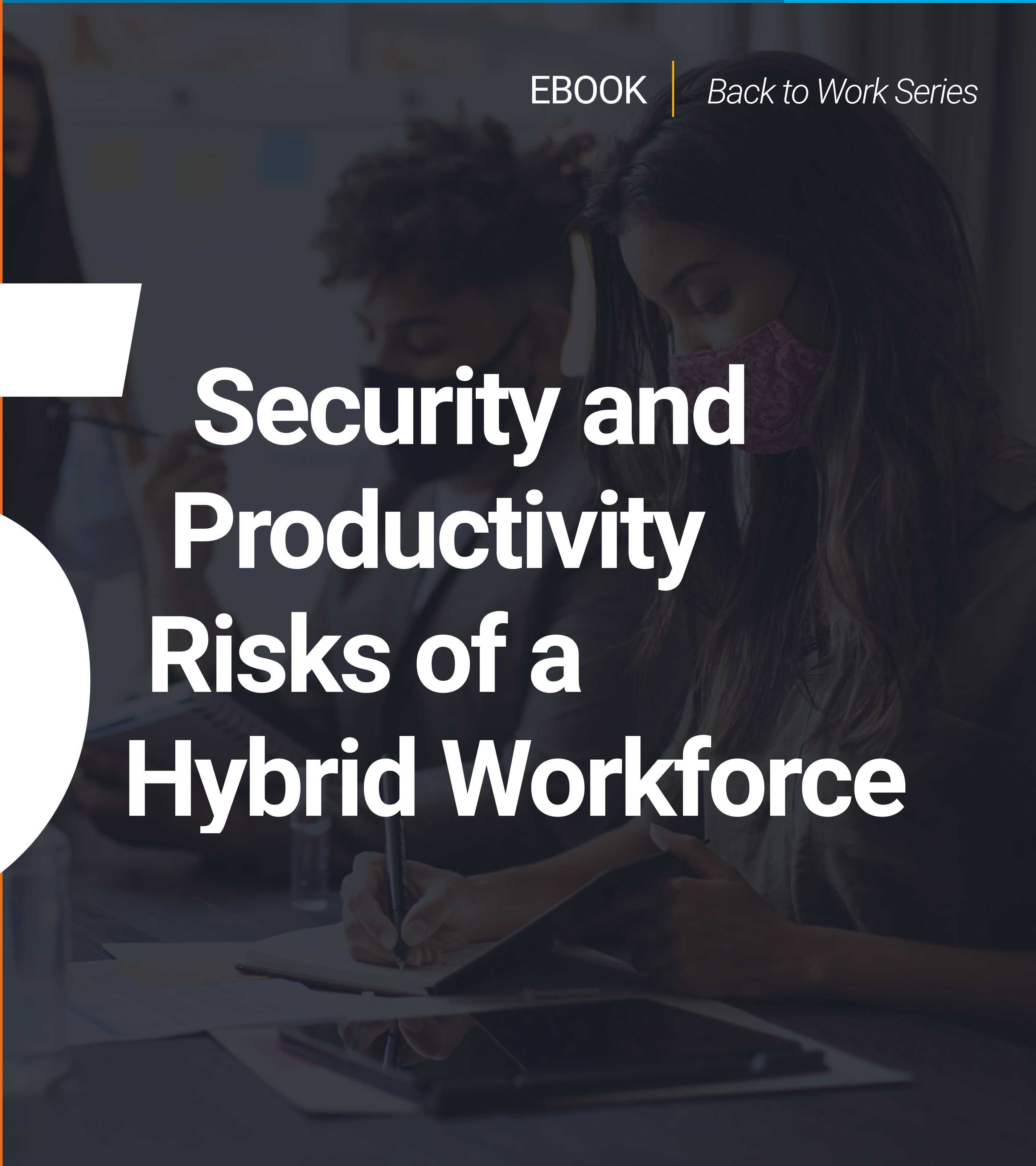
onelogin

EBOOK | *Back to Work Series*



5 Security and Productivity Risks of a Hybrid Workforce

Introduction

The Covid-19 crisis has forced global businesses to change operations in a variety of unprecedented ways. To navigate and halt the spread of the pandemic, organizations around the world adopted remote work policies where employees had to maintain work and productivity from the confines of their home. And although the pandemic is beginning to subside globally, remote work is here to stay. Even companies that plan on going back to the office are considering hybrid work options, meaning employees can work both remotely and in-person at the office.

Many organizations were unprepared for their employees to be entirely remote. They didn't have the processes, they didn't have the technology, and most importantly, they didn't have the right security measures in place to ensure that employees can safely access corporate applications and data. And unfortunately, because of the sudden shift, businesses had to make quick decisions to implement the right technology needed to not compromise security. While some businesses still have not adopted the right processes and technologies to fully enable remote work, most organizations have implemented some best practices. However, businesses now need to ensure that their remote work policies are sustainable, and that they have the right technology in place to ensure that their ongoing hybrid work environments will be successful.

One of the most effective ways for your teams to make a seamless transition to working hybrid or remotely, while ensuring the right security measures, is to implement an Identity and Access Management (IAM) solution, like OneLogin. An IAM solution enables your organization to connect with technology in a way that is secure, seamless, and scalable from any location on any device–so your business remains productive during times of change.

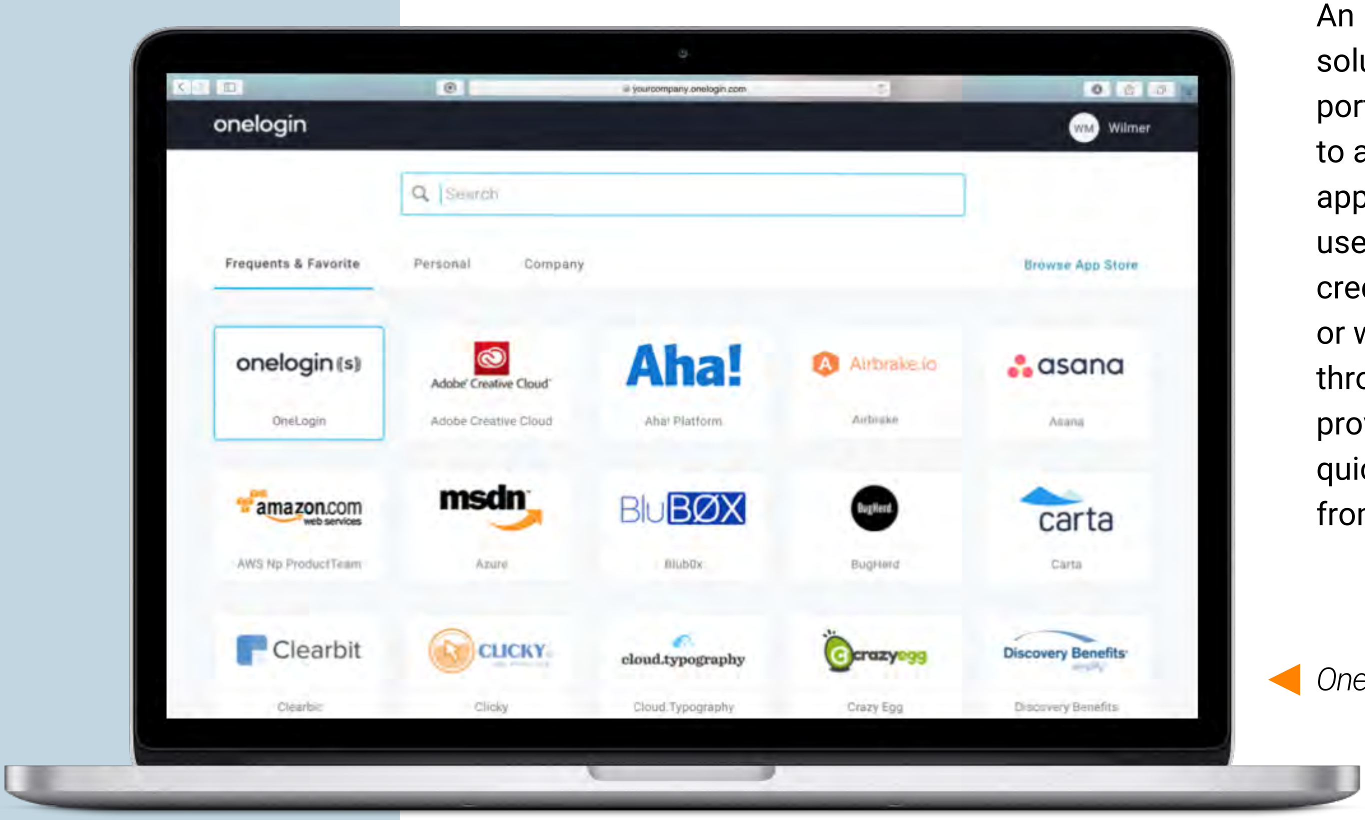
In this ebook, we discuss the top reasons why implementing an IAM solution is critical to the success of your hybrid workforce.

RISK 1

Your Employees Need Easy and Secure Access to their Applications

One of the most critical elements to keeping your business and employees productive whether working from your office or working remotely is the availability of business-critical applications. Your employees need to be able to work from anywhere without having to remember multiple passwords and keep track of multiple applications. Without a strategy and process around access, you can end up losing a lot of productivity. Imagine all of your employees trying to log into each of your applications from home on an unsecured network? Not only does this impact security, but it also hinders productivity as your employees scramble to access what they need to run the business.

An Identity and Access Management solution, like OneLogin, provides a single portal with a single and secure password to access all of your critical business applications. With Single Sign-On (SSO) users have to enter only one set of credentials to access both on-premesis or web-based applications. Additionally, through OneLogin's automated user provisioning, your IT department can quickly onboard and offboard employees from any location.



OneLogin Single Sign-On Portal

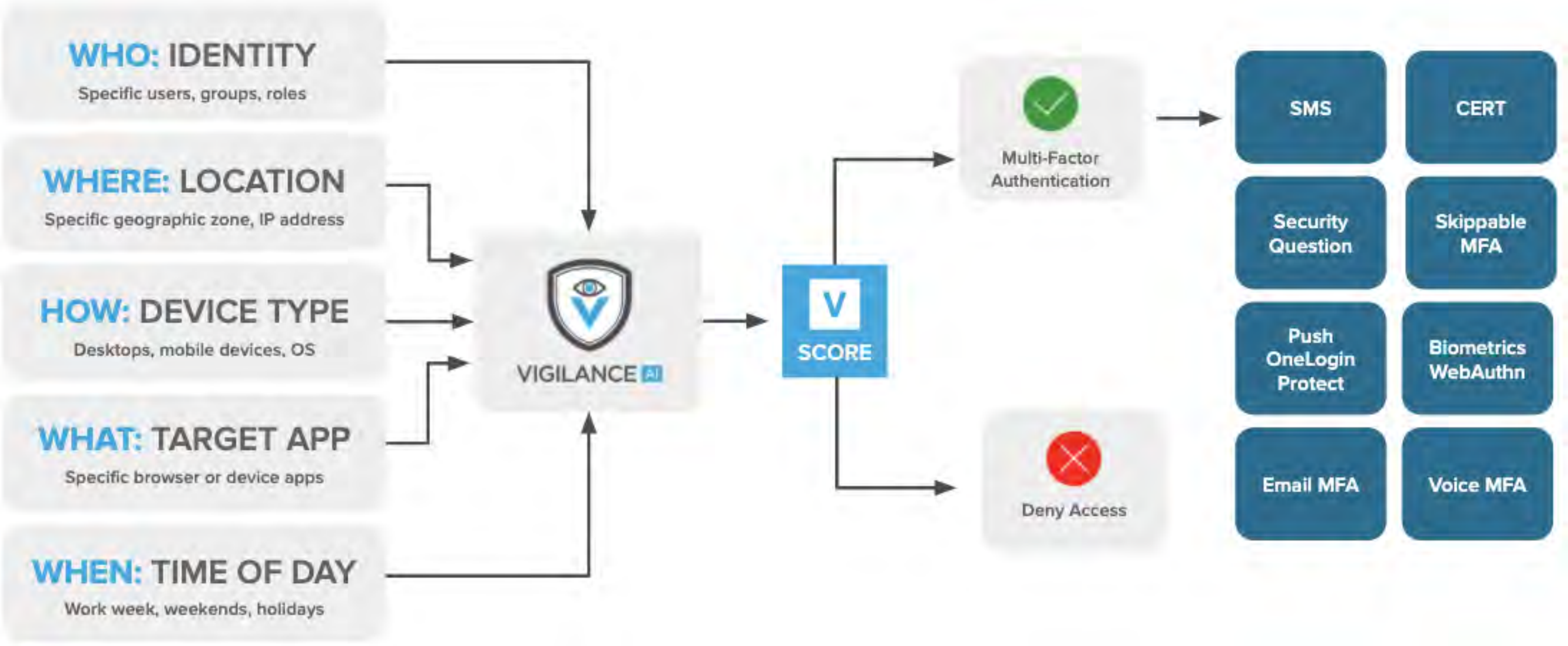
RISK 2

You Risk Losing Control Over Your Corporate Data

When your employees log in from remote locations and unsecured connections, you risk losing control over your corporate data, as most methods of remote access are vulnerable to security threats. You are no longer under the cover of your corporate internal network, you aren't able to implement security reviews, and your employees could be accessing applications from unmanaged devices. To ensure that your corporate data remains secure regardless of where your employees access that data, leveraging a VPN can provide the protection you need.

Because remote workforces are highly vulnerable, we saw a huge surge of cyberattacks at the height of the COVID-19 pandemic and we continue to see these numbers climb. Hackers are increasingly using social engineering and email phishing attacks to steal confidential data. And with many workers remaining remote and organizations embracing a hybrid work environment, we expect this to continue.

By implementing an IAM solution, you can secure your hybrid workforce through a variety of ways. With OneLogin, your workers can maintain one set of credentials to access their applications or connect to a VPN using a RADIUS endpoint. Additionally, by implementing Multi-Factor Authentication (MFA) that leverages machine learning capabilities, like OneLogin's SmartFactor Authentication™ , you can automatically detect risky behaviors and logins. SmartFactor uses OneLogin's Vigilance AI™ engine to generate different profiles of typical user behavior--like location, device, applications access, time-of-day, etc, and provide a risk score that enforces different authentication factors based on perceived risk. So, if SmartFactor detects a malicious login attempt, it can prompt the user for a variety of authentication factors or cut off access entirely.



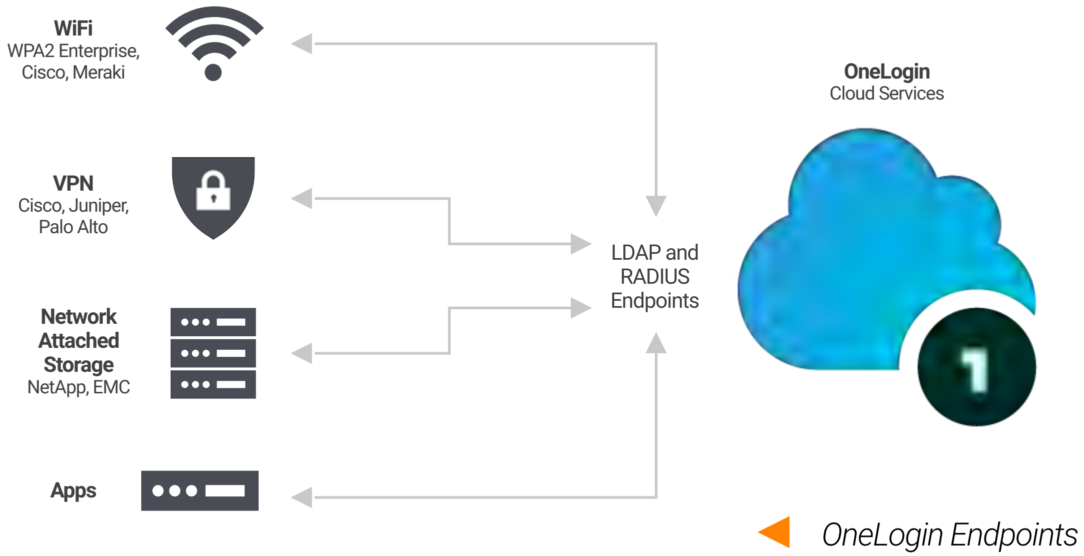
How SmartFactor Authentication Works

RISK 3

Your Employees Need to Access Both Cloud and On-Premises Applications

Many organizations have applications that live in the cloud and applications that live on-premises. And historically, access to these environments are often managed separately. If your employees are unable to access your critical on-premises applications, you run a very serious risk of lost productivity, lost revenue, and customer service implications.

Without a solution that can operate in a hybrid environment, you will be impacted with administration complexity, lost productivity, higher costs, security vulnerabilities, and more. To bridge the gap between the cloud and your on-premises applications, OneLogin Access becomes the central point of management for all of your directories, users, and authentication policies. By leveraging OneLogin, your applications can remain safely behind your firewall, no matter where your employees access your systems.



What if your organization uses Microsoft Remote Desktop Gateway (RDG) Server or Remote Desktop Web (RDWeb) to access your on-premises Windows servers or desktops?

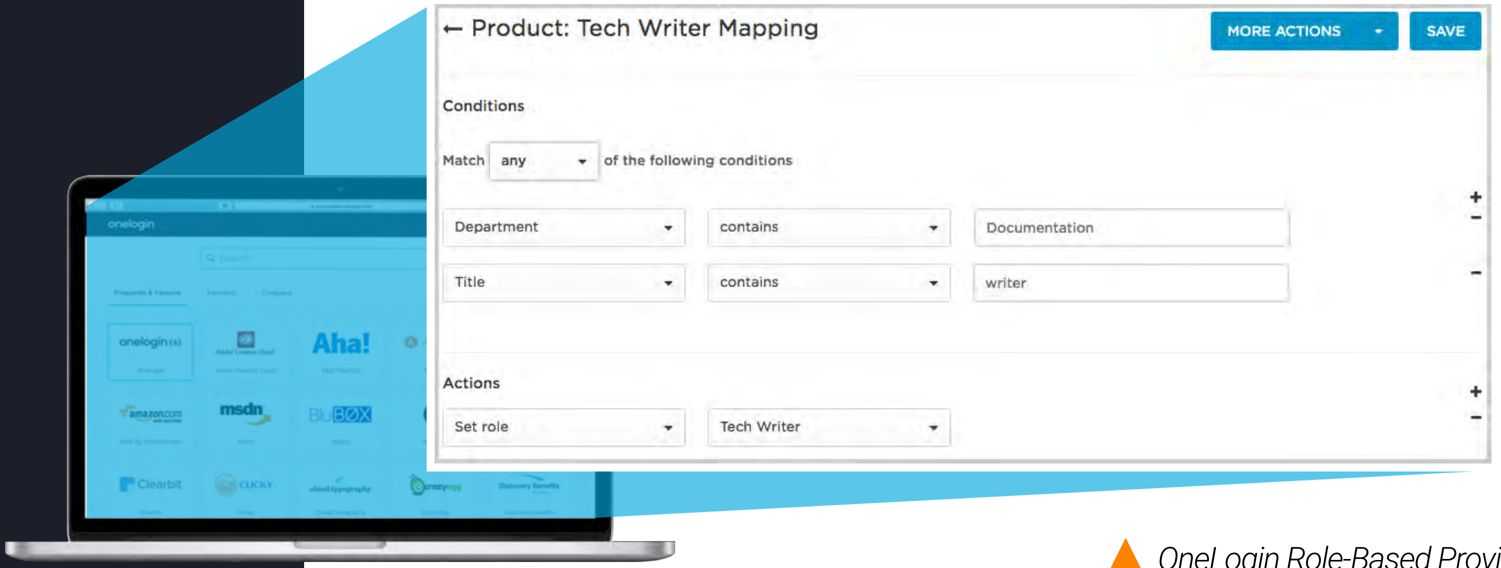
With OneLogin you can secure access to both by prompting your users for authentication.

RISK 4

Onboarding and Offboarding Remotely is Time Consuming and Labor Intensive

Manual user management is error-prone and incredibly labor intensive. Now, just imagine that your IT team has to consistently provision remote employees. Access provisioning typically involves a variety of activities including creation of user accounts, password management, application provisioning, and more. In many organizations all of this is done manually on a new hire's computer or maybe your IT department does some of it and the user completes the rest. And what about when an employee gets let go and you need to shut off access? If you are in a hybrid work environment, deprovisioning is not as easy as the employee dropping off a computer on the last day.

With an IAM solution, like OneLogin, administrators can streamline and automate the provisioning and deprovisioning process remotely in real-time. You can automate provisioning for different roles and levels across your organization by setting up rules and entitlements. And for offboarding, administrators have a "kill switch" for shutting down access in seconds.



← Product: Tech Writer Mapping

Conditions

Match any of the following conditions

Department contains Documentation

Title contains writer

Actions

Set role Tech Writer

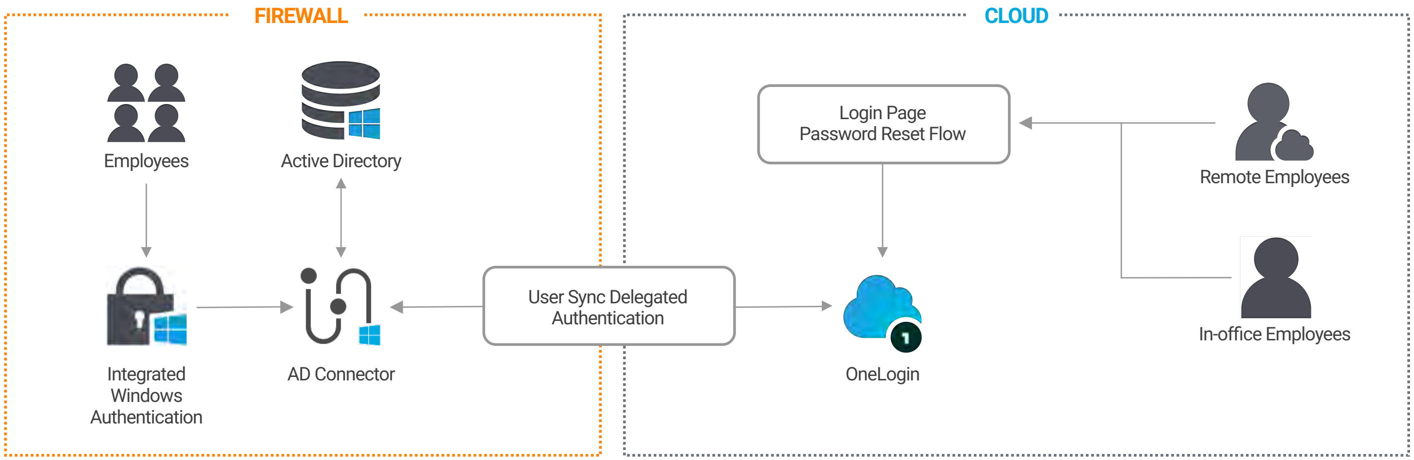
OneLogin Role-Based Provisioning

RISK 5

Password Resets and Locked Accounts Can Overwhelm Your IT Department

Your IT department and help desk is the linchpin to your hybrid work effectiveness. With so many of your employees working remotely, how do you scale? Your IT department is going to quickly get overwhelmed with tasks like password resets, account lock-outs, connection assistance, and more. Prior to 2020, according to Gartner, over 50% of help desk tickets in a typical organization are related to password reset. This has only increased with a largely remote workforce. Additionally, account lock-outs can be particularly detrimental for remote workers--not only is the employee frustrated and productivity is impacted, but operations slow down and there can be customer service and revenue implications if the locked-out employee is customer-facing.

By implementing OneLogin, your IT department can leverage a hands-off and easy way to synchronize password changes across Active Directory (AD), OneLogin, and your critical applications. When users either forget their passwords or their password expires, they can proactively change their password in AD directly through OneLogin—so your IT department saves a considerable amount of time.


FIREWALL
Employees
Active Directory
Integrated Windows Authentication
AD Connector
User Sync Delegated Authentication
CLOUD
Login Page Password Reset Flow
Remote Employees
OneLogin
In-office Employees

OneLogin Password Reset

Conclusion

Now that we are starting to recover from the pandemic, offices all over the world are opening. However, most organizations won't be returning to how things were pre-pandemic. Instead, companies and employees have embraced remote culture and will be building in technology and processes to enable successful hybrid environments.

To sustain a work from anywhere environment, organizations need to ensure the security of their data and accessibility of their systems. And by implementing an Identity and Access Management solution, like OneLogin, you can securely connect your people with the technology they need regardless

About OneLogin

OneLogin is the number one value-leader in Identity and Access Management. Our Trusted Experience Platform™ provides everything you need to secure your workforce, customers, and partners at a price that works with your budget. To learn more, visit https://www.onelogin.com/