7 Reasons Why Single Sign-On is a Must For Remote Working

my1login

Connecting People, Apps & Devices

Set against the backdrop of an increase in remote working, the continuing trend of moving to the cloud is making identity the fundamental security control in the new perimeter-less corporate world. To protect themselves, enterprise organisations are moving away from perimeter defence models, towards a focus on protection of data wherever it resides.

The migration to the cloud for apps and infrastructure necessitates that corporate security no longer focuses on its internal network boundary. As the march to the cloud continues, the resulting sprawl of corporate user identities and user credentials is causing password fatigue, complacency from users and putting business security at risk.

Verizon's Data Breach Investigations Report found that 81% of hacking-related data breaches leveraged either stolen, weak, or default passwords. This sheer scale of this attack vector is putting identity firmly at the heart of data breach risk. Identity sprawl and outdated password policies that expect end-user self-policing and rely on their ability to create strong, unique passwords and maintain best practices every day are leaving organisations exposed.

With a perimeter-less corporate environment, a workforce not contained to a physical location, and a myriad of devices being used to access corporate resources, managing corporate security is complex and difficult. The increasing number of employees working remotely is exacerbating these security challenges that already exist.

When considering Single Sign-On (SSO) as a solution that supports the organisational move towards a zero-trust model, it's crucial to believe in the fundamental tenet that if a user needs to remember more than one set of corporate login credentials, then they don't have Single Sign-On.

30 to 60 Seconds

The time it takes the average business user to log into a single application.

1.
Enablement & Productivity

We trust our employees to deliver their objectives regardless of where they are, but when it comes to accessing corporate resources, genuine obstacles are in their way when working from home, remotely or on a non-corporate device.

Single Sign-On provides seamless, managed access for all users to their most critical applications and resources from any device or location. Giving easy access to these applications means they have the tools to do their job, regardless of where they are or what device they're logging in from. There is no need for users to remember or manage passwords, removing the typical issues associated with remote workers having trouble accessing apps without the aid of IT. Productivity is improved through no more forgotten passwords and eliminating the downtime while these are reset.

With the average login time taking 30 to 60 seconds (or longer for less IT-literate users) to find and launch an application then find and correctly type a username and password, removing this stumbling block has significant productivity benefits for the business when a typical user uses at least 10 apps. The benefits lie, not only with the employee, but also the IT team and service desk who look after them – they no longer have to firefight forgotten passwords or permission issues. Employee access to corporate applications and resources can be linked directly to the corporate directory (e.g. Active Directory), meaning quick and easy provisioning and revocation of access to ensure the right people have access to the right applications and data at the right time.

While there is already a growing number of cloud apps being used in enterprise, a move to remote working will increase this number of applications and the frequency of their use. Video and audio-conferencing tools such as Zoom, GoToMeeting, Microsoft Teams, Hangouts and Cisco WebEx are more widely used when remote working. Document collaboration tools such as Dropbox, Box, O365 and G-Suite and IM tools such as Slack, Workplace or Hangouts are increasingly essential. Single Sign-On can ensure users have seamless, and secure, access to all of these apps without having to manage passwords for them.

An SSO solution that is not critically dependent on complex connectors with target applications can provide significant future-proofing.

2.
Protecting The Business From Unsecure End-User Behaviours

Providing access to corporate apps and resources is key to enabling business as usual with a remote workforce, however the cyber security risk of doing so is what will occupy the mind of senior IT and security officers. How exactly does an organisation ensure a remote workforce isn't putting the business at risk?

Single Sign-On is not a panacea, but it does solve a significant number of security issues at the same time as providing seamless access to applications. Centralised SSO enables organisations to ensure, first and foremost, that the right users have access to the right applications and data, essential when users are out of line of sight of IT. Furthermore, it removes the need for users to actually manage passwords – no more manually creating weak passwords or using insecure practices to remember them. With 81% of hacking-related data breaches being caused by either stolen, weak, or default passwords, that is a significant attack surface that Single Sign-On protects against.

Where the application supports it, passwords can be removed altogether, replacing credential-based authentication with token-based, e.g. SAML. This removes the need for passwords and the associated risks altogether. Where applications do not support these new protocols; strong, unique passwords can be automatically generated by more advanced Single Sign-On systems, enforced on the 3rd party applications and hidden from the user to reduce risk.

Ultimately, users can access their critical apps, but not be in a position to put the company at risk by using weak passwords or storing or sharing these credentials in unsecure ways. Where passwords legitimately need to be shared – company social media accounts for example – this can be done by the Single Sign-On solution (where it includes Enterprise Password Management functionality) ensuring this is performed securely and without disclosing the actual passwords to the users, or anyone in between.

Users gain access to the apps they need, and the SSO takes care of the access management. SSO can also give the IT team an audit trail of which users were using shared credentials assisting any investogations following an incident. The login event may have been with a shared set of credentials, but an audit trail within the SSO solution can identify which end user executed the login event with those credentials ensuring non-repudiation of access.

SSO also provides IT teams with the management information on which applications are being accessed by which users with data collected on a large number of factors including IP, time of day, and location.

Additionally, the strength of passwords used to protect applications can be determined and password changes enforced automatically on 3rd party applications, even where users are using non-corporate devices or are outside of the company network.

With users out of the line of site of IT, shadow IT - which is already thriving in most organisations - becomes more likely. Where your SSO solution has an application discovery feature, it can detect the apps being logged into, and enable IT to easily include or exclude these apps from SSO integration with the identity management solution. Based on My1Login customer data, enterprises found that they have 10 to 15 times more corporate apps in use than estimated – reinforcing that Shadow IT is an unknown quantity for many organisations and putting organisations at risk of being unable to protect what they don't know.

Online criminals adapt quickly to leverage stories in the headlines for new phishing campaigns that harvest credentials. Credentials compromised in this way often give the attacker a wider access to corporate resources as they masquerade as a legitimate user. While user education and threat detection are often the first port of call to mitigate the risk, leveraging Single Sign-On combined with an effective Enterprise Password Management solution that replaces or hides passwords can help eliminate phishing from the business altogether. If users don't know any passwords, how can they be phished of them?

Single Sign-On can also help centrally manage Multi-Factor Authentication (MFA), a must for remote workers by enabling MFA policies to be configured at a per application level or be invoked at the point of accessing the Single Sign-On solution itself. Additionally, data relating to login events can typically be exported or automatically linked to the customer's Security Information and Event Management (SIEM) solution, bringing all security intelligence together and providing the necessary insights to enable alerts and controls as necessary.

Organisations have 10 to 15 times more corprate apps in use than they estimate

3.
Reducing IT Administration For Joiners & Leavers

User account lifecycle management driven by onboarding and offboarding employees remotely is a growing consideration. For onboarding, SSO that supports the ability to create policies that control the provisioning of user accounts on 3rd party applications (e.g. using SAML) can streamline this process, providing quick access to the applications needed by a user on day one in the job. User access to specific applications can be linked to the user's group membership within the enterprise's existing directory structure (e.g. Active Directory) creating group-driven policies that enable Just-in-Time provisioning of user accounts on 3rd party applications, taking the administrative effort out of provisioning users on these apps. At a time when IT teams are fighting for budget and resource, freeing up this administrative overhead is a significant benefit.

With SSO, should an employee take an extended leave of absence, then ITs suspension of their Active Directory login can automatically suspend their ability to access their corporate applications, reducing effort at the same time as improving security. Should an employee leave the business, ceasing their corporate directory account will result in a revocation of their application access via the SSO solution automatically. SSO that includes Enterprise Password Management functionality also protects against the risk of employees leaving the business without divulging administrative credentials for critical systems as the Enterprise Password Manager enables these to be retained and accessed after exit.

4.
Ensuring The Business Remains In Control of Identities

The increasing number of attack vectors and the growing number of applications in use present a significant threat with a remote workforce that are out of line of sight from IT. Well intentioned, but blissfully ignorant users are putting businesses at risk all across the UK with often unintentionally lax security practices. This is why many forward-thinking organisations are moving towards a zero-trust security model, although historically this has often been aspirational due to overly complex and costly solutions. Technological advances in recent years makes this more of a reality, more so now Single Sign-On is capable of integrating with all application types from web to legacy Windows desktop.

With modern SSO and Enterprise Password Management solutions, enterprises can effectively enforce strong password policies, without having to rely on end-user discipline and self-policing. Single Sign-On and Enterprise Password Management removes reliance on end users, enabling the organisation to move towards zero trust by removing the ability of a user to put the business at risk. Simply, users are provisioned and provided with access to the apps they need, without the requirement to manage passwords or access. Should an employee leave, revocation of access to all apps can take place centrally and immediately to mitigate any risk.

Additionally, single threading on key individuals has always been a risk in many organisations with highly sensitive application and resource access that is restricted to a small number of individuals. SSO mitigates the risk, by enabling the business to always retain control over administrative credentials the control access to critical applications, without the risk of these being retained by departing employees. With an SSO solution that includes Enterprise Password Management functionality the business will never be in a position that should someone leave, the business is unable to regain access to specific applications. SSO removes the burden from the end-user and puts the business firmly back in control of identities.

5.
Audit & Compliance

Though a workforce may be working remotely, Single Sign-On enables IT and security teams to audit user access, providing effective governance over which users accessed what applications and when, enabling a centralised, granular audit trail over access to systems and data. Where login credentials are shared with specific users or teams (i.e. procurement accessing a supplier portal, marketing accessing the corporate social media accounts) using the Enterprise Password Manager, and a number of users have access to the application, the solution can provide an audit trail of which corporate user actually accessed the application using the shared credentials.

The audit logs can typically be integrated with the company SIEM solution to provide reporting and intelligence on user access and enable a response to any security incident. SSO and Enterprise Password Management also provides the necessary controls around access to data to help meet the strict audit and compliance obligations of the General Data Protection Regulation (GDPR), negating the challenges of whether users are within the corporate network or working remotely outside of it.

6.
Cost Savings

Reducing unnecessary costs is an ongoing exercise for all organisations, however it's often difficult to track software utilisation and just how effective the software is at releasing value into the business. Single Sign-On gives an organisation a centralised audit trail of application access by users. Some SSO solutions can provide additional management information that enables the enterprise to monitor and then rationalise software licence usage – either by identifying and removing subscription and licences that aren't used or monitoring concurrent licences so that secure sharing of credentials can be implemented where permitted by the software vendor.

Industry data puts the average end-user with the need to manage around 10 corporate passwords. Multiplied across the organisation, it's little surprise that many IT teams and service desks are busy with password related issues, especially after holiday season. Single Sign-On removes the need for employees to remember or manage any application passwords, whether they be cloud apps or internal legacy apps that IT and service desks are required to reset passwords for.

7.
Future Preparedness

While home working became an immediate priority for an unprecedented number of organisations in 2020, the benefits to the business, the employee and the planet are there for all to see. Businesses save money through reduced office space, the carbon footprint is hugely reduced with minimal commuting, and the employee can benefit from an improved work-life balance.

Putting in place the proper governance and measures to manage remote workers now, puts the business in a position to deal with the growing demand in the future. Single Sign-On is not a panacea for all business risk, but it offers ease of use, productivity, security, flexibility and cost benefits as organisations digitally transform with a move to the cloud set against a backdrop of a growing number of remote workers.

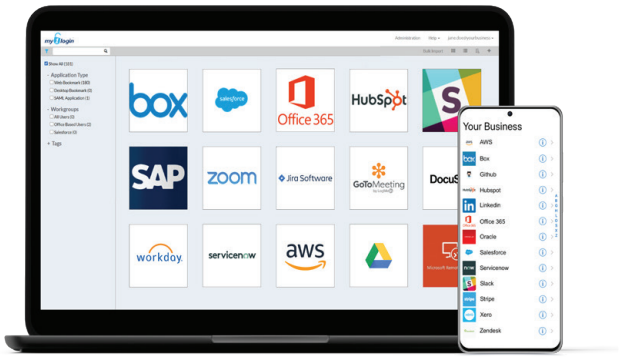
About My1Login

Founded in 2007, My1Login is a leader in Identity Management, protecting enterprises against cyber security threats through its Identity & Access Management (IAM) solution.

My1Login solves the problem of cyber-security risks created by the increasing sprawl of corporate user identities, usernames, and passwords by providing Single Sign-On for all web and Windows desktop applications that is seamlessly linked to the user's directory login.

My1Login's IAM solution removes the burden of passwords from users and puts the organisation back in control of security by enabling enterprises to transition from password-based to passwordless authentication. It centralises control of passwords, making processes such as onboarding and offboarding more secure and efficient. My1Login's auto-detection of applications being accessed further reduces the attack surface by identifying Shadow IT risks.

My1Login is the UK's most secure, most widely-compatible Identity & Access Management solution that enables organisations to mitigate password-related cyber-security risks, control user identities and help meet critical compliance obligations.



10,000+ Apps

In addition to working with today's enterprise cloud apps, My1Login also works with Windows desktop apps and mainframes, including IBM and Unisys, and integrates with virtualised apps such as XenDesktop, XenApp & Storefront.

Securely manage access to *every* application for *all* users from *any* device

SC 2020 awards EUROPE Winner

2017 · 2018 · 2019 Computing Security Awards WINNER

computing Security Excellence Awards 2018 Winner

HAVE A QUESTION? SPEAK TO OUR IDENTITY EXPERTS

Call
0800 044 3091

Email
contact@my1login.com

Visit
www.my1login.com

My1Login Limited, 207 Regent Street, London, W1B 3HH