



7 REASONS WHY SINGLE SIGN-ON IS A MUST FOR REMOTE WORKING



Connecting People, Apps and Devices

7 REASONS WHY SSO IS A MUST FOR REMOTE WORKING

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 Identity sprawl and outdated password policies that expect end-user self-policing and rely on their ability to create strong, unique passwords and maintain best practices every day are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 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 to find and correctly type a username and password per login (or longer for less IT-literate users) 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 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 deprovisioning 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 INSECURE 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 and not disclosed to the user.

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

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 insecurely. 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 Privileged Password Management functionality) ensuring this is done 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 intelligence on which users are using shared passwords at the time of any incident. The login event may have been with a shared set of credentials, but an audit trail within the SSO solution can identify which domain user executed the login event with those credentials.

SSO also provides IT teams with the intelligence 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 change enforced, even where users are using non-corporate devices or are outside of the company network. Should a company make a corporate decision not to use a specific application, Zoom for example, this can be detected by the IT team via the SSO solution, enabling action to be taken by IT.

With users out of the line of site of IT, shadow IT - which is already thriving in most organisations - becomes more likely. Where the SSO solution has an app discovery feature, it can detect what apps are being logged into, and enable IT to easily include or exclude these apps. Based on My1Login customer data, organisations have 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 to 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 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. MFA can be set at a per app level or be enacted at the point of accessing the Single Sign-On solution itself. Additionally, data relating to login events can typically be exported into the organisation's Security Information and Event Management (SIEM) solution, bringing all management intelligence together to provide the necessary insights to enable additional security controls to be put in place where necessary.

3. REDUCING IT ADMINISTRATION FOR JOINERS & LEAVERS

Onboarding and offboarding employees remotely is a growing consideration. For onboarding, SSO can streamline this process, providing quick access to the applications needed by a user on day one in the job. SSO can be linked to the company's existing directory structure (e.g. Active Directory) with group-driven policies to enable Just-in-Time provisioning to take the administrative effort out of provisioning users on 3rd party applications. 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, removing their AD access will result in a revocation of their application access automatically, without the need for action to be take in multiple locations. SSO with Privileged Password Management functionality also ensures that ownership of critical applications access can be retained by IT, ensuring that there is never a situation where access to an application is denied to IT by a leaving user, or in fact, a disgruntled user.

SSO can help further reduce IT administration by removing the need for IT to perform password resets on behalf of users. Self-service password reset is a feature of some Single Sign-On solutions and can remove the burden on the IT team.

4. ENSURING THE BUSINESS REMAINS IN CONTROL

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.

Now organisations do not have to rely on end-user self-policing and their ability to create strong, unique passwords and maintain best practices every day. Single Sign-On with Privileged Password Management removes user reliance, 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 sensitive apps, without the risk of these only ever being known to select end-users. With an SSO solution that includes Privileged Password Management functionality the business will never be in a position that should someone leave, the business itself 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 its application estate.



5. AUDIT AND COMPLIANCE

Though a workforce may be working remotely, Single Sign-On enables IT and security teams to track user access, providing effective governance over which users have access to what applications and when, enabling a centralised, granular audit trail to systems and data. Where login credentials are shared, and a number of users have access to the application, SSO can provide intelligence on which corporate user actually accessed the application with those shared credentials.

SSO application access 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 event. SSO 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 source of truth on application access and enables tracking of which users are logging into which apps. Some SSO solutions can provide additional management intelligence that enables an organisation to monitor and then rationalise software licence usage – either from identifying and removing licences that aren't used or monitoring concurrent licences so that licence sharing can be implemented where allowed by the software vendor.

Industry data puts the average end-user with the need to manage around 10 applications. Multiplied across the organisation, it's little surprise that many IT teams are busy with password resets, 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 are required to reset passwords for. Additionally, some SSO solutions have self-service password reset functionality for the directory login, removing this IT overhead and allowing for IT administration costs to be reduced.

7. FUTURE PREPAREDNESS

While home working has been 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.

There is no doubt that home working will form a greater part of every business norm from 2020 onwards. 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.



Industry data puts the average end-user with the need to manage access to around 10 applications.

About My1Login

Founded in 2007, My1Login has been cited as a Global Leader in Identity Management by CB Insights, protecting enterprise cyber security threats through its Identity and Access Management solutions.



My1Login's award-winning IAM solution solves the problem of weak passwords and practices, enabling organisations to control user access and centralise identity through Single Sign-On. Critical applications can be protected by auto-generated, strong, unique passwords that can be hidden from users, eliminating phishing. My1Login's auto-detection of application usage further reduces the attack surface by removing the blindspots created by Shadow IT.

My1Login is the UK's most secure, most widely-compatible, award-winning Enterprise IAM solution that enables organisations to mitigate password-related cyber-security risks, strengthen identity assurance and help meet critical compliance obligations such as GDPR.



10,000+ Apps

In addition to working with today's enterprise cloud apps, My1Login also works with legacy, thick-client apps, including IBM and Unisys mainframes, and virtualised applications such as Citrix.

Accreditations And Certifications



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

HAVE A QUESTION? SPEAK TO OUR IDENTITY EXPERTS



Call

0800 044 3091



Email

contact@my1login.



Visit

www.my1login.com



Reference

Gartner

My1Login Limited, 324 Regent Street, London, W1B 3HH

© My1Login. All rights reserved.