my1login

Connecting People, Apps & Devices

Award-Winning
Identity & Access Management

Computing Security Awards
WINNER

Challenges Facing CIOs Today

The trend towards SaaS is moving enterprise identities outside the traditional corporate infrastructure, creating a new set of identity challenges and exacerbating those that have always existed.

Insider Threat & Phishing

Verizon's Data Breach Investigations Report found 81% of hacking-related breaches involved weak or stolen passwords. Verizon's analysis of 1,600 cyber security incidents and 800 breaches found that phishing was involved in 90% of successful attacks. Whether malicious, or simply blissfully ignorant, employees are putting the business at risk by using weak passwords, storing them insecurely or being phished.

Password Fatigue

The trend towards cloud services has increased the number of logins that end-users have to remember and manage. Often these don't integrate with the corporate directory or existing Single Sign-On (SSO) solutions. The sheer volume of usernames and passwords end-users have to remember reduces productivity, increases downtime and creates unnecessary security risks.

Architectural Complexity

Organisations are now having to manage a disparate number of web, Windows and virtualized applications across public and private cloud infrastructures. Many of these apps do not integrate with the corporate user directory.

Escalating Password Reset Costs & Downtime

The increasing number of passwords end-users have to remember is resulting in a rise in IT helpdesk calls to reset forgotten passwords. Gartner report that password-related calls represent 20-50% of the IT helpdesk workload.

Compliance Obligations

Organisations are faced with meeting a range of compliance obligations that includes ISO, PCI and GDPR. Central to much of this is the need for control and governance over access to systems, data and applications in order to ensure only the 'right' people have access to the 'right' information. Effective authentication management across business systems is therefore required to mitigate the risk of malicious and unauthorised access and to enable governance and audit over access to data.

UK companies are also increasingly concerned about hosting data outside of the UK and over the use of US-headquartered SaaS vendors where access to their data can fall under the sovereign-right of a foreign nation.

Shadow IT & Control of User Access

The adoption of cloud applications outside of IT's knowledge creates significant challenges around identity governance, information security and control of access. With no centralised control over user access to apps and the increasing number of end-user devices, ex-employees often retain access to applications once they leave the organisation.

Return On Investment

Automated provisioning, SSO, Multi-Factor Authentication (MFA), secure user management and reporting are all prerequisites of any good Identity and Access Management (IAM) solution. However, in order to truly deliver the intended ROI it must work with all applications. My1Login enables an organisation to:

Eliminate Helpdesk Calls
20-50% of helpdesk calls are reported to be password related (Gartner).

Eliminate User Downtime
Save up to 30 minutes of time wasted by users for each password reset.

Eliminate Time Logging Into Apps
Free up to 10 minutes per day that users waste logging into applications.

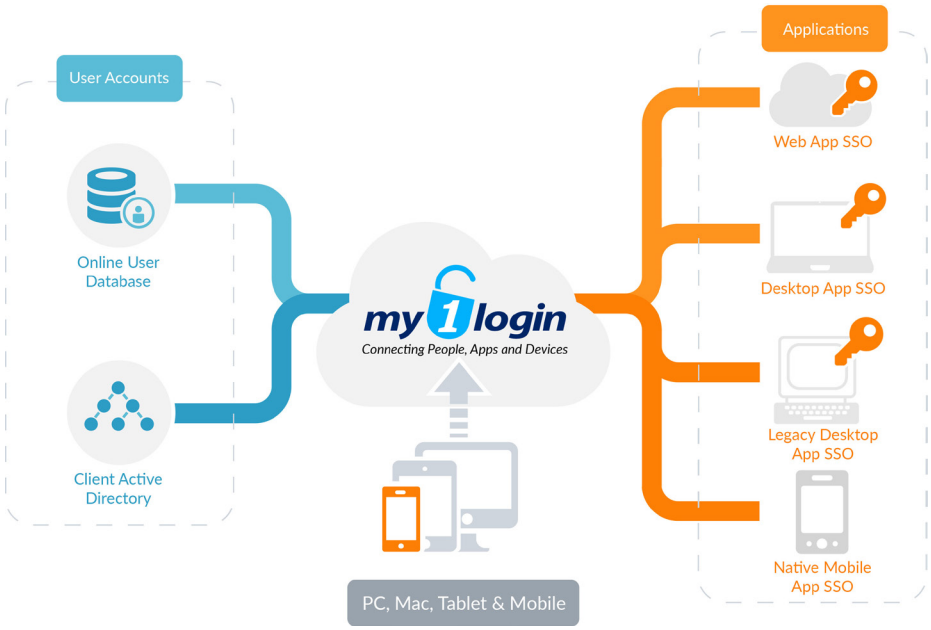
Eliminate Unused Software Licences
Application usage reports enable the software licence pool to be reduced.

Five IAM Vendor Questions That Will Maximise ROI

1. Does the IAM solution use client-side encryption where the vendor has no access to the encryption keys?
2. Can the solution automatically discover web apps being used by end users?
3. Can the solution alert IT of discovered apps and automatically integrate them with SSO if required?
4. Can the solution integrate with Windows desktop applications that only support password authentication?
5. Can the IAM solution eliminate phishing by automatically updating users' passwords for apps and hiding them from the user?

Why My1Login?

- Wholly UK-based Identity Provider with UK Data Storage
- Uses Proprietary, Patented Technology to Automatically Discover Web Apps Being Accessed
- Alerts IT of “Shadow-IT” Being Accessed by Users
- Can Automatically Integrate New Web Apps With SSO
- Enables SSO for Windows Desktop Apps That Only Support Password Authentication
- Client-Side Encryption, My1Login has no Access to Keys
- Can Automatically Update Users’ Passwords For Web and Windows Desktop Apps in Line With Policies
- In addition to Windows & OS X, My1Login also integrates with Citrix XenDesktop, XenApp & StoreFront
- Eliminates Phishing, Insecure Passwords and Shadow IT
- Satisfies Compliance Obligations i.e. GDPR



IAM Products

SSO for Web & Mobile Apps

- Integrates Target Apps with Connectors (e.g. SAML)
- Integrates Target Apps Without Connectors
- Auto-Detects and Auto-Integrates Web Apps
- Active Directory Integration
- Citrix Compatible
- SSO Without Revealing Credentials
- AD and External Users

SSO for Windows Desktop Apps

- Integrates Windows Desktop Apps without connectors (Password Vaulting & Forwarding)
- Auto-Integrates Users’ App Credentials
- Active Directory Integration
- Citrix & Mainframe Compatible
- SSO Without Revealing Credentials

Provisioning Engine

- Full Account Lifecycle Management
- Just-In-Time Provisioning of User Accounts on Target Apps
- AD Group-based Policies Can Automate User Account Provisioning

Multi-Factor Authentication

- Microsoft Authenticator
- Google Authenticator
- Duo
- Yubico Devices
- Universal Second Factor Device Compatible
- Other Integrations Available On Request

Privileged Password Manager

- Permission-based Sharing
- Automatic Secure Password Generation
- Automatic Password Updates on Target Applications
- SSO without Revealing Credentials
- App Specific Password Policies
- Temporal (Time bound) Access to Privileged Passwords

Self-service Password Reset

- AD Self-service Password Reset
- Reset From Mobile, Web Portal and Windows Desktop
- Configurable Challenge Response

About My1Login

Founded in 2007, My1Login has been cited as a Global Leader in Identity Management by CB Insights, protecting enterprises against cyber security threats through its Identity & Access Management solution.

My1Login's multi-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 and Privileged Password Management. 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 blind spots created by Shadow IT.

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 such as GDPR.

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.

Accreditations And Certifications

HM Government G-Cloud Supplier

The UK Access Management Federation FOR EDUCATION AND RESEARCH

CYBER ESSENTIALS PLUS

CSA cloud security alliance®

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.com

Visit www.my1login.com

Reference Us Via Gartner

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