With the GDPR (General Data Protection Regulation) now in force, it’s never been more important for businesses to have a robust identity and access management (IAM) solution in place. The majority of data breaches are caused by compromised user credentials with weak or stolen passwords, so eliminating these risks is essential.

My1Login is an ideal solution, as this wholly UK-based provider offers an easily deployed IAM solution, comprising single sign-on (SSO), user account provisioning and privileged password management capabilities. It works with all applications across all devices and removes the need for multiple passwords.

Along with seamless Active Directory (AD) integration, My1Login delivers a wealth of valuable security features. These include application auto-discovery and identification of unknown web applications, allowing shadow IT to be effectively managed.

Deployment is swift, as My1Login is a cloud-based service, providing a management portal. The only local components that need to be installed are a lightweight AD connector agent and an optional browser helper extension.

Roll-out is equally fast, as AD Group Policy is used to push settings to end users. My1Login offers two user experiences where the transparent mode takes over the authentication process entirely, so there is no change in user behaviour required. The user launches an app and is then automatically authenticated with credentials or SAML. The user neither knows, nor needs to know, any of their credentials.

The non-transparent mode passes AD authenticated users to a personal web portal, which presents all permitted apps. Click on an app icon and My1Login auto-fills the user’s credentials and authenticates them.

My1Login supports SAML-based authentication to web services such as Amazon Web Services and SalesForce. The user experience is no different, as they select the app from their portal and authentication is handled for them.

My1Login can also provide SSO into a thick client app installed on the user’s Windows desktop. When an app is launched, My1Login detects the user has an identity for it and automatically logs them in.

All login processes take seconds and require virtually no training, allowing My1Login to deliver a high adoption rate. Security is also very tight, as My1Login uses client-side encryption; so, unlike some other SSO providers, the encryption keys are known only to the customer.

The administrative portal provides full access to all features, including privileged password management. This allows security officers to provide swift access to apps on an ad-hoc basis, without users knowing the passwords.

Temporal access is a powerful feature, as it permits usage between specific time periods and it can be rescinded on demand where the app simply disappears from the user’s portal.

Remove a user from AD and My1Login automatically propagates the changes and denies access to all apps. This takes seconds to achieve, so staff departing the company could have all access blocked before they’ve even left the car park.

Auto-discovery lists unauthorised apps in the admin portal, alerts IT staff and asks if they want to integrate these with SSO. Moving them to the inclusion list allows My1Login to detect user credentials, highlight those that are weak and enforce strong passwords.

Detailed audit trails show which apps were accessed, who used them and when. Reporting features also include app licence utilisation details, allowing businesses to rationalise usage and save on costs.

My1Login is a true SSO solution that is remarkably easy to deploy and integrates seamlessly with a vast range of apps. It enables organisations to mitigate password-related security risks, control user identities and also meet critical compliance obligations.

Product: My1Login Enterprise IAM
Supplier: My1Login
Web site: www.my1login.com
Tel: 0800 044 3091
Sales: sales@my1login.com

www.computingsecurity.co.uk  @CSMagAndAwards  July/August 2018  computing security