Case Study

Cogito Group

All-In-One IdAM Solution

The Client Need

Our client wanted to ensure appropriate access to resources across increasingly heterogeneous technology environments. The goal was to improve security, manage access for internal users and provide simple and secure self-service access to consumers of our client's products and services.

The Challenge

Access control is ultimately the 'gateway' through which all access—authorised and unauthorised—to information and assets must pass. This can also be one of the most challenging business initiatives to address as it is also the area of information security with the most direct inter-relationship with end-users.

As services are trending towards the cloud, our client was finding it difficult to maintain control over the access to these services for their internal users and facilitate timely and controlled access to their external users. Multiple logins were a problem.

What was needed was an innovative solution that provided a secure, stable and scalable identity management platform delivering a great user experience. Importantly the solution needed to support the end-to-end lifecycle of user access, be cost effective and able to be implemented quickly and efficiently with little impact on existing resources.

The Client Solution

ForgeRock OpenAM solution, to provide IdAM services for the web, cloud and mobile devices, in a highly scalable, modular and easy to deploy architecture.

- Federation with Office365.
- Availability and Performance.
- Future Proof.
- Security.
- Standards-compliant.
- Multi-factor Authentication.
- Extensibility.
- Single Sign-On.

All-In-One IdAM Solution

Case Study

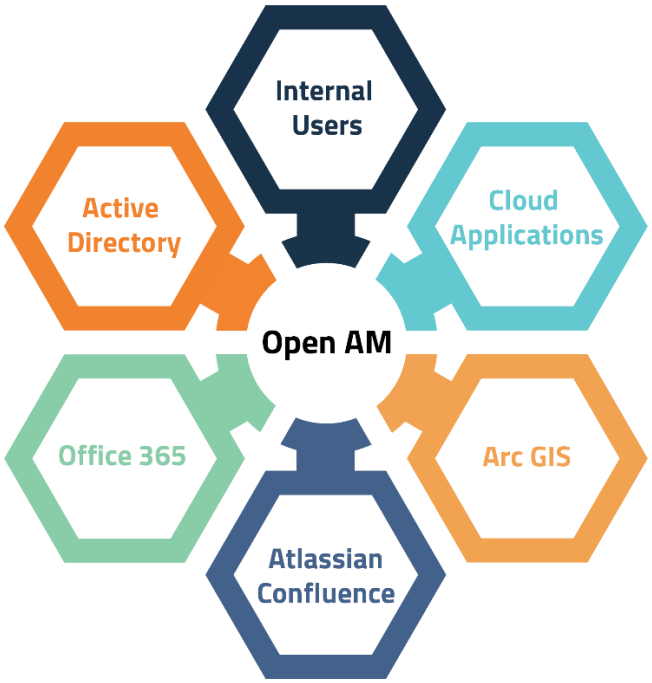

Figure 1: ForgeRock OpenAM Solution

The Software Solution: ForgeRock OpenAM

ForgeRock OpenAM has a highly scalable, modular, easy-to-deploy architecture that includes:

- Authentication based on dynamic, context-based access that is responsive to user location, time zone, device, IP address, time of day, and more, providing endless personalisation possibilities and mitigation of risk.
- Entitlement management that enables users to access applications and services based on permissions and policies defined by the business without creating complexity using embedded policy engine tools.
- Federation and single sign-on with a single identity, allowing users to access services that span the cloud and mobile devices, on premises and off, eliminating the need for multiple passwords, user profiles, or the complexity that creates friction and slows adoption.
- Social sign-on that supports integration with "sign up and log in with Facebook"-style access, which eliminates the need for user registration and allow rapid consumer adoption.
- Adaptive risk that combines contextual information to evaluate the risk of users attempting to access resources, and, if they are deemed suspicious, require a higher level of authentication or identity-proofing.

Outcome

Our client's users now have the capability to have a single identity allowing them to access services that span the cloud and mobile devices, on premises and off, reducing the need for multiple passwords user profiles or the complexity that creates friction and slows adoption.

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.