The client needed to move its business partners' portal from a heavily customized legacy platform, including such disparate tools as CA SiteMinder, RSA adaptive risk authentication, and HID two-factor authentication, to a more flexible and scalable architecture. This required a review of the custom authentication schemes, authorization models, password policies, and user experience. It also meant defining a solution using ForgeRock and designing it for short-term co-existence with the existing solution, as well as the migration of protected applications to the new ForgeRock-based solution.

We took a phased approach for both feature and application migration to allow for enhanced user experience and reduce risk and maintain high availability.

- First, we developed a co-existence model where ForgeRock and the existing access management components worked in tandem. The existing solution continued to be the primary authentication solution (IdP), while a few applications were fully migrated to ForgeRock (SP). Federation was established between the two access management solutions for seamless user sessions and to address other access management functions. We also developed custom authentication modules in both platforms to create user sessions based on a valid token in either of the access management platforms, regardless of point of entry.
- We then developed authorization policies in ForgeRock to replace a legacy solution that relied on LDAP for authorization checks (outside SiteMinder). We also developed a process to automatically create and manage authorization policies via RESTful call from the identity management system when applications are onboarded (or when business rules change).
- PwC developed a custom authentication module, replacing a heavily customized and legacy impersonation module (vendor provided) in SiteMinder, allowing business partners to switch between multiple personas seamlessly.
- We developed integration with ForgeRock authenticator to support multi-factor authentication for access to critical applications.
- PwC developed an adaptive authentication solution in ForgeRock (to replace RSA) to challenge users to step-up the authentication based on defined risk factors.
- We also developed a solution to migrate password policies, which are rigidly coupled with SiteMinder, to more flexible LDAP-based policies.
- Finally, we developed a reverse co-existence and cut-over plan to completely turn off SiteMinder, RSA, and HID when all applications were fully migrated into the ForgeRock platform.

Our solution

- Our client was able to consolidate their business partner access management portal into a single technology and sunset legacy solutions like SiteMinder, RSA, and HID. This resulted in significant savings in terms of licensing and platform maintenance.
- The client was also able to cut down the services cost to CA for maintaining several vendor-developed customizations (specifically developed for the client).
- The solution resolved several high and critical security vulnerabilities that were not addressable in the legacy solution.
- Our solution achieved a zero downtime requirement from the business via the ForgeRock Active-Active architecture for applications across multiple data centers; SSO is established even if a user tries to navigate from an application hosted in a data center to an application hosted in another data center.
- The solution resulted in zero impact to end-users, including any change in user experience or need to change password or security questions.

Key contacts: Alex Coassin, Rajesh Prabhu

Can be used as reference: Yes
Reference contact details: Request information from key contact.