

Case Study:

Centralized Identity Access Management with Azure Active Directory

Law firm leverages Azure AD to increase security posture and protect business-critical data and applications without disrupting user productivity.

CHALLENGE

An Am Law 200 law firm client was providing their employees and network users with access to more than one hundred SaaS applications. While some of these applications had been previously configured for Security Assertion Markup Language (SAML) authentication to their identity provider, Active Directory Federation Services (ADFS), others were using local account management. As part of their cloud-first initiative, our client wanted to move away from managing their on-premises ADFS environment. They aimed to leverage Azure AD as the new Identity Provider, which was already synchronized with Azure AD Connect. Additionally, our client hoped to leverage security features like Conditional Access in Azure AD.

SOLUTION

Canalini Consulting Group developed a migration plan to move the client's SaaS applications from ADFS to Azure AD. Canalini also configured SAML authentication for the additional SaaS applications that had been set up with identities local to those systems. Working alongside the client's internal IT team, Canalini delivered the following capabilities:

- Provided security controls at the Identity Provider layer to all SaaS applications
- Centralized management of Identity and Access to applications
- Configured Office Portal Access to all SaaS applications

RESULTS

- All SaaS applications along with other remote access services like VPN and Citrix were reconfigured with Enterprise Applications in Azure AD with their respective SAML configuration.
- Canalini overlaid existing Conditional Access policies and additional security controls that were previously unavailable with ADFS and native SaaS providers. This included requiring Multi-Factor Authentication for all users.
- Identity to Azure AD centralization eliminated the need to access multiple systems for user onboarding, password changes, and security controls.
- Identity Platform management was offloaded from on-premises to the Microsoft Cloud.



IDENTITY ACCESS MANAGEMENT

Centralized the identity platform for all applications to a single Identity Provider



SECURITY

Added security features and enhanced the consistency of security posture across all SaaS applications



CLOUD MIGRATION

Consolidated identity providers to a single Cloud-hosted Identity and Access Solution