CANALINI
CONSULTING GROUP

Case Study:

Enhanced Security and Compliance with Microsoft Azure GCC High

Federal client leverages Azure GCC High to meet compliance, security and access requirements.

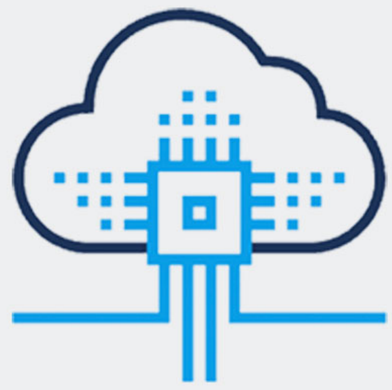
CHALLENGE

A federal client was managing multiple technologies on-premises including messaging, identity, files, remote access, and MDM/MAM. The client determined that they required a technology refresh and a migration from on-premises services to a secure cloud platform that met federal regulations for compliance and cybersecurity. The client hoped to consolidate identity, implement multi-factor authentication for all users and offload infrastructure management from the internal IT team. Finally, the client aimed to provide a remote access solution built on ZTNA technology for users working outside of on-site offices.

SOLUTION

Canalini Consulting Group determined that Microsoft Azure GCC High was the ideal platform to not only meet the organization's requirements, but also to enable the consolidation of multiple existing technologies into a single, streamlined platform. Canalini worked with the client to provide end-to-end security with hardware-level MFA and streamlined user experience with single sign-on capabilities that leveraged Azure AD. Canalini delivered the following capabilities:

- Synchronization of identity from on-premises Active Directory to Azure AD
- Migration of messaging from on-premises Exchange to Exchange Online while also providing S/MIME capabilities
- Migration of mobile device management from Citrix XenMobile to Microsoft Intune
- Migration of Unified Communications from Skype for Business on-premises to Microsoft Teams
- Migration of on-premises file shares to Microsoft OneDrive with Known Folder Move (KFM)
- Remote access to the environment was previously provided with a Cisco AnyConnect VPN solution. Zscaler Private Access (ZPA) was deployed to segmentation at the application level instead of providing full network access.



CONSOLIDATION & MIGRATION

Consolidated technologies and services from multiple vendors running in an on-premises datacenter to running within the Azure GCC High tenant.

SECURITY

Strengthened security posture by leveraging multi-factor authentication with a hardware token, Azure GCC High authentication and authorization control requirements.

CLOUD BASED. CLIENT FOCUSED.

RESULTS

- All data was migrated securely and stored on a FedRAMP cloud platform that required security controls for user and device access to data and applications.
- Email was migrated to Exchange Online while also adding support for S/MIME encryption.
- Desktops, Laptops and Mobile devices were required to be managed with Hybrid Azure AD Join or Intune registration prior to accessing any corporate data.
- Hardware-based multi-factor authentication was enforced for device and application access while providing single sign-on capabilities. Furthermore, all remote access to data and applications leveraged a solution built on ZTNA architecture.
- Various technology vendors were consolidated to Microsoft Azure GCC High services to lower total cost of ownership by cutting hardware and software licensing costs.

REMOTE ACCESS

Provided authentication, authorization and access to applications and data running in Azure GCC High using a remote access solution built on ZTNA technology.

CLOUD BASED. CLIENT FOCUSED.