Enterprise Mobility + Security – Implementation

Cambay Consulting
Accelerating Digital Transformation

Microsoft Managed Partner

As COVID-19 continues to spread around the globe, millions of people have moved to remote work. Due to increasing remote work, employees access company data, applications, and other systems virtually from anywhere, any device.

Microsoft Enterprise Mobility + Security is the best choice to secure your enterprise data & apps without compromising user experience. EMS is intelligent mobility management and security platform.

Enterprise Mobility + Security (EMS) – Implementation, Adoption and Training

Cambay reviews your infrastructure post-knowledge of cloud infra along with your goals and expectations. Unlike many automated tests created to work on every cloud environment, Cambay's approach is backed by years of experience on projects analyzing diverse environments to help better address your needs and ensure that your enterprise assets are secure.

Cambay's professional services for EMS will assess, design, and implement the entire EMS suite for your organization.

Why Cambay

- Microsoft Managed Partner and Gold Competencies in Collaboration & Content and Cloud Productivity.
- Helping enterprises create digital experiences for employees that unite enterprises.
- Trusted digital workplace partner for several leading enterprises

EMS Implementation, Adoption and Training Scope

Identity & Access Management

- Deploy or validate Azure AD Connect for a single Active Directory (AD) domain.
- Enable modern authentication for a single Microsoft 365 tenant.
- License and provision users in a single Microsoft 365 tenant.
- Configure Azure AD P1 and EMS licensed users for a self-service portal.
- Configure sync of all supported modern workstations in a single AD domain.
- Enable seamless Single Sign-On (SSO) via Group Policy or Intune.
- Configure company branding.
- Create Azure AD groups to use for targeting policy configurations.

Conditional Access and MFA

- Enforce MFA for all the users accessing company data, email, and devices.
- Configure automated risk-based policies for Azure AD P2 users.

Microsoft Defender for Office 365

- Configure Anti-Phishing policies.
- Configure Anti-Spoofing policies.
- Configure Safe Links baseline policy.
- Configure Safe Attachments baseline policy.
- Configure Malware Detection baseline policy.

Mobile Device Management (MDM)

- Create a baseline MDM device compliance policy to include device encryption, data containerization, and device PIN lock.
- Create a baseline Mobile Application Management (MAM) Intune app policy to include data encryption, data containerization, and app PIN lock.
- Device enrollment training and Standard Operating Procedures (SOP).
- Setup device profiles, device management policies, conditional access policies, and application management.
- Publishing line of business applications.
- Blocking the use of native email applications.
- Policy testing on specific people from each department.

Workstation Management (Windows 10)

- Create a baseline Windows 10 device compliance policy.
- Create a baseline MacOS device compliance policy.
- Create a Windows 10 security baseline profile.
- Create a Microsoft Defender ATP Baseline profile.
- Configure OneDrive Known Folder Move policies for Windows 10.
- Remove Windows 10 consumer experience and uninstall bloatware.

Data Loss Prevention (DLP)

- Enable global Office 365 DLP Policies for Exchange Online for company's confidential information.
- Configure baseline Office Message Encryption templates for end-users.
- Configure retention policies.
- Enable Unified Labeling Experience.
- Configure Azure Information Protection Agent deployment via Intune.

Microsoft Defender for Identity

- Deploy the Advanced Threat Analytics (ATA) lightweight gateway on up to two domain controllers.
- Configure monitoring alerts.
- Integrate with Microsoft Defender ATP.
- Review of configured environment.
- Configure the Windows Defender Security Portal.
- Configure Microsoft Defender ATP Onboarding via Intune.
- Enable integration with Microsoft Cloud App Security.

Deliverables

- Device enrollment Standard Operating Procedures (SOP).
- Solution Architecture Document (SAD) for the solution.
- (8) Hours of training of IT staff for baseline configuration and customization.

Duration & Cost

- EMS Implementation – **10 Weeks**
- Cost - **US $20,000**