A leading IT services provider seamlessly deploys Microsoft EMS to enable secure enterprise mobility

Implements IT security posture, boosts enterprise productivity and enhances user experience

About the Client
The client is a leading IT services provider offering application architecture, development and management services across multiple verticals. With over USD 1 billion in revenues, the firm operates more than 30 offices in 19 countries with outsourcing centers in India, Sri Lanka, China, Australia, Japan, North America, and Europe.

Goals
Addressing unique data security and compliance requirements
The client was part of an acquisition exercise that resulted in it operating two distinct business units, one serving the parent company and another serving the other Lines of Business (LoB). This led to the emergence of three distinct types of users within the client’s internal IT environment - direct business channel, parent company business channel and non-India/other location users. Of the total number of 22,500 users that were covered by Microsoft Office 365 licenses, active mobile users comprised 10,000. The client faced three key challenges in enabling the following:

#1 Services that conformed to the requirements of their Compliance and Regulatory Officer: The company was looking to meet internal security compliance requirements with respect to its mobility offerings. For instance, parent company channel users were not allowed to download email attachments over their mobile devices, neither could they print/download from the document library.

#2 LoB mobile apps for enterprise needs: The client was working on a parallel project for developing mobile apps and needed a platform to push/deploy these apps without publishing them on the internet.

#3 Data security and protection in BYOD: Given the client’s distributed end-user environment and enablement of BYOD, it required a robust solution to safeguard business critical data from insider threats as well as external threats such as data leakage, malware or ransomware attacks.

The client’s existing messaging infrastructure was built on MS Exchange 2007, which could not serve all of the client’s diversified compliance needs, despite its ability to support conditional access. This meant users could download anything over their mobile devices, leading to heightened data security risks. Moreover, their MS Exchange 2007 environment server hardware license was due to expire soon. The client therefore decided to migrate to Microsoft Office 365 as well as setup Microsoft Enterprise Mobility Suite (EMS) to capitalize on its existing investments in the Microsoft suite of products, while enabling seamless enterprise mobility for all its end users.

The client was therefore looking for an experienced service partner to efficiently deploy the mobility solution in tight integration with other cloud based services, email, SharePoint, etc.

Microland
Delivering robust enterprise mobility solutions backed by best-in-class IT infrastructure services
Microland was chosen as the preferred partner to implement the mobility solution due to its proven expertise in implementing enterprise mobility solutions, Microsoft Office 365 services, and deep domain knowledge in end user technologies.

Microland is a valued Practice Development Unit (PDU) partner for Microsoft and is a Gold certified partner for Cloud Productivity and Enterprise Mobility Management. The company’s long and successful track record of providing best-in-class IT infrastructure services, backed by a suite of proprietary frameworks, tools and methodologies enables it to spearhead enterprises’ transformation - from a technology-led to a services-led business model.

Microland’s expertise with Microsoft technologies (such as Microsoft Intune, Azure Active Directory, Advanced Threat Analytics, and Cloud App Security) were instrumental in helping the client build a secure, user-friendly, and mobile-first end user computing environment.

Transformation
Adopting a phased approach for seamless mobile solution deployment
Microland deployed Microsoft EMS using a phased approach (see Figure 1). Over 10,000 mobile devices are currently enrolled under the solution.
Some of the areas covered as part of the engagement included:

**#1 Identity and access management (MS Azure AD):** The Microland team helped sync on-premises and cloud Office 365 applications for all users. Active Directory Federation Services (ADFS) claim rules were setup to achieve the necessary controls such as blocking of unsecured basic authentication, enforcement of the Intune managed browser as the default browser on all mobile devices, etc.

**#2 Azure rights management:** The initial assessment was followed up with Azure rights management configuration. Prior to the implementation of Microland solution, a narrow on-premise Windows Rights Management Services (RMS) solution existed that covered only the legal and HR departments. This provided limited compliance and data security, that too only for the data at rest. With Office 365, the entire user base of more than 22,500 users is now covered under Azure Rights Management, enabling end-to-end data protection for all MS office documents.

**#3 Mobile Application Provisioning:** The client wanted to publish their mobile apps and manage them in-house, rather than over the Internet. This was achieved using the MS Intune App Store, specific to the client's tenant. This, in turn, enabled automatic updates and push-based deployment to mobile devices, even for the client's internal LoB web-apps that were published as shortcuts.

**#4 Advanced Threat Analytics (ATA) and data security:** We deployed MS Advanced Threat Analytics solution - an on-premise solution that leverages analytics to monitor the network and user behavior to protect the business against malicious activity and attacks.

**#5 Change management & user adoption:** Our team of experts provided change management services, including reengineering of certain processes (such as employee departure) and internal marketing communications to drive adoption and usage of the new solutions. We also recommended that a set of policies, including mobile data wipe, be implemented on all end-user devices to prevent data breaches.
Outcomes

Seamless enterprise mobility for enhanced security and productivity

Microland’s solid expertise in EMM, Office 365 deployment, and proven technology integration methodologies enabled seamless migration and transformation of the client’s end user infrastructure, resulting in the following key benefits:

#1 Complete mobility with access control for enhanced productivity: The client gained complete control and holistic visibility into all its mobile device platforms including MDM, MAM, and MCM, enabling proactive monitoring and analysis as well as maximized uptime. All Office 365 services were enabled over secure mobile devices, enhancing user productivity.

#2 Improved data security: Significantly reduced risk of malicious attacks with an improved security posture, enabled by conditional access of Office 365 services. For instance, if a user logs in with a personal laptop, he/she can access information only through the IE browser and no downloads are permitted. Advanced Threat Analytics (ATA) protects the client against malicious user activity, penetration attacks, zero day attacks, etc.

#3 VPN cost savings and enhanced user experience: Prior to deploying Microland’s solution, the client extensively used VPN to provide access to the internal web apps for its various LoBs. Using Azure app proxy, which acts as a reverse proxy, the internal apps are now accessed over the internet, leading to significant VPN cost savings and superior user experience.

About Microland

Microland is a leading Hybrid IT service provider and a trusted partner to enterprises in their IT-as-a-Service journey. Headquartered in Bangalore, India, Microland has more than 3,700 professionals across its offices in Australia, Europe, India, Middle East & North America. Microland enables global enterprises become more agile and innovative through a comprehensive portfolio of services that addresses hybrid IT transformation, workspace, service and end-to-end IT management.