Wysetek Implements Workspace ONE UEM Solution for leading Oil Refinery Company

The Customer's Business

Workspace ONE UEM implemented by Wysetek to manage Device, Application, Email and Browser management for total 2500 Android and IOS devices.

It is a privately held downstream oil company based in India, that encompasses refining, marketing, production, and a network of over 6,000+ retail fuel outlets in India.

The Need for a Solution

The Company wanted to manage BYOD (personal devices) and corporate devices to secure and protect corporate data using workspace one UEM product.

Using workspace one UEM, Wysetek team deployed below components to manage company's data.

1. Secure email gateway – using this component we are managing and securing on premises exchange email using VMware boxer mobile applications.
2. Tunnel Gateway – using this component we are managing and securing intranet websites (VMware web browser) and application (corporate apps)
3. Content Gateway -- using this component we are managing and securing Network file server for end users devices using VMware content locker mobile application.

Wysetek has setup workspace one UEM console to manage android and IOS devices by enrolling using Intelligent hub client application.

Through Workspace one UEM we are publishing corporate and public application for android & IOS devices.

The Implementation

The implementation consisted of Workspace one UEM console, devices services, API, AWCM ON premises installation and Unified access Gateway appliance deployment and it has Tunnel, content and secure email gateway components.

Workspace ONE UEM is composed of separate services that can be installed on multiple-server architecture to meet security and load requirements. Service endpoints can be spread across different security zones, with those that require external, inbound access located in a DMZ and the administrative console located in a protected, internal network.

Syncing with internal resources such as Active Directory or a Certificate Authority can be achieved directly from the core components (Device Services and Admin Console) or using an AirWatch Cloud Connector. The separate connector can run within the LAN in outbound-only connection mode, meaning the connector receives no incoming connections from the DMZ.

The implementation is separated into the three main components:

1. Workspace ONE UEM Admin Console
2. Workspace ONE UEM Device Services

Component	Description
Workspace ONE UEM Console	Administration console for configuring policies within Workspace ONE UEM, to monitor and manage devices and the environment. This service is hosted in the cloud and is managed for you as a part of the SaaS offering.
Workspace ONE UEM Device Services	Services that communicate with managed devices. Workspace ONE UEM relies on this component for: • Device enrollment • Application provisioning • Delivering device commands and receiving device data • Hosting the Workspace ONE UEM self-service catalog This service is hosted in the cloud and is managed for you as a part of the SaaS offering.
API endpoint	Collection of RESTful APIs, provided by Workspace ONE UEM, that allows external programs to use the core product functionality by integrating the APIs with existing IT infrastructures and third-party applications. Workspace ONE APIs are also used by various Workspace ONE UEM services, such as Secure Email Gateway for interactions and data gathering. This service is hosted in the cloud and is managed for you as a part of the SaaS offering.
AirWatch Cloud Messaging service (AWCM)	Service used in conjunction with the AirWatch Cloud Connector to provide secure communication to your backend systems. AirWatch Cloud Connector also uses AWCM to communicate with the Workspace ONE UEM Console. AWCM also streamlines the delivery of messages and commands from the Workspace ONE UEM Console by eliminating the need for end users to access the public Internet or utilize consumer accounts, such as Google IDs. It serves as a comprehensive substitute for Google Cloud Messaging (GCM) for Android devices and is the only option for providing mobile device management (MDM) capabilities for Windows rugged devices. Also, Windows desktop devices that use the VMware Workspace ONE® Intelligent Hub use AWCM for real-time notifications. This service is hosted in the cloud and is managed for you as a part of the SaaS offering.
Database	Microsoft SQL Server database that stores Workspace ONE UEM device and environment data. All relevant application configuration data, such as profiles and compliance policies, persist and reside in this database. Consequently, the majority of the application's backend workload is processed here.
VMware Tunnel	The VMware Tunnel provides a secure and effective method for individual applications to access corporate resources hosted in the internal network. The VMware Tunnel uses a unique X.509 certificate (delivered to enrolled devices by Workspace ONE) to authenticate and encrypt traffic from applications to the tunnel. VMware Tunnel has two components – Proxy and Per-App VPN. The Proxy component is responsible for securing traffic from endpoint devices to internal resources through the VMware Workspace ONE® Web app and through enterprise apps that leverage the Workspace ONE SDK. The Per-App Tunnel component enables application-level tunneling (as opposed to full device-level tunneling) for managed applications on iOS, macOS, Android, and Windows devices.
Workspace ONE UEM Secure Email Gateway (proxy)	Microsoft Exchange 2010, 2013, and 2016
Content Gateway	VMware Content Gateway provides a secure and effective method for end users to access internal repositories. Users are granted access only to their approved files and folders based on the access control lists defined in the internal repository through Workspace ONE Content. To prevent security vulnerabilities, Content Gateway servers support only Server Message Block (SMB) v2.0 and SMBv3.0. SMBv2.0 is the default. Content Gateway offers basic and cascade mode (formally known as relay-endpoint) architecture models for deployment.

The Solution

Unified Endpoint Management: Manage the full lifecycle of any endpoint – mobile (Android, iOS) in WS1 ONE management console to support all your mobility use cases.

Assurance and Productivity: Deliver a great employee experience that's consistent on Android, iOS devices , no matter where employees work, by combining a self-service unified app catalog with SSO, Assist remote support, and Privacy Guard to secure user data.

Corporate Data and App Protection: Protect data and defend against modern day security threats with conditional access and compliance policies. Workspace ONE UEM offers a comprehensive security approach that encompasses user, endpoint, app, data and network.

Benefits

Provide security and DLP for end user android and IOS devices to protect corporate data, Application and intranet websites.

Key Benefits of Workspace one UEM

1. Manage Android, iOS devices in a Single Solution
   - Workspace ONE is built to manage the entire lifecycle of any endpoint, across all major operating systems in a single management console.
2. Support the Full App Lifecycle from Development to Deployment
   - Workspace ONE supports the complete app lifecycle including sourcing or developing an app, applying security policies, deploying an app catalog and analyzing app metrics.
3. Protect Corporate Apps and Data on Any Network
   - Workspace ONE provides a layered security approach that encompasses the user, endpoint, app, data and network. All security settings and policies can be configured using a single platform for a comprehensive security model.
4. Increase Mobile Productivity with Engaging Business Apps
   - The VMware Workspace ONE productivity apps suite available with Workspace ONE provides frictionless access to business apps with inherent security for employee productivity.
5. Automate Processes and Deliver Insights for a More Efficient IT
   - Ease the strain on IT that is typically associated with initial device deployment and day-to-day mobility management.