TaaS Service Portfolio for Enterprise Mobility with VMware Workspace ONE

mobile mentor

Document Information

Organisation	Mobile Mentor
Project Name:	Telecommunications as a Service
Document Name:	Service Portfolio for Enterprise Mobility with VMware Workspace ONE (AirWatch)
Author/s:	Denis O'Shea
Contributors	Liz Knight, Amanda Gray, Daniel McCarthy, William Todd

Reference documents

Title	Author	Version
Managed Security Service Catalogue	DIA	2019
Service Aggregation Service Catalogue	DIA	2019

1. Service Portfolio for Enterprise Mobility

1.1. Purpose

This document outlines the portfolio of services in two service catalogues and provides an explanation of each with the relevant inclusions, exclusions and SLAs.

This is intended to be a buyer's guide to identify the relevant services and product codes.

Prices and detailed service descriptions can be found in the two Service Catalogues on the DIA portal; Managed Security and Service Aggregation.

1.2. Service Map

The illustration below outlines each of the services and how they address enterprise mobility.

Mobile Device Management and Mobile Threat Management services at TaaS Certified.

Managed Security

1. Mobile Device Management
2. Integration Services
3. Secure Content
4. Policy Management
5. Mobile Threat Management

Service Aggregation

1. Mobile Asset Management
2. Mobile Service Desk
3. Hardware Lifecycle Management
4. Mobile App Management
5. Personal Spend Management

2. Managed Security Catalogue Summary

2.1. Mobile Device Management (Taas Certified)

The MDM service is based on the VMware Workspace ONE (AirWatch) platform which is hosted and managed by Mobile Mentor and is certified by TaaS.

VMware (AirWatch) is the leading global vendor for device management providing Agencies with secure access to WiFi, email, calendar, contacts and enterprise apps.

Service Element	Service Description
1. Hosted in CCL Revera IaaS	Our MDM infrastructure is hosted in New Zealand and certified by the DIA - GCDO.
2. High Availability	Application level high availability with an active / passive model by using passive secondary servers.
3. Geo-Diversity	Automated fail-over and fail-back through geographically diverse, inter-connected data centers.
4 iOS, Android & Win 10	Standard configuration includes 3 sets of policies and profiles for each OS (Android, iOS and Windows 10).
5. Enterprise App Store	Provision of an enterprise app store to present users with a catalogue of internal apps and a white-list of approved public apps and black-list of apps known to be malicious.
6. App Distribution	Distribute, update and revoke enterprise apps using distribution groups and the enterprise app store.
7. Software Assurance	Software license assurance is provided by Mobile Mentor.
8. Regular Software Updates	The software is maintained by Mobile Mentor's certified engineering team, in line with AirWatch's best practices.
9. Live Reporting Dashboard	Mobile Mentor provide a dashboard of reports showing all managed devices, time last seen, policy compliance etc.
Reference	*PD1S in the Managed Security Service Catalogue*

2.2. Integration Services

This uplift provides the integration between the MDM platform and the Agency's Active Directory, Certificate and Exchange / Office 365 Services.

Service Element	Service Description
Active Directory	Directory Services – authenticate devices and administrators from the Agency's Active Directory.
Certificate Services	Certificate Services – enable MDM to issue device certificates from in-house, or cloud Public Key Infrastructure (PKI) to permit or deny mobile access to resources such as Wi-Fi and application gateways.
PowerShell Connector	Microsoft 365 – PowerShell integration to ensure Exchange Online is only accessible to complaint managed devices.
Secure Email Gateway	Exchange on-premise – Physical server configured in front of the corporate email server to implement a pre-defined set of compliance decisions for every mobile device it manages.
Reference	*PD2S in the Managed Security Service Catalogue*

2.3. Secure Content

This uplift provides an encrypted container to separate work data from personal data in email, calendar and contacts. It also includes a secure browser with per-app VPN for accessing internal content securely.

Service Element	Service Description
Containerised Email	VMware Boxer email client which provides a secure encrypted container for email and calendar.
Secure Browsing	VMware Secure Browser to open and view attachments using a per-app VPN connection.
Microsoft 365	PowerShell integration to Microsoft 365 to control Exchange Online access for non-compliant devices..
Secure Email Gateway	Exchange on-premise – Physical server configured in front of the corporate email server to implement a pre-defined set of compliance decisions for every mobile device it manages.
Reference	*PD3S in the Managed Security Service Catalogue*

2.4 Proactive Policy Management

Proactive Policy Management to ensure that the mobile policy is implemented, enforced, monitored and managed.

Service Element	Service Description
Policy Splash Screen	The agency's mobile policy is presented via an interactive mobile app with a readable, bullet point summary and questions related to data security and privacy.
Policy Sign-on-Screen	The employee accepts the terms, signs on-screen and submits the signed policy which is saved to a database accessible by the Agency's HR department.
Policy Management	If a policy breach or security incident occurs, the organisation is equipped with a signed policy from the user and is able to take the appropriate action.
Compliance Monitoring	Mobile Mentor monitors the devices under management for compliance with policy and identifies non-compliance events to be addressed.
Compliance Monitoring	We report on policy compliance through the ZOOOOM dashboard. Every three months we review the policy and make adjustments to reflect industry threats, organisational changes and the most common breaches.
Reference	*PD4S in the Managed Security Service Catalogue*

2.5 Mobile Threat Management (TaaS Certified)

App scanning and analysis to detect, assess, report and mitigate the risks of malware and malicious apps.

Service Element	Service Description
App Reputation and Network Scanning	App reputation scanning using an industry leading platform to detect malicious apps and determine risk severity. Detection of malicious network activity.
Threat Analysis	Industry scanning and threat analysis to assess the security posture of the device OS, EMM platform, AV and apps under management;
Severity Scoring	New threats or changes graded by severity and likelihood by a qualified security analyst and documented for auditability;
Risk Mitigation	Software patching, app updates, policy changes and changes to system settings to mitigate identified risks.
Risk Reporting	Reporting on device security posture, risk scores and system health.
Reference	*PD5S in the Managed Security Service Catalogue*

3. Service Aggregation Catalogue

3.1 Mobile Asset Management

Mobile Asset Management is the combination of 3 essential services:

1. Mobile expense management (analysis and optimization);
2. Rapid replacement, service restoration, repair management for devices;
3. Reporting Dashboard

Service Element	Service Description
Report	The billing feeds are extracted from the network providers (at a minimum these are Vodafone, Spark and 2Degrees) to build a mobile billing data warehouse.
Optimise	An in-depth analysis of monthly spend is performed, highlighting outliers, trends and savings are identified, with an action plan to realise savings.
Implement	We seek approval for the proposed changes and then implement the agreed changes directly in the billing systems of the mobile service providers.
Replacement	When an Agency user loses, breaks or damages a mobile or tablet, Mobile Mentor provisions a similar replacement device to the user. Mobile Mentor manages the buffer stock, provided by the Agency, which may represent 3% of the fleet. Mobile Mentor pays for couriers and insurance.
Restoration	We proactively assist to restore settings, email, apps and content so the user can quickly 'Return to Operation'. We report on RTO monthly.
Repair	We manage the repair process in the background, perform triage in-house, manage the warranty process and select the appropriate repair agent to ensure all repairs are done at the lowest cost to the Agency. .

Reporting Dashboard	Mobile Mentor provides a web-based dashboard to give agencies an overview of key metrics for the services lines provided to the agency
Reference	*PD1A in the Aggregation Service Catalogue*

3.2 Service Desk

24 x 7 specialist team for mobile procurement, provisioning, enrolment and user support through the **m.power** mobile support app.

This service applies to all mobile devices, all networks, with all major MDM providers, and all ownership models (BYOD, CYOD & COPE).

Service Element	Service Description
24 x 7 x 365 Mobile Service Desk	The service desk is staffed by a team of dedicated mobile experts who have the appropriate skills, experience and industry certifications. Our mobile service desk is distributed between Auckland and Wellington and staff can be located at the customer's premises by special arrangement. The Mobile Mentor specialist service desk can be provided on a white label basis so that we essentially become an extension of the Agency's service desk. Specialist service desk operating during NZ business hours with SLAs as defined. Outside business hours an oncall service is provided with an objective of calls returned within 30 minutes.
Procurement	Procurement activity is handled by the Service Desk and devices are delivered directly to the user. For large clients we integrate tightly with their internal procurement processes.
Assisted Enrolment	Highly visual and intuitive enrolment guides are provided for each OS and version. Assistance is also provided over the phone to assist users with the process of enrolling their devices where required
Reference	*PD2A in the Aggregation Service Catalogue*

3.3 Personal Spend Management

Separate business and personal usage for end users and cost center managers and reconcile employee reimbursements for personal usage.

Unique process for identification, reimbursement and reconciliation of personal usage for end-users and cost center managers.

Service Element	Service Description
Itemised Reports	Detailed usage and spend reports are provided each month to three groups: • ISR: Individual Spend Report (separates personal and business usage) • CCR: Cost Center Report (roll-up of all users in the cost centre) • GMR: General Manager Report (roll-up of all cost centres)
Reimbursement via Payroll	Automated reimbursement process integrated to the Agency's payroll process.
Reconciliation with Cost Centers	Reconciliation of employee reimbursements with the cost centers to provide complete transparency and accountability.
Reference	*PD3A in the Aggregation Service Catalogue*

3.4 Hardware Lifecycle Management

Management of the hardware life-cycle from device selection, accessories, repair and secure erasure at end of life.

Hardware lifecycle management service that applies to all mobile devices and all ownership models (BYOD, CYOD & COPE).

Service Element	Service Description
Sensible Short-List	Mobile Mentor operates independently of the hardware manufacturers. We guide our clients towards the devices that can be secured, managed and supported by their MDM platform.
Accessories	All smartphones and tablets procured through Mobile Mentor will receive a silicone case and/or a screen protector to extend the life of the device.
Refresh Program	Device upgrades managed according to any available carrier hardware subsidies or internal refresh programme.
Asset Tagging	Maintain a configuration management database of all hardware assets under management.
Secure Erasure	A secure erasure is performed on devices prior to repair, re-allocation to new user or recycling. This uses a tool that wipes a device beyond the level of a factory reset to ensure that it can be re-used for Government or healthcare purposes without any risk of residual data remaining on the device
Reference	*PD4A in the Aggregation Service Catalogue*

3.5 App Management

App distribution through the enterprise app store, release management, Level 1 support and analytics for enterprise apps.

Management of the portfolio of productivity apps (both public and enterprise apps) deployed to Agency devices.

Service Element	Service Description
Enterprise App Store Management	Management of the Agency's app store with 10 standard public apps per OS included.
Apple Volume Purchase Program	Administration of the Apple VPP account and management of app licenses to appropriate distribution groups
Level 1 Support for Vertical Apps	Support internal users with app installation and connectivity for up to 5 vertical / Line Of Business apps.
Release Management for Vertical Apps	Planning, approval, basic testing, rollout, communications & documentation for a combined total of 30 app updates p.a. for internal users.
App Analytics	Analysis and reporting of app inventory, trends, usage (if available) and opportunities for productivity improvement.
Reference	*PD6A in the Aggregation Service Catalogue*