



Consolidated Technology Services • WA

CTS Mobile Data Management (MDM) Service Offering November 30, 2014

Feature Comparison

AirWatch Management Suites:

AirWatch markets their products in Management Suites. Using a color code (see [AW Management Suites](#)), each suite offers increasing levels of MDM functionality. At the time CTS released its RFP, AirWatch management suites did not exist. Since the RFP, AirWatch has defined four management suites; Green, Orange, Blue, and Yellow. CTS is grandfathered into the next-to-the-highest Blue Management Suite. The only difference between the Blue management suite and the higher Yellow management suite is the inclusion of Secure Content Locker Collaborate.

Helpful Terms:

- Secure Email Gateway (SEG) – Advanced email security including certificate based email authentication.
- Managed Application Gateway (MAG) – The MAG manages access to backend applications on corporate file servers. The MAG requires a security review before implementation can occur.
- Secure Content Locker (SCL) – A secure compartment to view and or edit documents on a mobile device.
 - Secure Content Locker View – a read only version
 - Secure Content Locker Collaborate – a read/write version

Feature Comparison Table

Feature	Included in CTS offering?	Secure Email Gateway (SEG) required?	Managed Application Gateway (MAG) required?	Secure Content Locker required?
<p>Mobile Device Management AirWatch® Mobile Device Management enables businesses to address challenges associated with mobility by providing a simplified, efficient way to view and manage all devices from the central admin console. Our solution enables you to enroll devices in your enterprise environment quickly, configure and update device settings over-the-air, and secure mobile devices. With AirWatch, you can manage a diverse fleet of Android, Apple iOS, BlackBerry, Mac OS, Symbian, Windows Mobile, Windows PC/RT and Windows Phone devices from a single management console.</p>	Yes	No	No	No
<p>Workspace Management AirWatch® Workspace Management provides complete separation of corporate and personal data on devices, securing corporate resources and maintaining employee privacy. AirWatch enables organizations to standardize enterprise security and data loss prevention strategies across mobile devices through our flexible approach to containerization. With app-level and AirWatch Workspace options for containerization, you can deploy corporate containers to fit your enterprise security requirements.</p>	Yes Requires AirWatch Workspace app	No	No	No
<p>App Catalog AirWatch® Mobile Application Management addresses the challenge of acquiring, distributing, securing and tracking mobile applications. Easily manage internal, public and purchased apps across employee-owned, corporate-owned and shared devices from one central console.</p>	Yes	No	No	No
<p>Inbox AirWatch® Mobile Email Management delivers comprehensive security for corporate</p>	Yes	Yes, if encryption is	No	Yes, if encryption is

Feature	Included in CTS offering?	Secure Email Gateway (SEG) required?	Managed Application Gateway (MAG) required?	Secure Content Locker required?
<p>email infrastructures. Email security requirements vary for organizations, depending on supported device ownership models and industry regulations. AirWatch offers flexible options for your email management strategy, giving you choice over the deployment strategy that best fits your business and security requirements. Integration with existing email infrastructures ensures you are maximizing your technology investments. Access to corporate email can be configured through the native device client or the AirWatch Inbox, a containerized email solution.</p>	Requires AirWatch Inbox app	needed, else No.		needed, else No.
<p>App Wrapping AirWatch App Wrapping gives your existing internal applications an extra level of security and management capabilities, without further development or code change. Administrators can quickly and easily wrap applications from the admin console, and be confident their applications are secure.</p>	Yes	No	Yes, if tunneling to internal resources, else no	No
<p>App Reputation Scanning As employees increasingly demand more apps for business, IT administrators must block malicious applications and certify that internal and third-party applications meet their organization’s security standards. Administrators need to protect organizations from publicly available malicious applications, risks that come with internal and third-party apps, and address concerns around apps accessing personal data on employee-owned devices.</p> <p>AirWatch® App Reputation Scanning allows IT to identify common app risks, such as access to privacy settings, insecure network connections, malicious code and more. With AirWatch, you can run app scans, view the results and take action. Our comprehensive mobile ecosystem includes leading app risk management providers to deliver advanced app risk management functions integrated with AirWatch.</p> <p>Administrators can scan applications directly in the admin console. From the application list view, administrators simply select an application and click the ‘Run</p>	Yes	No	No	No

Feature	Included in CTS offering?	Secure Email Gateway (SEG) required?	Managed Application Gateway (MAG) required?	Secure Content Locker required?
<p>Reputation Analysis' command. During the scan, AirWatch identifies potential privacy, behavior, and design and programming risks.</p>				
<p>Browser AirWatch® Mobile Browsing Management enables secure browsing and provides organizations with the ability to configure customized settings to meet their unique business and end-user needs. AirWatch® Browser allows administrators to define and enforce secure browsing policies from the admin console. Our secure browser allows corporations to take advantage of mobile browsing without security risks.</p> <p>With AirWatch, you can disable native browsers and public browser applications to drive all browsing through AirWatch Browser. This allows you to customize web browsing to fit your specific business requirements; whitelist IP addresses for access; define use policies for cookie acceptance, copy/paste, printing and capturing browsing history; and require Terms of Use (TOU) agreement acceptance. You can also require downloaded content to open in Secure Content Locker TM.</p>	Yes	No	No	No
<p>Secure Content Locker AirWatch by VMware enables secure mobile access to content anytime, anywhere. AirWatch® Secure Content Locker® protects your sensitive content in a corporate container and provides users with a central application to securely access, store, update and distribute the latest documents from their mobile devices.</p> <p>Secure Content Locker (SCL) View – a read only version of SCL</p>	Yes	No	No	Yes Requires AirWatch SCL app.

Feature	Included in CTS offering?	Secure Email Gateway (SEG) required?	Managed Application Gateway (MAG) required?	Secure Content Locker required?
Secure Content Locker (SCL) Collaborate – a read/write version of SCL	No Under CTS review. This AirWatch offering did not exist at the time the RFP was released. As such, it was not identified as a requirement.	Yes, if encryption is needed, else No.	No	Yes, if encryption is needed, else No.

Road Map

- Phase 1 MDM deployment – complete October 1
- Phase 2 preliminary Planning – complete November 30
- Assign a Project Manager and begin planning: Scope, Schedule, and Budget for phase 2 (SEG and MAG) December 1, 2014.
- Configuration complete in the Lab - January 5th, 2015
- Production Design Complete February 1.
 - SEG
 - MAG
 - SCL Collaborate – this feature is new since the completion of the CTS RFP. As such, it was not in scope at the time the RFP was let. It is an additional cost to the AirWatch license. Inclusion in the CTS service offering is dependent on passing a security design review, testing, rate impact analysis, and customer demand. Assuming these caveats come together in an acceptable way then CTS will pursue inclusion on this feature in its MDM service offering.
 - Secure Texting – this feature is new since the completion of the CTS RFP. As such, it was not in scope at the time the RFP was let. It is not yet known if it is an additional cost to the AirWatch license. Inclusion in the CTS service offering is dependent on passing a security design review,

testing, rate impact analysis, and customer demand. Assuming these caveats come together in an acceptable way then CTS will pursue inclusion on this feature in its MDM service offering. In the meantime, secure texting is available today via Lync.

- Security Design Review Complete March 1
- Rate Analysis March 1 thru March 31
- Test March 1 thru March 31
- Customer pilot April 1 thru April 30
- Production Deployment Complete, SEG and Mag – June 30, 2015
 - SEG – Encrypted Documents, Email, and Licensing
 - MAG – Access to Internal apps
 - Secure Content Locker Collaboration (per caveats above)
 - Secure Texting (per caveats above)

DRAFT

CTS MDM Phase 2 Road Map Diagram

