Mobile Device Management (MDM)

Begin with the Basics: Manage the Complete Device Lifecycle

Secure Productivity Apps: Mail, Calendar, Docs, and Chat

Workspace ONE includes email, calendar, contacts, documents, chat, and enterprise social that employees want to use while invisible security measures protect the organization from data leakage by restricting how attachments and files can be edited and shared.

Far from a “walled garden;” team chat, enterprise discussions, Q&A, content access and other social tools that allow employees to work collaboratively in real time can be integrated into the apps and tools they already use - moving from productivity to real employee engagement.

FEATURE	DESCRIPTION
Consumer-simple Email app delights consumers but is designed for business	A faster, smarter, secure email app that supports your Gmail, Exchange, Outlook, Yahoo, Hotmail, iCloud, Office 365, IMAP & POP3 mail accounts. With integrations to your favorite services like Dropbox, Box and Evernote, it’s easier than ever to stay organized.
Integrated Calendar with email makes it simple to set meetings	By integrating email and calendar you no longer have to move out of the email app when you received a meeting invitation. With a few clicks, you can review, respond to the meeting or suggest a new time based on your availability without having to navigate between apps.
Advanced email attachment security reduces data leakage	Secure email and attachments through the use of the AirWatch Secure Email Gateway that can enforce enterprise encryption, wipe, and “open in” controls keeping attachments secure.
Content Management App permits line of business to push and manage secure content on the device	AirWatch Content Locker mobile app permits IT to deliver files directly to devices across a range of internal repositories and external cloud storage providers to ensure the latest, most up-to-date information is at employees fingertips.
Enterprise Chat that increases employee engagement	Secure enterprise chat platform bridges systems of record by integrating into existing enterprise applications while providing a customizable mobile-first chat and notification experience.

Add new devices quickly and easily provision apps and policies without IT involvement.

- Configure devices with bulk provisioning programs such as the Apple Device Enrollment Program (DEP), Knox Mobile Enrollment and Android zero-touch enrollment
- Enable users to self-activate devices by entering their corporate credentials in a simple MDM onboarding workflow
- Configure MDM policies for device restrictions, layout, settings access, notifications and more and assign based on OS or ownership type (BYO or corporate-owned)
- Deploy public, internal or bulk-purchased apps to devices automatically or to an enterprise app catalog for on-demand install
- Connect to enterprise email, VPN, Wi-Fi, content, intranet sites and other backend resources

Protect corporate information through device security and data loss prevention (DLP) policies.

- Enable device-level encryption, data encryption and hardware security policies (TPM, biometrics, etc.)
- Enforce a device- and/or app-level passcode with complexity and history requirements
- Configure policies including: app blacklists, device pairing, Wi-Fi security, TLS enforcement and others
- Prevent data loss with app sharing permissions, copy/paste restrictions, geo-fencing policies, and more
- Monitor for malware threats or jailbroken devices and automatically remediate with a remote lock, device wipe or customizable device quarantine controls

Get full visibility and manage all endpoints from a single admin console.

- Gain visibility into all endpoints across BYO, corporate-owned and line of business ownership models in a single admin console
- Delegate management across divisions, regions and departments with our multitenant architecture and role-based access controls
- Get real-time MDM deployment analytics from modular and role-based dashboards by devices, apps, email, security, telecom and more
- Capture detailed analytics with report templates and granular device, app and console event logging
- Export deployment analytics to third-party business intelligence (BI) solutions with DataMart integration

Enable remote commands and controls to easily troubleshoot devices.

- Request device information and perform remote commands such as clear passcode, send message, lock device, or perform an enterprise or device wipe
- Troubleshoot devices using remote control to view the device screen and gain access to the file manager, command prompts and more
- Enable users with self-service access to basic management capabilities, such as resetting a passcode, to alleviate IT ticket requests