AT&T Business

Help safeguard your mobile inventories and extend the reach of your workforce.

Features

- Fast user configuration from a single console
- Policy customization and administration
- Lock/Wipe lost or stolen devices
- Integrates with existing enterprise resources
- Shared or dedicated architecture available

VMware AirWatch® Enterprise Mobility Management™ supports deployments of mobile devices at any scale. In today's business environment it is critical to keep employees connected and able to work virtually anytime, anywhere on any device while keeping corporate data protected.

VMware AirWatch is a leading Enterprise Mobility Management platform that enables central management of devices, apps, and content – both corporate-owned and personally-owned devices.

The Solution is a shared or dedicated hosted enterprise mobility management software application solution set comprised of four generally available management suites, and one suite for primary and secondary educational institutions. The suites are offered in progressive layers to deliver a Customer's specific needs for features and functionality. All suites include VMware AirWatch Mobile Device Management™, VMware AirWatch Mobile Application Management™, VMware AirWatch Container™ and VMware AirWatch App Catalog™.

VMware Airwatch **Mobile Device Management**

- The Solution's core is AirWatch Mobile Device Management, which enables broad scale deployment of mobile devices with quick enrollment and easy configuration. Updates are provided over-the- air, and IT administrators can enforce policies, set restrictions, and provide security for devices while in use and if lost or stolen. This Solution supports Android, iOS, BlackBerry, Apple Mac OS, and Windows operating systems from a single console.
- Customers can manage many functions from a single administrative portal.

VMware Airwatch **Mobile Application Management**

VMware AirWatch Mobile Application Management offers a comprehensive set of services and tools that can be used to provide highly secure delivery, management, and tracking of mobile applications deployed on end users' devices. Mobile Application Management supports management of internal, public, and purchased applications from a single console.

VMware Airwatch **Container**

VMware AirWatch Container separates corporate and personal data on iOS or Android smartphone devices, helping to ensure that Customer resources are highly secure and employee privacy is maintained.

VMware AirWatch Container creates a virtual container on devices where both AirWatch and Customer developed applications may be viewed inside and outside the AirWatch Container view but are secured through use of a shared container passcode. Access to applications is granted to end users as apps in the container and can be managed by an administrator at the application level rather than the device level.

VMware Airwatch **App Catalog**

VMware AirWatch App Catalog enables Customers to manage and distribute enterprise applications via the AirWatch Admin Console. Customers' end users can

locate and access applications within the App Catalog based on policy settings established within the console, which can distribute, update, track and recommend applications in the AirWatch App Catalog to end users.

VMware Airwatch Solutions

	AirWatch **Green Suite**	AirWatch **Orange Suite**	AirWatch **Blue Suite**	AirWatch **Yellow Suite**	AirWatch **K-12 EDU Suite†**
AirWatch Mobile Device Management	■	■	■	■	■
AirWatch Mobile Application Management	■	■	■	■	■
AirWatch Container	■	■	■	■	■
AirWatch App Catalog	■	■	■	■	■
VMware Boxer		■	■	■	■
AirWatch App Wrapping			■	■	■
VMware Browser			■	■	■
VMware Identity Manager			■	■	■
VMware Content Locker – Standard			■	■	■
VMware Content Locker - Advanced				■	
AirWatch Advanced Telecom				■	

† This suite is only available to primary and secondary educational institutions

Management Suites

The Solution is offered in four suites: VMware AirWatch Green Management Suite™, VMware AirWatch Orange Management Suite™, VMware AirWatch Blue Management Suite™, and VMware AirWatch Yellow Management Suite™, as well as a suite for educational institutions. All suites include AirWatch Mobile Device Management, AirWatch Mobile Application Management, AirWatch Container and AirWatch App Catalog. The features available with each suite are described in the Optional Software Features section below.

Optional Software Features

The following optional features are available individually or as components of the suites described in the table on the previous page.

VMware Content Locker (Optional)

VMware AirWatch Container separates corporate and personal data on iOS or Android smartphone devices, helping to ensure that Customer resources are highly secure and employee privacy is maintained.

VMware Content Locker – Standard
VMware Content Locker™ - Standard provides highly secure document distribution and mobile access to Customer documents using mobile applications on users' devices. Content Locker helps protect sensitive content in a highly secure container and provides users a central application to access Customer documents from their mobile devices. Access to mobile applications is available for use on iOS, Android and Windows devices.

VMware Content Locker – Advanced
VMware Content Locker™ - Advanced offers the features and functionality of Content Locker – Standard plus Advanced features such as editing, annotation and commenting capabilities on shared files are also included. Content Locker Sync™ provides users with two-way synchronization of content between desktops and devices. Content Locker Sync provides PC users with highly secure access to corporate content on their personal computers. The web-based self-service portal allows PC users to add, manage and share individually created content.

Additional Professional Services are required.

VMware AirWatch App Wrapping (Optional)

VMware AirWatch App Wrapping™ is an optional feature that allows a Customer to incorporate additional functionality into its developed applications that may reduce or eliminate the need for development or code changes. The process of wrapping an application is initiated directly from the AirWatch Admin Console. Once an application is wrapped, the Customer can perform a number of administrative actions on the application, including actions to increase security.

AirWatch App Wrapping functionalities include the ability to:

- Detect and prevent access to compromised devices
- Prevent data-loss by disabling the copy and paste, Bluetooth and camera functions (on Android and iOS devices)
- Control devices' ability to access networks based on network type or by service set identifiers ("SSID"s)
- Control offline access to applications
- Redirect traffic using App Tunneling with the AirWatch Mobile Access Gateway ("MAG"). (Requires purchase of MAG Installation Professional Service)

VMware AirWatch Software Development Kit (App Wrapping Required)

VMware AirWatch Software Development Kit is included as part of the AirWatch App Wrapping option and allows functionality to be applied to custom iOS and Android applications, as well as other AirWatch applications. Customers can choose to apply profile settings and policies at an Organization Group ("OG") level. These options are shared across applications located in the OG. Customers can also customize profiles for App Wrapping, and other AirWatch applications. Options are mirrored in each area.

Note: AirWatch Software Development Kit technical support is available directly from AirWatch. Customers must agree to the terms and conditions of a separate AirWatch Software Development Kit License Agreement. A copy of the AirWatch Software Development Kit License Agreement is found at: http:// www.air-watch.com/downloads/ legal/201411-SDK-License-Agreement.pdf

VMware Boxer (Optional)

VMware Boxer provides highly secure mobile access to corporate email, calendar and contacts across corporate-owned and personally owned devices while respecting user privacy.

- Gives users everything they need to be productive in a single app with integrated mail, calendar and contacts
- Implements Exchange ActiveSync (EAS) and IMAP protocols to connect to various email systems
- Enables quick actions, including pre- determined email replies, predictive move to folders and one-tap sharing of calendar availability
- Allows users to personalize their experience with customizable swipe gestures, contact avatars and more
- Integrates with third-party business apps to simplify daily workflows and increase mobile productivity

VMware Browser (Optional)

VMware Browser™ is a highly secure Internet browsing alternative to native Internet browsers and provides Customers the ability to configure and enforce browsing policies for Internet and Intranet sites without requiring a device-level VPN. Browsing is enabled by utilizing one of the two browsing options described below.

Restricted Mode
This mode affects the browser's functionality and its ability to access specified web content. For example, administrators can restrict web access from certain websites or provide an Internet portal for devices used as a mobile point of sale.

Kiosk Mode
This mode restricts the VMware Browser to a specific home page. It also disables the navigation bar, which limits navigation to links that appear on the home page.

VMware Identity Manager (Optional)

VMware Identity Manager™ is identity management for the mobile cloud that delivers one-touch access to nearly any app, from any subscribed device, optimized with AirWatch Conditional Access. Empower employees to get productive quickly with a self-service app store, while giving IT a central

place to manage user provisioning and access policy with enterprise-class directory integration, identity federation and user analytics.

- Enterprise single sign-on. Simplify business mobility with included identity provider (IDP) or integrate with existing on-premises identity providers to aggregate SaaS (Software-as-a-Service) and Native Mobile and Windows 10 apps into a single catalog
- Self-service app store. Supports a Customer branded app store that enables users to subscribe to applications across devices with automated or manual provisioning
- Identity management with adaptive access. Establishes trust between users, devices and the hybrid cloud, providing conditional access controls that leverage AirWatch device enrollment and SSO

VMware AirWatch Advanced Telecom (Optional)

VMware AirWatch Advanced Telecom includes capabilities available with VMware AirWatch Mobile Device Management plus advanced capabilities to define users' usage plans, set usage thresholds and enforce compliance policies. AirWatch Advanced Telecom can create telecom usage plans, either per device or by group, and define usage thresholds for voice, SMS and data usage based on plan limits. Compliance policies can be configured around usage thresholds to help prevent end users from going over plan limits for voice, SMS and data usage by automatically triggering alerts or removing profiles at specified thresholds. Additional Professional Services are required.

Certificates and Kerberos Delegation

Certificate authentication enables enterprises to verify end users' identity without requiring them to enter usernames and passwords on their mobile devices to access enterprise resources, such as Exchange ActiveSync, VPN or an enterprise's Wi-Fi.

Service Scope

AT&T will implement and configure the integration settings to enable the Solution to issue certificates to mobile devices from a supported interface to Customer's Certificate Authority.

In completing the Certificate Authority integration AT&T will:

- Create one certificate template representing the Customer's desired type of identity certificate
- Define one device policy profile for Exchange ActiveSync auto-configuration using an MDM-issued identity certificate
- Define one device policy profile for VPN client auto-configuration using an identity certificate
- Define one device policy profile for the preferred Wi-Fi network auto- configuration using an identity certificate
- Configure the service accounts in Active Directory (User or Computer object) for Kerberos authentication delegation and create service principal names ("SPNs") if necessary
- Configure the email proxy service to request Kerberos delegated credentials on behalf of device users for mailbox access
- Assist with the testing of each device profile on a single supported device*

EMM Software Installation and Configuration Services (Required)

One of the four immediately following Installation and Configuration Services options is required.

Basic Installation and Training (Required for AirWatch Mobile Device Management) AT&T will provide implementation services. The deployment will be conducted in an AirWatch hosted environment with optional integration supported by an AirWatch Connector in the Customer's data centers and initial deployment of an initial pilot set of devices. This service consists of two meetings.

Basic Plus Installation and Training (Required for AirWatch Mobile Device Management when supporting mobile devices with multiple users) Basic Plus offer includes all of the features of Basic Installation and Training plus the configuration of the AirWatch Launcher feature for the setup of shared Android devices.

Premium Installation and Training Services for EMM Software (Required for designs that contain a Secure Email Gateway) AT&T will provide implementation services. The services include installation of the AirWatch Console, an optional Connector and either a Secure Email Gateway or PowerShell Integration for email management and an initial pilot set of devices. These services include four meetings.

Premium Plus Installation and Training for use of EMM Software (Required for the installation of a Mobile Access Gateway) Premium Plus Installation and Training Services include all the features of Premium Installation and Training, as well as installation of a Mobile Access Gateway for content management or highly secure browsing, and installation, configuration, and training for VMware Identity Manager.

VMware Content Locker – Advanced Training (Optional)

AT&T will provide implementation services associated with the purchase of AirWatch software licenses and hosting fees. The deployment includes one meeting that will be conducted remotely in Customer's hosted environment, with integration provided using an existing Mobile Access Gateway.

Advanced Telecom Configuration and Training AT&T will provide implementation services associated with the purchase of AirWatch Advanced Telecom. The deployment includes one meeting that will be conducted remotely using an existing AirWatch hosted environment.

VMware AirWatch Secure Email Gateway Implementation and Configuration

AT&T will remotely configure and integrate one Secure Email Gateway into an existing AirWatch environment. Setup will include basic Secure Email Gateway configuration and integration with Customer's existing (Exchange or Lotus Notes) email environment. For high- availability environments, configuration of the network load balancer cluster and monitoring for cluster member management is the sole responsibility of Customer.

VMware AirWatch Mobile Access Gateway Implementation and Configuration

AT&T will remotely configure and integrate one Mobile Access Gateway into an AirWatch environment. Setup will include integration to one or all of the following:

- Internal document repositories and content using the AirWatch Content Locker
- Internal websites using the VMware Browser
- Internal web applications with access to internal resources

VMware AirWatch Connector Implementation and Configuration

AT&T will remotely configure and integrate one AirWatch Connector. Setup will include integration to one Active Directory server. Customer is responsible for provisioning a server in accordance with the configuration checklist provided.

EMM Operations Training (Optional)

AT&T will conduct knowledge share and training for Customer's technical staff on the Solution. The engagement is up to five hours in duration. The training is delivered remotely via web conference and includes Customer hands-on configuration of Boxer container setup, AirWatch App Wrapping of one Customer developed application, VMware Browser and Bookmarks, and Content Locker files on the AirWatch Platform.

Presentation Topics that can be selected by the Customer include the following:

- User management
- Device registration and retirement
- Policy management and security
- Device configuration management
- Reports and logs

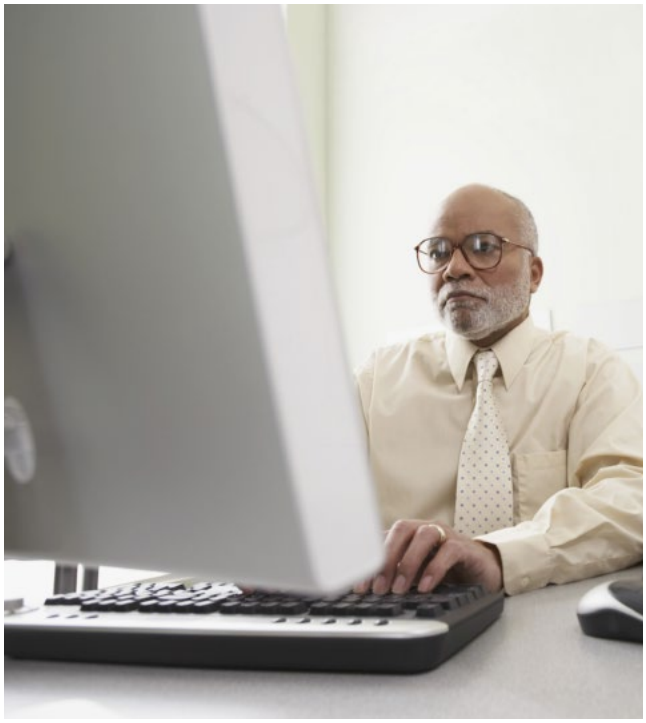
AT&T will coordinate the web conference and a pre-call will be set-up with the Customer by AT&T to review the session agenda and logistics.

Managed Service Health Check (Optional)

AT&T will remotely inspect and review the current state of the Customer's platform and validate that the server, software implementation and configuration are consistent with the managed solution platform vendor's and AT&T's best practices and recommendations. This health check is typically delivered remotely over two days by an AT&T Professional Services Consultant.

VMware AirWatch Public Key Infrastructure ("PKI") Integration and Identity Certificate Device Configuration (Optional)

AT&T will implement and configure the integration settings to enable AirWatch to issue certificates to mobile devices from the Customer's Certificate authority using the Customer's AirWatch-supported PKI integration interface. AT&T will also assist with the testing of each device profile on a single supported device.



(REQUIRED) Application Service Desk (ASD)**

Application Service Desk Support Plans are provided by the AT&T Global Mobility Applications and Security ("GMAS") ASD organization and are available to Customers that have not previously purchased a Mobile Device Management Solution from AT&T. The components of these ASD Plans include the following:

- Technical Support
- MACD (moves, adds, changes, disconnects) Administration
- Service Optimization

Monthly recurring charge ("MRC") subscriptions to all AirWatch Hosted Management Suites include an AirWatch license plus an Application Service Desk Support Plan. For orders placed before May 17, 2016, orders include the AT&T Application Support Desk 9x5 Support Plan, with an optional upgrade to the ASD 24x7 Support Plan. For orders placed on or after May 17, 2016, orders include the ASD 24x7 Support Plan. For all other subscription types (perpetual and annual term licenses) for AirWatch Hosted Management Suites (perpetual and annual term licenses), an Application Service Desk Support Plan (either 9x5 or 24x7) is required and must be purchased separately.

ASD 9x5 Support

The ASD 9x5 Support Plan best serves Customers that provide the day-to-day administration of their EMM platform and prefer to use AT&T for triage, support, and How-To and FAQs during standard business hours. It includes:

- Help desk to help desk (Tier 2) technical support from 8 a.m. - 5 p.m. local time, based on the Customer's support headquarters location, with the ability to report Severity 1 (outage) events 24x7x365
- Support to triage, escalate and attempt to resolve service issues and support requests
- Single point of contact for Tier 2 and above support to address
- interoperability between multi-carrier mobile devices, networks, the EMM platform, mobile applications and hosted infrastructure
- How-To and FAQ support for EMM platform use, configuration and best practices

ASD 24x7 Support

The ASD 24x7 Support Plan includes all the features of the 9x5 plan and is provided on a 7 day per week, 24 hour per day basis.

Notes: U.S. based Application Service Desk support is generally available Monday through Friday 7:30 a.m. to 5:30 p.m. Eastern Time zone, excluding U.S. holidays. There may be circumstances during these hours where Application Service Desk support will be provided by personnel located outside the U.S.

The on-boarding fee is waived with purchase of service application installation, configuration and training. Annual Managed Service Health Checks may be purchased for an additional charge.

Customer is solely responsible for its employees', agents' and subcontractors' use of the AirWatch Admin Console, including, without limitation, the enrollment and retirement of EMM device users.

Remote Administration Service Plan (Optional)

The Remote Administration Service Plan is a comprehensive program available at either a Basic or Advanced level that is designed for organizations that have limited internal support resources and mobile expertise. AT&T will provide the staff needed to administer Customer's EMM platform and provide an EMM consultant to assist Customer.

In addition to the services included in the ASD 24x7 Support Plan, the Remote Administration Service Plan includes:

- A solution for which AT&T provides comprehensive daily, ongoing configuration and life cycle administration of the EMM platform that includes user management, policy management, device configuration management and app and content management. In addition, Customer has access to the AirWatch Admin Console for the following: Dashboard View, Verify Device Enrollment or Registration, Passcode Reset/Unlock, Lock Device, Locate/Find, Send Messages, Run/Create Reports, Add/Delete Users, Device Enrollment (Bulk or Individual), and Wipe
- An assigned EMM consultant who will provide recommendations and ongoing consultation on Customer's EMM design, implementation and administration
- Support that enables Customer to update security policies and authorized device configurations
- Annual performance health checks for Customer installations with at least 500 devices

The Basic level of Remote Administration Service includes:

- Device Management
- User and Group Management
- Policy Management and Compliance
- Application and Content Management
- Active Directory Integration
- Certificate Management
- Support for EMM integration with email***

The Advanced level of Remote Administration Service offers all the features of ASD Remote Administration Basic Support plus:

- Complex network architecture support
- EMM advanced features support

VMware Airwatch Subscriptions (includes maintenance and hosting fees)

Description of Charges – Shared Hosted	Monthly Charge	1 Year	2 Years	3 Years
AirWatch Green Suite Device-Based Subscription	$4.25	$51.00	$102.00	$153.00
AirWatch Green Suite User-Based Subscription	$8.50	$102.00	$204.00	$306.00
AirWatch Orange Suite Device-Based Subscription	$5.00	$60.00	$120.00	$180.00
AirWatch Orange Suite User-Based Subscription	$10.00	$120.00	$240.00	$360.00
AirWatch Blue Suite Device-Based Subscription	$6.25	$75.00	$150.00	$225.00
AirWatch Blue Suite User-Based Subscription	$12.50	$150.00	$300.00	$450.00
AirWatch Yellow Suite Device-Based Subscription	$9.17	$110.00	$220.00	$440.00
AirWatch Yellow Suite User-Based Subscription	$18.33	$220.00	$440.00	$660.00
AirWatch K-12 EDU Suite Device-Based Subscription*	n/a	$13.00	$25.00	$35.00
AirWatch Advanced Telecom – Device-Based Subscription	$1.00	n/a	n/a	n/a
AirWatch Advanced Telecom – User-Based Subscription	$2.00	n/a	n/a	n/a

*K-12 Hosted Subscriptions also require purchase of 9x5 OR 24x7 ASD

Description of Charges – Dedicated Hosted	Monthly Charge	1 Year	2 Years	3 Years
AirWatch Green Suite Device-Based Subscription	$5.25	$63.00	$126.00	$189.00
AirWatch Green Suite User-Based Subscription	$10.50	$126.00	$252.00	$378.00
AirWatch Orange Suite Device-Based Subscription	$6.00	$72.00	$144.00	$216.00
AirWatch Orange Suite User-Based Subscription	$12.00	$144.00	$288.00	$432.00
AirWatch Blue Suite Device-Based Subscription	$7.25	$87.00	$174.00	$261.00
AirWatch Blue Suite User-Based Subscription	$14.50	$174.00	$348.00	$522.00
AirWatch Yellow Suite Device-Based Subscription	$10.17	$122.00	$244.00	$366.00
AirWatch Yellow Suite User-Based Subscription	$20.33	$244.00	$488.00	$732.00
AirWatch Advanced Telecom – Device-Based Subscription	$2.00	n/a	n/a	n/a
AirWatch Advanced Telecom – User-Based Subscription	$4.00	n/a	n/a	n/a

*Dedicated Hosted Subscriptions also require Dedicated Hosting Set-Up Fee

VMware Airwatch Perpetual Licenses and Maintenance

(Hosted customers required to add Hosting Fees and Application Service Desk) **Description of Charge**	**One-Time Charge**	**Annual Charge**
AirWatch Green Suite Perpetual License; Device-Based License	$50.00	
AirWatch Green Suite Perpetual License Maintenance; Device-Based License		$10.00
AirWatch Green Suite Perpetual License; User-Based License	$100.00	
AirWatch Green Suite Perpetual License Maintenance; User-Based License		$20.00
AirWatch Green Suite to AirWatch Orange Suite Upgrade – Perpetual License; Device-Based License	$22.00	
AirWatch Green Suite to AirWatch Orange Suite Upgrade – Perpetual License Maintenance; Device-Based License	$4.50	
AirWatch Green Suite to AirWatch Blue Suite Upgrade – Perpetual License; Device-Based License	$44.00	
AirWatch Green Suite to AirWatch Blue Suite – Perpetual License Maintenance; Device-Based License	$8.75	
AirWatch Green Suite to AirWatch Yellow Suite Upgrade – Perpetual License; Device-Based License	$88.00	
AirWatch Green Suite to AirWatch Yellow Suite Upgrade – Perpetual License Maintenance; Device-Based License	$17.50	
AirWatch Green Suite Perpetual Device License to Perpetual User-Based License	$55.00	
AirWatch Green Suite Perpetual Device License to User-Based License Upgrade Maintenance	$11.00	
AirWatch Orange Suite Perpetual License; Device-Based License	$70.00	
AirWatch Orange Suite Perpetual License Maintenance; Device-Based License		$14.00
AirWatch Orange Suite Perpetual License; User-Based License	$140.00	
AirWatch Orange Suite Perpetual License Maintenance; User-Based License		$28.00
AirWatch Orange Suite to AirWatch Blue Suite Upgrade – Perpetual License; Device-Based License	$22.00	
AirWatch Orange Suite to AirWatch Blue Suite Upgrade – Perpetual License Maintenance; Device-Based License	$4.50	
AirWatch Orange Suite to AirWatch Yellow Suite Upgrade – Perpetual License; Device-Based License	$66.00	
AirWatch Orange Suite to AirWatch Yellow Suite Upgrade – Perpetual License Maintenance; Device-Based License	$13.25	
AirWatch Orange Suite Perpetual Device License to Perpetual User-Based License	$77.00	
AirWatch Orange Suite Perpetual Device License to User-Based License Upgrade Maintenance	$15.50	
AirWatch Blue Suite Perpetual License; Device-Based License	$90.00	
AirWatch Blue Suite Perpetual License Maintenance; Device-Based License		$18.00
AirWatch Blue Suite Perpetual License; User-Based License	$180.00	
AirWatch Blue Suite Perpetual License Maintenance; User-Based License		$36.00
AirWatch Blue Suite to AirWatch Yellow Suite Upgrade – Perpetual License; Device-Based License	$44.00	
AirWatch Blue Suite to AirWatch Yellow Suite Upgrade – Perpetual License Maintenance; Device-Based License	$8.75	
AirWatch Blue Suite Perpetual Device License to Perpetual User-Based License	$99.00	
AirWatch Blue Suite Perpetual Device License to User-Based License Upgrade Maintenance	$19.75	
AirWatch Yellow Suite Perpetual License; Device-Based License	$130.00	
AirWatch Yellow Suite Perpetual License Maintenance; Device-Based License		$26.00
AirWatch Yellow Suite Perpetual License; User-Based License	$260.00	
AirWatch Yellow Suite Perpetual License Maintenance; User-Based License		$52.00
AirWatch Yellow Suite Perpetual Device License to Perpetual User	$143.00	
AirWatch Yellow Suite Perpetual Device License to User-Based License Upgrade Maintenance	$28.50	
AirWatch K-12 EDU Suite Perpetual License; Device-Based License	$24.00	
AirWatch K-12 EDU Suite Perpetual License Maintenance; Device-Based License		$5.00
AirWatch Advanced Telecom Perpetual License – Device-Based License	$20.00	
AirWatch Advanced Telecom Perpetual License – Device-Based License Maintenance		$4.00
AirWatch Advanced Telecom Perpetual License – User-Based License	$40.00	
AirWatch Advanced Telecom Perpetual License – User-Based License Maintenance		$8.00

Professional Services, Hosting Fees, and Application Service Desk			
Description of Charge	**Monthly Charge**	**One-Time Charge**	**Annual Charge**
Shared Hosting Fee – Per Device (Perpetual)	$1.00	n/a	$12.00
Dedicated Hosting Fee – Per Device (Perpetual)	$2.00	n/a	$24.00
Application Service Desk 9x5 Per Device (Perpetual)	$0.50	n/a	$6.00
Application Service Desk 9x5 Per User (Perpetual)	$0.75	n/a	$9.00
Application Service Desk 24x7 Per Device (Perpetual)	$0.75	n/a	$9.00
Application Service Desk 24x7 Per User (Perpetual)	$1.50	n/a	$18.00
Remote Administration – Basic	$750.00	n/a	$9,000.00
Remote Administration – Advanced	$2,500.00	n/a	$30,000.00
Dedicated Hosting Set-up Fee		$10,000.00	
Dedicated UAT Environment			$10,000.00
AirWatch Hosted Basic Installation and Training		$1,000.00	
AirWatch Hosted Basic Plus Installation and Training		$1,500.00	
AirWatch Hosted Premium Installation and Training		$2,000.00	
AirWatch Hosted Premium Plus Installation and Training		$4,500.00	
Content Locker - Advanced Add-On Training		$1,000.00	
AirWatch Advanced Telecom Configuration and Training		$500.00	
VMware Identity Manager Configuration and Training		$1,200.00	
EMM Operations Training		$1,500.00	
EMM Managed Service Health Check		$1,750.00	
AirWatch PKI Integration and Identity Certificate Device Configuration		$1,750.00	
Additional ACC Implementation and Configuration		$500.00	
Additional SEG Implementation and Configuration		$1,000.00	
Additional MAG Implementation and Configuration		$1,000.00	
AirWatch Professional Services – 8 Hours		$1,200.00	
AirWatch Software Upgrade for Dedicated SaaS Deployments		$2,500.00	
AirWatch PS Custom – SOW		Custom Pricing	

User-based licenses may be applied on up to 3 devices. All prices exclude applicable taxes, fees and surcharges.

Important Information

General: VMware AirWatch Hosted as described in this product brief (the "Solution") is available only to eligible customers with a qualified AT&T agreement ("Qualified Agreement") and a Foundation Account Number ("FAN"). The Solution is subject to (a) the terms and conditions found at: https://www.vmware.com/download/eula/universal_eula.html ("Additional Product Terms"); (b) the Qualified Agreement; and (c) applicable Sales Information. For government customers, any Additional Product Terms not allowable under applicable law will not apply, and the Qualified Agreement will control in the event of any material conflict between the Qualified Agreement and the Additional Product Terms. Any service discounts, equipment discounts, and/or other discounts set forth in the Qualified Agreement do not apply to the Solution. The Solution may not be available for purchase in all sales channels or in all areas. Additional hardware, software, service and/or network connection may be required to access the Solution.

Availability, security, speed, timeliness, accuracy and reliability of service are not guaranteed by AT&T.

Except for government customers, (i) Customer must accept the Additional Product Terms as the party liable for each user of a Customer owned device, and agrees in such case that each such user will comply with the obligations under the Additional Product Terms; (ii) Customer is responsible for providing each such user with a copy of the Additional Product Terms; (iii) Customer and each such user are individually and jointly liable under those terms; (iv) Customer may not enroll users of individually owned or subscribed devices ("Individual Users") in the Solution unless it has obtained and preserves proof that each Individual User has reviewed and accepted the terms and conditions of the Additional Product terms; and (v) Customer shall indemnify and hold harmless AT&T against all claims by any Individual User relating to or arising from such use of the Solution if he or she has not accepted the terms and conditions of the Additional Product Terms. In addition, if and to the extent that users who are not residents of the United States download and use the Solution software on devices outside of the United States, Customer agrees to be subject to the Country Specific Provisions in the Solution Service Guide located at http://serviceguidenew.att.com/sg_customPreviewPDFPage?testid=068C0000001fyNEIAY.

Requirements; Technical Information: A minimum of 20 Solution licenses is required for initial order. All fees paid for the Solution are non-refundable. Customers choosing the Annual License must pay in advance and there are no refunds. Customers choosing the Monthly License pay in arrears. The Solution is available for use with multiple network service providers. For users subscribed to an AT&T wireless service, activation of an eligible AT&T data plan on a compatible device with short message service ("SMS") capabilities is required. For users of the Solution with devices subscribed to non-AT&T wireless providers, customer is responsible for ensuring that customer, its applicable end users and the Solution comply with all applicable terms of service of such other wireless carrier(s). All associated voice, messaging and data usage will be subject to the applicable rates and terms of such other wireless carrier(s). Refer to applicable wireless carrier(s) for such rates, terms and conditions. A compatible device with SMS capabilities and AirWatch software is required. The Solution's administrative interface is accessed via a Web portal and requires a PC with Internet connection. The Solution may be used as a tool to configure and customize certain settings and features and perform software updates only for compatible devices. Improper or incomplete configuration and/or downloads performed by Customer may result in service interruptions and/or device failures. AT&T does not guarantee compliance with such customized settings and/or updates. Customer will not permit any individually responsible user ("IRU") or BYOD user to register as a user of the Solution unless customer obtains and preserves proof that the IRU or BYOD user has accepted the Additional Product Terms. Upon reasonable request from AT&T, Customer will permit AT&T to review customer's records of users' acceptances. The Solution's functionality is limited to certain mobile devices and operating systems. A list of compatible devices and operating systems is available by contacting an AT&T Account Executive. Not all features are available on all devices. If and to the extent that end users who are not residents of the United States download and use the Solution software on devices outside of the United States, Customer agrees to be subject to the Country Specific Provisions in the Solution Service Guide located at: http://serviceguidenew.att.com/sg_customPreviewPDFPage?testid=068C0000001fyNEIAY , provided that government customers shall not be subject to any such terms that are not allowable under applicable law.

AT&T reserves the right to perform work at a remote location or use, in AT&T's sole discretion, employees, contractors or suppliers located outside the United States to perform work in connection with or in support of the Solution. AT&T will not provide technical support to end users and will not provide technical support for the applications and/or content that customer chooses to distribute and which are not included in the Solution's feature list. Customer will not instruct end users to call AT&T Customer Care at 611 or any other wireless carrier's customer care center in connection with end users' use of the Solution. Not all features are available on all devices. AT&T reserves the right to (i) modify or discontinue the Solution in whole or in part and/or (ii) terminate the Solution at any time without cause.

AT&T shall pass through to Customer any warranties for the VMware AirWatch software available from the licensor. VMware, not AT&T is responsible for any such warranty terms and commitments. ALL SOFTWARE IS OTHERWISE PROVIDED TO CUSTOMER ON AN "AS IS" BASIS. AT&T HAS NO DEFENSE, SETTLEMENT, INDEMNIFICATION OR OTHER OBLIGATION OR LIABILITY ARISING FROM THE ACTUAL OR ALLEGED INFRINGEMENT OR MISAPPROPRIATION OF INTELLECTUAL PROPERTY BASED ON THE SOLUTION. Except for government Customers, Customer's sole and exclusive remedy for any damages, losses, costs and expenses arising out of or relating to use of the Solution will be termination of service. All amounts paid for the Solution are non-refundable. Billing begins as of Effective Date of applicable order.

Professional Services: Upon completion of any Professional Services, customer must either sign the acceptance document AT&T presents or provide within five (5) business days of the service completion date written notice to AT&T identifying any non-conforming Professional Services. If customer fails to provide such notice, customer is deemed to have accepted the Professional Services. Customer will in a timely manner allow AT&T access as reasonably required for the Professional Services to property and equipment that customer controls. Customer will ensure that the location(s) to which access is provided offer(s) a safe working environment, free of hazardous materials and reasonably suitable for the Professional Services. The Professional Services provided will be performed Monday through Friday, 9:00 a.m. to 5:00 p.m., local time. The mandatory software installation and configuration is estimated to take two days and must be completed within 45 days of order placement. If customer's acts or omissions cause delay of installation and configuration beyond 45 days of order placement, AT&T will invoice customer for the installation and configuration charges after the 45th day. If the Professional Services provided in connection with the Solution are more complex than those described in this product brief, then a separate statement of work describing the activity and related terms and pricing will be executed. If impediments, complications or customer-requested changes in scope arise, the schedule, the Solution, and fees could be impacted.

Data: Customer Personal Data may be transferred to or accessible by (i) AT&T personnel around the world; (ii) third parties who act on AT&T's or AT&T's supplier's behalf as subcontractors; and (iii) third parties (such as courts, law enforcement or regulatory authorities) where required by law. Customer will only provide or make Customer Personal Data accessible when customer has the legal authority to do so and for which it has obtained the necessary consents from its end users, and will camouflage or securely encrypt customer Personal Data in a manner compatible with the Solution. As used herein, the term Customer Personal Data includes, without limitation, name, phone number, email address, wireless location information or any other information that identifies or could reasonably be used to identify customer or its end users. Customer is responsible for providing end users with clear notice of AT&T's and customer's collection and use of Customer Personal Data obtained via the Solution, including, without limitation, end user device location information, and for obtaining end user consent to that collection and use. Customer may satisfy its notification requirements as to AT&T by advising end users in writing that AT&T and its suppliers may collect and use Customer Personal Data by providing for end user review the relevant links to the product brief or other sales information that describes the Solution and to AT&T's Privacy Policy at http://www.att.com/gen/privacy-policy?pid=2506. Customer is responsible for notifying end users that the Solution provides mobile device management (MDM) capabilities and allows customer to have full visibility and control of end users' devices, as well as any content on them.

For more information contact an AT&T Representative or visit www.att.com/emm.

To learn more about VMware AirWatch, visit www.att.com/emm or have us contact you.

Share this with your peers

* Diagnosis and remediation of failed test cases to verify that a certificate of the correct type is issued by the Certificate Authority and installed within the device certificate store. Customer is responsible for any diagnosis or remediation of authentication or authorization failures within the authentication, authorization and accounting (AAA) infrastructure.
** Customers that have previously subscribed to the now discontinued 9x5, Silver, Gold or Platinum ASD plans should contact an Account Representative for details.
*** AT&T will not provide technical support to end users and will not provide technical support for the applications and/or content that Customer chooses to distribute and which are not included in the Solution's feature list.