VMWARE AIRWATCH RUGGED DEVICE MANAGEMENT

Enable Mobile Workers in Even the Toughest Environments

OVERVIEW

VMware AirWatch® Unified Endpoint Management (UEM) platform provides comprehensive solutions for organizations to easily deploy, provision, and secure ruggedized notebooks, tablets, smartphones, and handheld barcode scanners, alongside non-rugged deployments, from one central console.

KEY BENEFITS

- Save time and resources with low-touch enrollment and configuration
- Protect corporate data with device controls and policies
- Give workers access to mission-critical apps that drive business operations
- Assist users in the field with remote control and management tools

Why VMware AirWatch for Purpose-Built Mission-Critical Devices

Rapid Deployment | Simplified Provisioning | Remote Management

Enterprise mobility goes far beyond the corporate office to reach the devices in tough work environments such as a warehouse, manufacturing plant, oil rig, or hospital. Rugged devices are designed for business-critical operations and optimized for entering data, navigating line of business (LOB) applications or interfacing to backend systems. These devices are typically corporate owned and shared by multiple employees throughout shift schedules across all industries, including healthcare, retail, manufacturing, distribution, and transportation.

The VMware AirWatch Unified Endpoint Management (UEM) platform provides a simple yet robust solution to manage and support semi- and fully ruggedized laptops, tablets, smartphones, and handheld scanners. AirWatch supports native and OEM-specific Android, QNX and Windows CE operating systems as well as Zebra devices, including Symbol and Motorola, Honeywell devices, including Intermec and LXE, Sonim devices, and Bluebird devices, including Pidion. As the industry-leading UEM platform, AirWatch delivers comprehensive support for ruggedized devices:

- Rapid deployment and provisioning
- Device security and controls
- App delivery and user enablement
- Remote management and control

Rapid Deployment and Provisioning

When devices are deployed outside of the corporate office and away from IT, it's essential that enrollment and configuration is low-touch. AirWatch supports several onboarding options for easy and automated enrollment, including barcode scanning, side loading, and web. Upon enrollment, AirWatch enables immediate visibility into managed devices by enabling IT to track and collect critical information, such as system diagnostics, network information, certificates, internal and external apps, and IT-defined custom attributes. And with our flexible and scalable platform, deployments can be easily scaled to support a growing and diverse fleet of devices.

Configure installation of Wi-Fi, VPN and email profiles, applications, files and actions using product provisioning. Products can be delivered to rugged devices on demand, or based on a schedule or device conditions, such as Wi-Fi connectivity or battery level. Provision and deliver content to rugged devices with a local or remote relay server to decrease the network traffic load on the central server, improving your network bandwidth utilization

OUR PARTNERS

Honeywell

ZEBRA TECHNOLOGIES

SEE MORE. DO MORE.

Panasonic

sonim BUILT FOR LIFE™

BLUEBIRD Spread your wings

and maintaining positive network speeds. Enable cold boot persistence to prevent devices from downloading configurations multiple times from the admin console. For organizations leveraging third party systems for device provisioning, AirWatch provides advanced, rugged-specific API integration.

Device Security and Controls

Protect corporate data on ruggedized devices with granular device controls and policies. Enforce a passcode with complexity requirements and device encryption. With AirWatch, restrict functionality on the device such as camera, screen capture, external storage usage, Bluetooth, device tethering and more to prevent data loss. Advanced user authentication using certificate lifecycle management protects corporate Wi-Fi and VPN networks from unauthorized access. The AirWatch compliance engine monitors device compliance through IT-defined rules with escalating actions to automatically remediate with remote lock or enterprise wipe.

App Delivery and User Enablement

Business operations on ruggedized devices are primarily achieved through mission-critical applications that enable everything from accurate inventory and on-time deliveries to proper medication administration based on a patient's barcode. AirWatch supports the complete app lifecycle including sourcing or developing an app, applying security policies, deploying to devices and analyzing app metrics. Silently install both internally developed and public store applications to devices. Required app lists, app whitelists and app blacklists ensure only approved applications are installed on the device. For organizations developing internal apps, AirWatch supports three approaches: AppConfig Community, VMware AirWatch® Software Development Kit™ or app wrapping. From the admin console, admins are able to gain visibility over apps deployed to rugged devices, including the ability to view installed applications, app versions and app status on devices.

For organizational use cases such as kiosk and user-less devices, AirWatch provides IT with options to easily configure in a single or multi-app mode and prevent user access to settings with VMware AirWatch® Launcher™. Customize application access, device background, size and configuration of icons, and specify available settings. For example, configure a retail device into a product lookup kiosk or lock down a field device to the two data input apps required for the job.

Since deploying a device to each user can be cost-prohibitive and often employees leveraging ruggedized devices are working in shifts, many organizations configure a single device to be shared by multiple users. AirWatch enables a user to authenticate into a device, or check out, and then dynamically deploy the specific apps and settings for that user to the device. Once the employee is done using the device at the end of their shift, they simply check in the device and it's back to a blank state and ready for the next user. Settings can be configured across an organizational group or specific to individual users. Shared devices remain enrolled and under management during the check-out and check-in process, so devices remain secure, even when not in use.

LEARN MORE

TRY

30-day Free Trial
air-watch.com/free-trial

CALL

+1 404.478.7500

VISIT

airwatch.com

Remote Management and Control

When it comes to field workers, nothing is more important than reliable remote support. With AirWatch remote management capabilities, IT and support teams are able to easily remotely manage and maintain as well as support and troubleshoot corporate-owned, business-critical devices that remote workers need to do their job, significantly increasing productivity and reducing downtime.

- Remotely connect to any device in seconds from the AirWatch console using any web browser
- View any device's screen in real-time, in its skin, and control it with the device keypad, as if it were in your hand, or through your computer's controls and keyboard
- Resolve problems faster with immediate visibility into device, including support session history, system diagnostics, network information, installed apps and profiles, device info and more
- Notify users when their screen is visible and enable them to pause a remote session for enhanced privacy

Also perform remote actions from the AirWatch console such as send message, clear passcode, warm or cold boot, remote lock and more. If a device is lost or compromised, perform a remote device lock that only an administrator can unlock, or perform enterprise wipe or full device wipe.

vmware® airwatch®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com