airwatch®

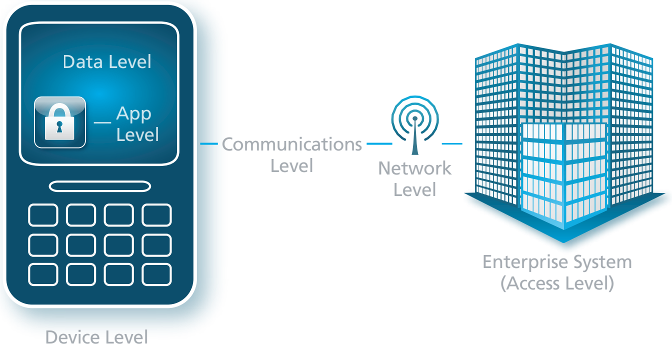
We Simplify Enterprise Mobility™

# Migrate from BlackBerry to a Secure, Multi-OS Environment

The uncertainty of BlackBerry's future has highlighted a fundamental challenge that IT professionals must face: migrating to a secure multi-OS environment. Organizations must take action soon according to Gartner, who, "Recommends that our [BlackBerry enterprise] clients take no more than six months to consider and implement alternatives to BlackBerry," said Gartner analyst Bill Menezes in an email interview with CIO.com. AirWatch® understands and addresses the challenges associated with migrating away from BlackBerry to secure, multi-OS environment, especially in highly regulated industries.

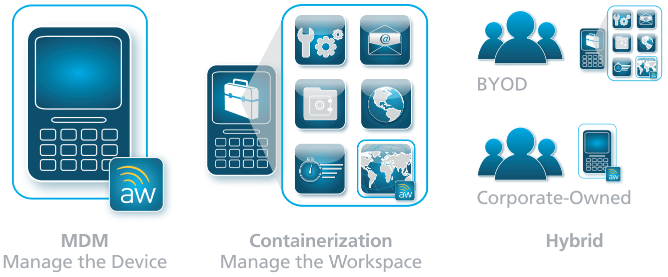
## Develop a Layered Approach to Security

AirWatch offers a layered approach to security that protects enterprise data at the device, application, communication, network and enterprise system levels. Our security framework extends across our comprehensive enterprise mobility management platform and market-leading solutions for managing devices, apps, content, email and browsing across corporate-issued and employee-owned (BYOD) mobile deployments in a single integrated console.



## Evaluate Multiple Security Approaches

With AirWatch, organizations have the flexibility to deploy multiple security approaches using AirWatch® Mobile Device Management and AirWatch® Workspace, a containerized solution for devices that are not managed with mobile device management (MDM). AirWatch Workspace allows administrators to encrypt and manage enterprise applications and data without having to manage the entire device, which is ideal for both BYOD scenarios and for sharing sensitive data in the extended enterprise. AirWatch Workspace was built from the ground up, which means administration of enterprise data on both managed and unmanaged devices is completely integrated in a central console.



## Enforce Security Across Any Platform

Multiple device types and operating systems are supported with AirWatch. From smartphones to tablets to laptops, all devices can be secured and managed from a single console. AirWatch offers same-day support for the latest software releases and enables a secure, consistent user experience across platforms and device types.

## Develop a Comprehensive Mobility Strategy

### AirWatch Workspace

AirWatch Workspace provides complete separation of corporate and personal data on a device, ensuring corporate resources are secure and employee privacy is maintained. AirWatch enables organizations to standardize enterprise security and data loss prevention strategies across device fleets through a flexible approach to containerization with AirWatch Workspace. A secure containerized solution for all enterprise data including email, applications, content and browsing, AirWatch Workspace is managed at the application level without MDM, making it ideal for BYOD and high regulation deployments.

### Bring Your Own Device (BYOD)

AirWatch provides unprecedented choices over the types of devices you manage, without compromising security. Our flexible model can support corporate-owned, employee-owned and shared devices. Centrally manage all devices, protect users' privacy, allow users basic administration and secure corporate data.

### Mobile Device Management

AirWatch allows you to gain visibility into the devices – including smartphones, tablets and laptops – connecting to your enterprise network, content and resources. Quickly enroll devices in your enterprise environment, configure and update device settings over-the-air, and enforce security policies and compliance across your entire device fleet.

### Mobile Application Management

AirWatch enables you to manage internal, public and purchased apps across devices enrolled in your organization. Distribute, update, track and recommend apps over-the-air with the AirWatch® App Catalog. Build custom internal apps with the AirWatch® Software Development Kit, or wrap existing internal applications for advanced security with AirWatch® App Wrapping.

### Mobile Content Management

AirWatch secures document distribution and promotes collaboration of corporate content anytime, anywhere in AirWatch® Secure Content Locker™. Store your corporate documents, email attachments and more in a secure container and protect sensitive files with user authentication, file encryption, geofencing, sharing limitations and offline viewing restrictions.

### Mobile Email Management

AirWatch integrates with your existing email infrastructure to deliver comprehensive security for mobile email. Control device access to corporate email, utilize AirWatch® Secure Email Gateway and encrypt sensitive data to prevent data loss. Containerize email and provide a native user experience with AirWatch® Inbox for Android™ and Apple® iOS. Open email attachments in AirWatch Secure Content Locker to maximize data loss prevention.

### Mobile Browsing Management

AirWatch® Browser is a secure browsing alternative to native browsers and provides corporations 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 for intranet sites without a device-level VPN, and enable secure browsing with whitelists and blacklists or kiosk mode.