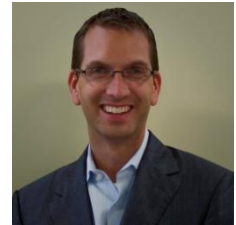




Empowering the Mobile Enterprise

Flexibility is Key in Today's Changing Industry

By John Marshall
CEO
AirWatch



The rapid evolution of mobile technology and applications (apps) is pushing enterprises to develop flexible mobility strategies so they can benefit from the industry's latest advancements. AirWatch enables this agility in enterprises with mobility solutions that provide unprecedented choices over the types of devices they deploy, their device ownership models and "build" versus "buy" deployments, without compromising the security and management of their mobile fleets.

Having this array of choice frees enterprises to focus on the strategic aspects of their mobility investments rather than getting caught up in the tactical struggles of deploying mobile technology. AirWatch empowers the mobile enterprise with the following broad array of mobile device management options:

- ***Cross-platform Support: Android, Apple iOS, BlackBerry, Symbian and Windows***

AirWatch's cross-platform solution allows end users to enjoy the mobile experience of their choice by using the device/mobile OS that they want, while meeting the IT department's requirements for policy setting, standardization and enforcement. AirWatch helps fill the gap across the various mobile operating systems by centralizing the management of security policies, settings, corporate access and apps, regardless of mobile platform, with a common interface.

- ***Device Ownership Models: Corporate, Employee-Liable or Shared***

With the consumerization of enterprise mobility and the increasing costs of supporting corporate-owned devices, many enterprises are turning to "Bring Your Own Device" (BYOD) models or a hybrid of corporate- and employee-owned programs. AirWatch provides a flexible model for asset management, distribution of profiles, security policies, integration and app deployment based on device ownership. Most importantly, AirWatch has incorporated privacy settings into these capabilities to help minimize the legal and business risk associated with these programs, while keeping personal data private and separate.

- ***Deployment Options: On-Premise or in the Cloud (SaaS)***

AirWatch offers three delivery models. Organizations can deploy AirWatch MDM on premise, either behind the corporate firewall or as a dedicated software appliance. Alternatively, enterprises can turn to a cloud model, using AirWatch in a pay-as-you-go Software as a Service (SaaS) model. Companies have the flexibility to easily transition from one model to another, as their mobile strategies, infrastructures, resources and operations evolve. Regardless of the deployment method and size, implementing AirWatch is a streamlined process because of its architecture.

- ***Highly Scalable and Multi-tenant Architecture***

AirWatch is built on a highly scalable, multi-tenant architecture and meets enterprise requirements for high availability and disaster recovery. AirWatch's multi-tenant architecture allows enterprises to uniquely manage across regions or P&Ls with various requirements for directory services, certificate authorities, corporate services, security and compliance.

2011 Mobile Device Management Challenge

• **Enterprise Integration**

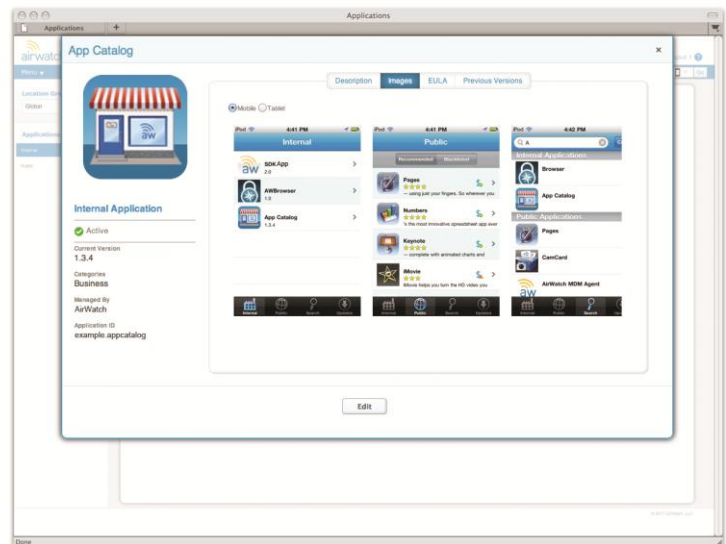
AirWatch integrates with key enterprise systems to leverage existing processes to manage users and devices. AirWatch's multi-tenant architecture makes it easy for global companies to integrate multiple authentication methods (smart cards, tokens, SAML, authentication proxies), directory services (Microsoft Active Directory, Lotus Domino and LDAP), email platforms (Exchange, Traveler, BPOS-D, Office365, Gmail), VPN clients (IPsec, Juniper SSL, F5 SSL and Cisco AnyConnect) and PKI certificate systems onto a common platform to securely manage access to corporate services and apps. AirWatch also includes an API library for integration to additional enterprise systems such as ERP, CRM, SCCM and identity management systems.

Increase Productivity through Mobile Apps

To be fully productive, mobile workers expect to use not only the latest mobile devices but also a suite of complementary apps. In addition, mobile apps have become a strategic initiative across many organizations, creating a competitive differentiator in their marketplace. As enterprises continue to leverage and develop applications that require deeper access to corporate resources and proprietary information outside the enterprise, AirWatch plays an increasingly critical role in streamlining and securing the distribution of apps, enforcing security and compliance and helping companies build apps that leverage core AirWatch functionality. We do so in the following ways:

• **App Distribution via an Enterprise App Catalog**

AirWatch's app catalog provides a simplified tool to manage, distribute and update custom-built apps without user interaction (see screen shot). Additionally the app catalog interfaces with public marketplaces to limit selection, recommend and ease distribution of publicly available apps, including apps purchased through the Apple Volume Purchase Program (VPP). Enterprises enrolled in VPP benefit from AirWatch's integrated order tracking, secure distribution of redemption codes, compliance monitoring and license management.



• **App Compliance**

Using AirWatch's advanced app compliance engine, IT administrators can define approved apps, blacklisted apps and business requirements for accessing internal apps. In the event a user violates corporate policy, IT administrators can set up automated rules to notify the user, then based on their response or time frame, initiate a corporate device wipe or full device wipe.

• **App-level Security Leveraging AirWatch's Software Developer Kit (SDK)**

AirWatch offers the industry's most developed SDK, which can be built into custom apps to enhance security with app-level passcodes, user authentication, app level certificates, encryption, compromised device detection, usage statistics and automated app lock and wipe capabilities.

Secure Corporate Assets Inside and Outside the Enterprise

Growing, complex and globally distributed mobile workforces are accessing corporate assets inside and outside the corporate network. With AirWatch, companies can enforce consistent security policies and monitor compliance across their entire mobile environment. Here's how:

2011 Mobile Device Management Challenge

• **Secure Email Gateway**

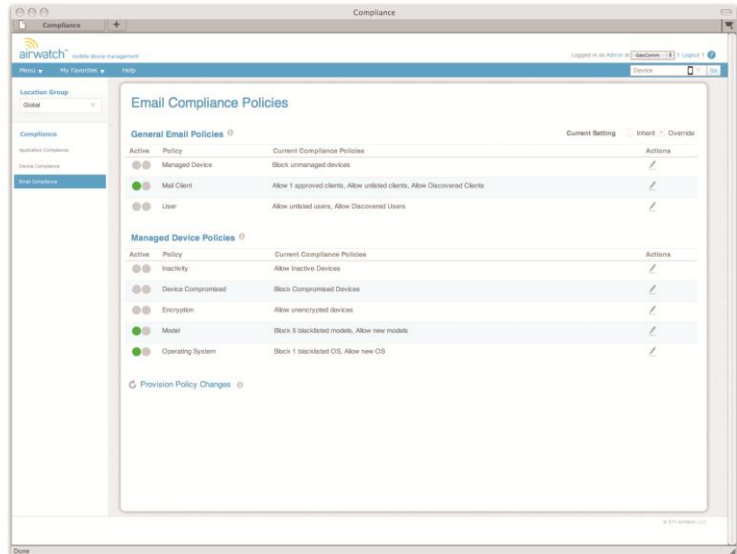
The email gateway secures corporate email by defining the business logic for device connectivity. IT administrators can allow or block mobile users, devices and classes. They can also create rule sets that require users to access mail using only approved email clients and services (see screen shot). The gateway is compatible with all deployment options, including SaaS.

• **Secure Content Locker**

The content locker provides secure storage, transfer and containerization for sensitive enterprise documents. Within the content locker application, users can access documents and receive secure updates over the air. AirWatch also prevents the transfer of documents outside the application.

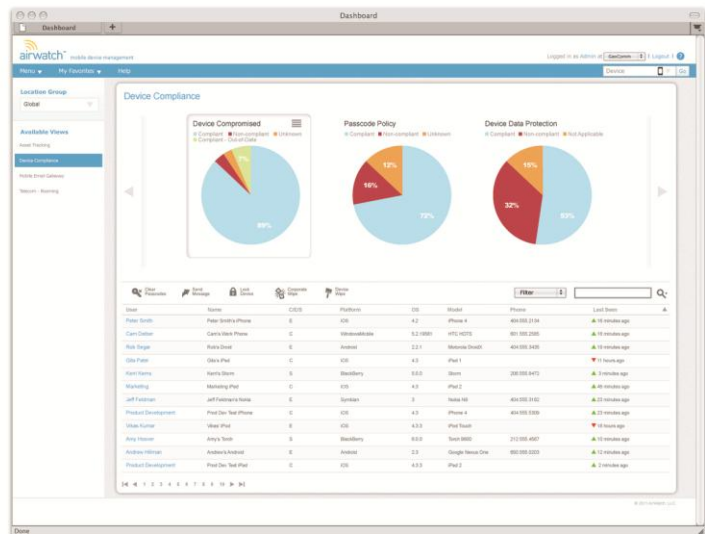
• **Secure Mobile Browser**

AirWatch's secure browser brings the same level of control to mobile browsing that enterprises have traditionally experienced on PCs. The browser provides the ability to push bookmarks to recommended sites, set allowed and blocked Web sites and restrict access to a single Web site.



Detect Compromised Devices and Comply with Policy

AirWatch can detect if a device is jail-broken or rooted through the AirWatch agent on the device or through custom apps developed with the AirWatch SDK. In the event a device is compromised, AirWatch prevents enrollment into the enterprise. If the device is already enrolled, AirWatch notifies IT operations, prohibits access to corporate services and apps and performs a selective or full device wipe. AirWatch's compliance engine can be set up based on the type of violation to take automatic action.



Empower the Mobile Enterprise

Mobility in the enterprise has quickly become all about choice and flexibility. Enterprises that control mobile users by restricting user behavior and technologies available to them will soon fall behind the competitive curve. On the other hand, those with a comprehensive mobility platform that allows freedom of choice alongside strong policy enforcement and no compromise in security and management will advance through a fully productive mobile workforce.

For more information about AirWatch solutions described here, please visit: www.air-watch.com or call AirWatch at 866.501.7705.