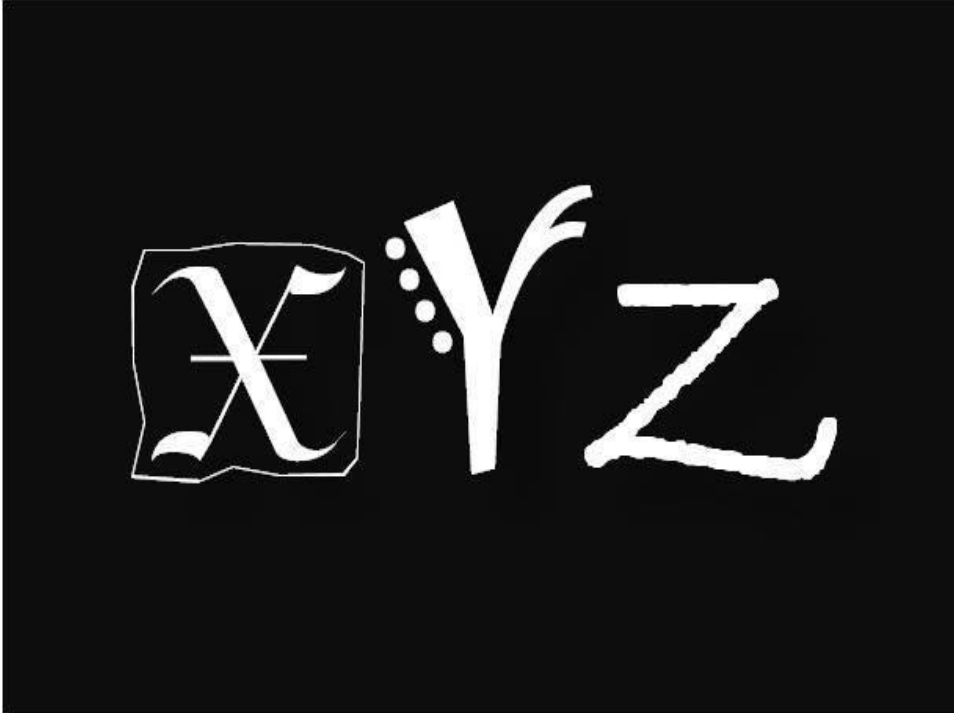


## Mobile Device Management and BYOD

An insight in a mobile device management platform and market experiences from AirWatch





## Mobility enables value, ... And risks

- ▶ Advantages of a BYOD policy
  - ▶ Reduces **costs**
  - ▶ Enables staff to work from **anywhere**
  - ▶ Increases **flexibility** of remote staff
  - ▶ Employees can meet their own demands for the most **up-to-date device**
  - ▶ Employees are more productive using devices with which they're **comfortable**
- ▶ Drawbacks of a BYOD policy
  - ▶ It's difficult to make sure all employee devices have been **registered** and updated with **remote-wiping** software
  - ▶ **Increased risk** for introducing malware to the corporate network
  - ▶ Network access must be **revoked** when no longer applicable

## Copyright © SC Magazine, US edition

- ▶ *“The first step for any organization is to develop a **mobile device management policy** that clearly articulates the expectation to privacy an employee will have if they use their own device to connect to the network.*
- ▶ *“The next step is to implement technology that enables IT to **sandbox corporate data** on an employee-owned device. In the case of an employee leaving the organization who has been using his/her own device to access the network, IT can reach out and delete all files that have been sandboxed.”*
- ▶ *As with all IT policy, it is **about what is right for the organization** within its sector, but if this is a viable problem-solver then it may be a potential light at the end of the tunnel and be responsible for a surge in secure gateway sales.*



Manu Luyten – manu.luyten@on2it.be - 0474 / 94 90 34

5



## Empower the mobile enterprise

Requirements for a BYO (mobile) D using AirWatch  
Mobile Device Management

## Achieving the full productive mobile workforce

- ▶ Mobility is all about ...
  - ▶ Choice
  - ▶ Flexibility
- ▶ Controlling mobile users is not about restricting ....
  - ▶ User behavior
  - ▶ Technology
- ▶ A comprehensive mobility platform
  - ▶ Allows freedom of choice
  - ▶ Enforces strong policies
  - ▶ Does not allow compromises in security and management



Manu Luyten – manu.luyten@on2it.be - 0474 / 94 90 34

## How to achieve the full benefit for a BYOD policy

- ▶ **Flexibility**, Key in Today's changing industry
- ▶ **Increase productivity** through mobile apps
- ▶ **Secure Corporate assets** inside and outside the Enterprise
- ▶ **Detect compromised devices and comply with policy**



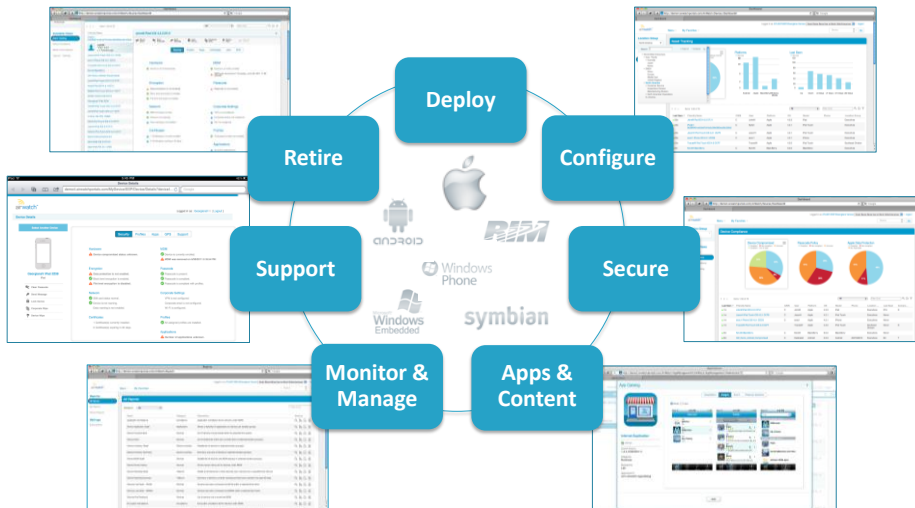
Manu Luyten – manu.luyten@on2it.be - 0474 / 94 90 34



# Flexibility is Key in Today's changing industry

And all about enabling choice




## Enabling Choice – cross platform support



## Enabling Choice – Device ownership models

- ▶ Corporate
- ▶ Employee-Liable
- ▶ Shared

## Enabling Choice – Deployment Options

Software as a Service (SaaS)	On-premise	Appliance
<ul style="list-style-type: none"> <li>▶ Multiple redundant data centers</li> <li>▶ Best of class hardware - Cisco, F5, EMC and Dell</li> <li>▶ 24 / 7 / 365 Atlanta support center</li> <li>▶ High availability (HA)</li> <li>▶ Standard SLA &gt; 99.9%</li> </ul>	<ul style="list-style-type: none"> <li>▶ Physical or virtual hardware</li> <li>▶ Single server to highly available, redundant environment</li> <li>▶ .NET, SQL architecture</li> <li>▶ Streamlined installation</li> </ul>	<ul style="list-style-type: none"> <li>▶ Tiered solutions to optimize appliance size</li> <li>▶ Industry standard hardware</li> <li>▶ Redundant hardware components</li> <li>▶ AirWatch perpetual licenses</li> </ul>
		

## Highly Scalable and Multi-tenant Architecture requirements

- ▶ Highly scalable:
  - ▶ Strong track record with deployments exceeding **50,000+** devices, growing to **100,000+**
- ▶ Meets enterprise requirements for
  - ▶ high availability
  - ▶ Disaster recovery
- ▶ Multi-tenant architecture manages users across
  - ▶ Regions
  - ▶ P & L 's
  - ▶ Various support for directory services, certificate authorities, corporate services, security and compliance

## Industry Recognition

- ▶ Positioned as a **LEADER** in **Gartner**. 2011 Magic Quadrant for Mobile Device Management Software
  - ▶ “**Multitenant support** is designed in for improved scaling, with selective isolation for large installations.”
- ▶ Identified as a **CHAMPION** in **INFO-TECH RESEARCH GROUP** 2011 Mobile Device Management Vendor Landscape
  - ▶ “AirWatch gives you the best bang for your buck.
  - ▶ Has many advanced features that other vendors do not, such as **sophisticated browser control, location services, and complex reporting.**
  - ▶ SaaS options and a low price point make AirWatch ideal for small and medium businesses.”

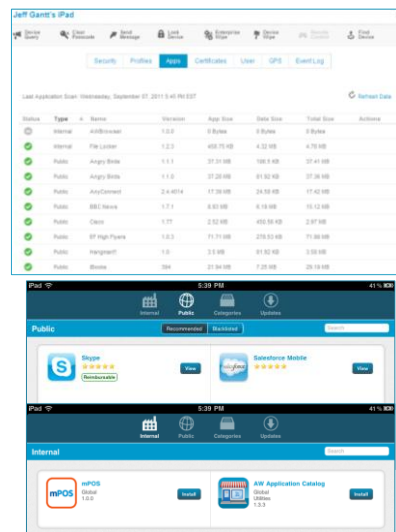


## Increase productivity through mobile apps

15

### App Distribution via an Enterprise App Catalog

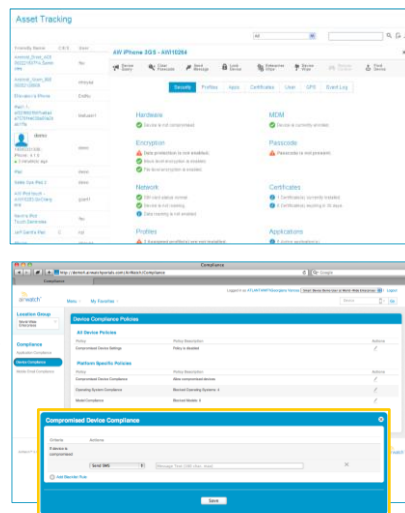
- ▶ Distribute and perform silent updates to enterprise apps
- ▶ Limit selection, recommend and ease the distribution of publicly available apps (Apple AppStore or Android Market)
- ▶ Monitor app lists (installed/not installed/out of date), app usage and data usage
- ▶ Manage app white lists/black lists and compliance policies
- ▶ Lock down devices (kiosk mode) to an IT-approved set of programs or apps
- ▶ Set up a workflow to automatically manage policy violations:
  - Notify user and/or IT
  - Disable app/corporate access (Wi-Fi, VPN, Email)
  - Selective/corporate or full wipe



Manu Luyten – manu.luyten@on2it.be - 0474 / 94 90 34

## App compliance - Secure Mobile App delivery

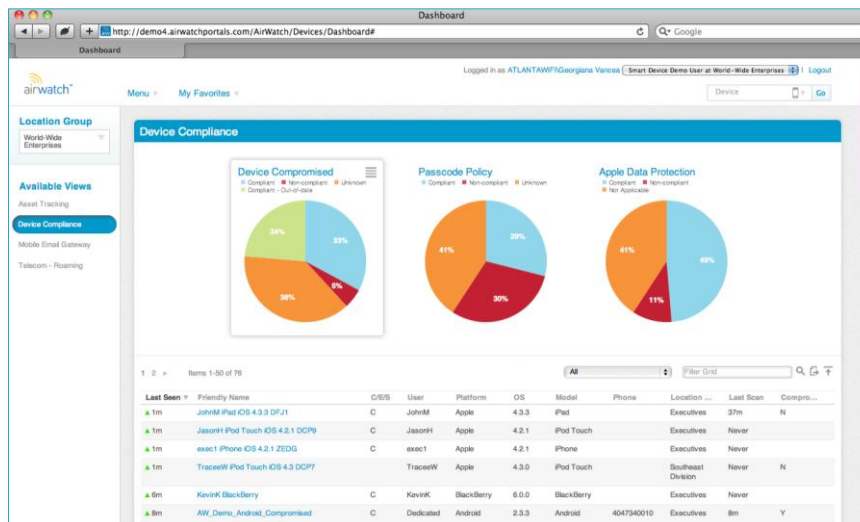
- ▶ Enterprise directory-based authentication
- ▶ SCEP/Certificate Authority integration
- ▶ Configurable device password policies
- ▶ Device data encryption
- ▶ Compromised device detection
- ▶ Secure email gateway with device level access control and policies for securing attachments
- ▶ Secure mobile web browser
- ▶ Application lock down
- ▶ Security audits, events logs and compliance engine
- ▶ Remote lock, corporate/selective or full wipe
- ▶ Configurable privacy policies for employee-liable versus corporate-owned devices
- ▶ Role-based console access with enterprise directory integration



Manu Luyten – manu.luyten@on2it.be - 0474 / 94 90 34

17

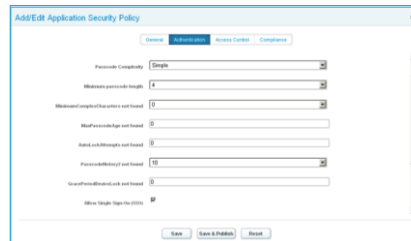
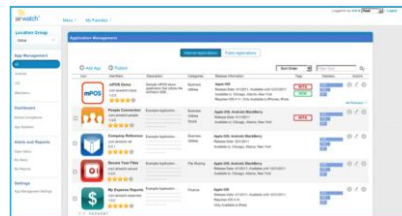
## Compliance Dashboard



Manu Luyten – manu.luyten@on2it.be - 0474 / 94 90 34

## App level security, leveraging AirWatch's SDK

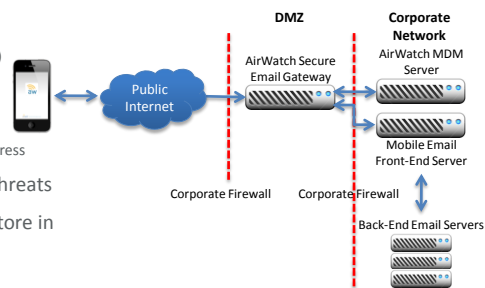
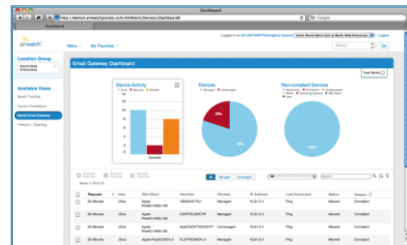
- ▶ Developer toolkit for iOS enterprise apps
- ▶ Device check-in and usage monitoring
  - ▶ Device location
  - ▶ App launch frequency
  - ▶ App usage duration
  - ▶ Data usage
- ▶ Compromised device detection with the ability to automatically wipe corporate data
- ▶ Enterprise app single sign-on with certificate or location-based authentication
- ▶ Enterprise app passcode and lock capabilities
- ▶ Data encryption for data stored within an enterprise app
- ▶ Remote wipe of corporate data based on # of failed passcode attempts or on-demand



Secure Corporate assets inside  
and outside the Enterprise

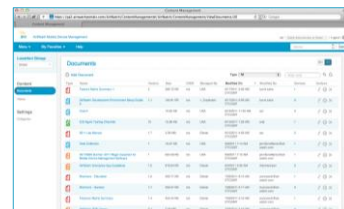
## Secure Corporate Email – Secure Email Gateway

- ▶ Allow or block devices using white lists and black lists or manually based on exceptions
- ▶ Validate devices based on:
  - ▶ Mobile user's email username
  - ▶ Mobile user's email address
  - ▶ Device serial number and OS version
  - ▶ Unique device certificate
- ▶ Monitor interactions with the email server:
  - ▶ Date and time of sync attempt
  - ▶ ActiveSync command (SYNC, PROVISION, etc.)
  - ▶ Amount of data traffic to and from the device
  - ▶ ActiveSync version
  - ▶ Device type (e.g., iPhone, iPod, iPad) & IP address
- ▶ View and filter information for exceptions/threats
- ▶ Intercept sensitive email attachments and store in a secure document viewer



## Content Locker Application

- ▶ Enable secure content management through the native content locker app
- ▶ Enforce basic, LDAP and Proxy user authentication to access content locker
- ▶ Upload content individually or in bulk and organize into categories and sub-categories
  - ▶ Document types supported: MS Office, iWork, PDF, XML, JPG, PNG, Rich text format
  - ▶ Define effective and expiration dates for each document
- ▶ Distribute content based on user role, device group or ownership
  - ▶ Define distribution method – cellular versus Wi-Fi only
- ▶ Encrypt content data



## Content Locker Application Cont.

- ▶ Manage access to content in online and offline modes
- ▶ Enable users to download content on-demand or push content automatically
  - Define download priority as high, medium and low
- ▶ Enable users to search, filter by favorites and view by most recent documents
- ▶ Track content versions and notify users when updates are available
- ▶ Detailed content visibility at the device level:
  - Content status (unknown, installed, uninstalled)
  - Content priority (high, medium and low)
  - Deployment method (on demand or automatic)
  - Content version and size
  - When the document was downloaded
  - When it was last viewed
- ▶ If a device is compromised/MDM is broken, prevent access to content locker



## Secure access to corporate applications - Secure Mobile Browser

- ▶ Whitelists / blacklists
  - Set allowed and blocked web sites, URLs, and web site categories
  - Lists can be set individually by user or device, and enforced based on location
- ▶ Bookmark provisioning
  - Push down bookmarks to enterprise recommended sites or Intranet sites
  - Bookmarks can be individualized for each user
- ▶ Kiosk mode
  - Set the browser to only allow access to a single web site
- ▶ History monitoring
  - Track web-browsing history in the console



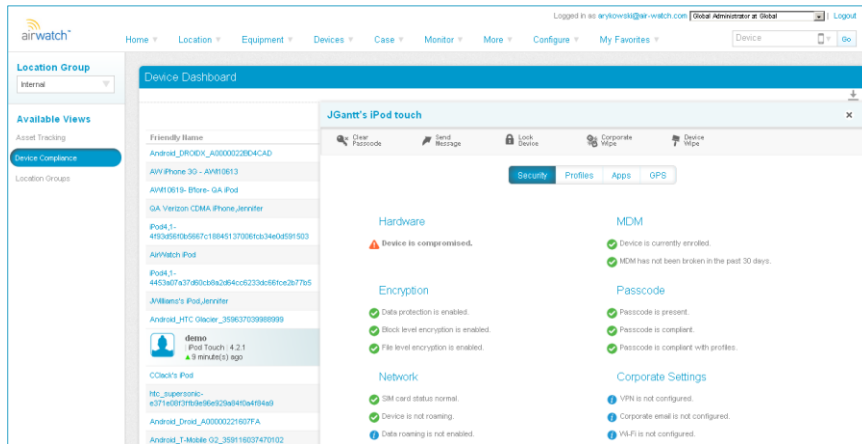
## Detect compromised devices and comply with policy

25

### Compromised Device Detection

- ▶ Detect jail-broken or rooted devices using
  - ▶ AirWatch agent
  - ▶ Custom apps developed with the AirWatch SDK
- ▶ And ...
  - ▶ Block initial authentication and enrollment
  - ▶ Prevent access to corporate resources
  - ▶ Restrict access to enterprise applications
  - ▶ On-going device compliance monitoring
  - ▶ Ensure compliance with industry regulations
  - ▶ Minimize sensitive data loss
  - ▶ Mitigate business and legal risk

# Compliance Audit



airwatch **ON2IT** SECURITY Manu Luyten – manu.luyten@on2it.be - 0474 / 94 90 34



And .....

## What about automation - Flexible Rules Engine

- ▶ Detect during device enrollment
- ▶ Detect while device is under management
- ▶ Automated compliance rules:
  - ▶ Notify user and/or IT
  - ▶ Disable corporate apps and services (Wi-Fi, VPN, Email)
  - ▶ Selective/corporate or full wipe



Manu Luyten – manu.luyten@on2it.be - 0474 / 94 90 34

## Achieving the full productive mobile workforce

- ▶ Requirements for a comprehensive mobility platform to achieve the full productive mobile workforce
  - ▶ Enable mobility by enabling choice and flexibility
  - ▶ Don't restrict user behavior nor technology in an attempt to control mobile users
- ▶ A comprehensive mobility platform
  - ▶ Allow freedom of choice
  - ▶ Enforce strong policies
  - ▶ Does not allow compromises in security and management



Manu Luyten – manu.luyten@on2it.be - 0474 / 94 90 34

## How ??????

### Architecture

- ▶ Multi OS support
- ▶ Multi-tenant
- ▶ Highly scalable
- ▶ Role-based access
- ▶ API Integration
- ▶ HTML 5 UI
- ▶ Custom branding

### Mobile Security

- ▶ Secure email gateway
- ▶ Secure content locker
- ▶ Secure mobile browser
- ▶ Compromised device detection
- ▶ Compliance rules engine
- ▶ Enterprise or full device wipe
- ▶ Privacy policies based on ownership

### SDK Library

- ▶ Single sign-on
- ▶ App passcode, lock and wipe
- ▶ App data encryption
- ▶ Compromised device detection
- ▶ App and data usage monitoring

### Enterprise Integration

- ▶ SCEP, PKI (Certificate Authorities)
- ▶ Directory services (LDAP/AD, Domino)
- ▶ Smart-card, token, SAML authentication
- ▶ Email (Exchange, Traveler, BPOS-D, Office 365 and Gmail)
- ▶ VPN (IPsec, Juniper SSL, F5 SSL and Cisco AnyConnect)
- ▶ Wi-Fi (WEP, WPA, WPA Enterprise - TLS, TTLS, EAP, PEAP)

### Configuration and Profiles

- ▶ Corporate-liable, employee-liable or shared devices with unique policies
- ▶ Automated profile distribution by user roles, groups and device types
- ▶ Certificate integration
- ▶ Shift and user-based reconfiguration
- ▶ Location-based provisioning

### Self-Service

- ▶ Registration and activation
- ▶ Device locator
- ▶ Clear passcode, lock and wipe
- ▶ Compliance audit
- ▶ Optional profiles
- ▶ App requests
- ▶ Technical support

### Flexible Delivery

- ▶ SaaS - \$3/device/month
- ▶ Software appliance - \$6,500
- ▶ On-premise - \$40/device
- ▶ Professional services
- ▶ 24/7/365 global support

### Applications

- ▶ App inventory and distribution
- ▶ HTML and native app catalog
- ▶ White lists and black lists
- ▶ Compliance engine
- ▶ Volume Purchase Program

### Mobile Intelligence

- ▶ Alerts via console, Email or SMS
- ▶ 100+ customizable reports with automated distribution
- ▶ Automated business rules to respond to exceptions or threats
- ▶ DataMart export to BI tools
- ▶ Mobile telecom management