VMware Identity Manager and AirWatch Cloud Mobile App Delivery

Five Common Challenges Customers are Facing with Cloud Mobile App Delivery

Line of business leaders can purchase SaaS apps without IT

The adoption and deployment of SaaS can be done without IT assistance on purpose, proliferating new apps and new risks of data loss

Once an organization is using three to five SaaS apps, management scale becomes a problem

A line of business might manage one or two apps, but soon, users are overwhelmed with different passwords and the helpdesk gets overwhelmed— the enterprise goes from managing one identity to 2,3,4,5, or more

Network access is no longer an effective means of access control—and passwords may not be good enough

Revoking network access in the directory used to be enough. Now it's only a part of the solution—and not all data is equal. Sometimes you need stronger authentication than just a password

Many SaaS services have both web and native mobile experiences

There has been no effective way of combining mobile app and SaaS app identity management. Existing methods require cumbersome codes and configuration that users have to navigate themselves

User expectations are rising every day

Consumer apps have raised the expectations of end users (and business decision makers) on what a good user experience should be

Delivered Two Ways

Software as a service

Operates on vCloudAir in three regions (US, EMEA, and APAC)
Massively scalable multi-tenant environment
Three "9s" SLA based on redundant physical datacenters
Requires installation of an on-premises connector
Fastest way to receive new features and updates

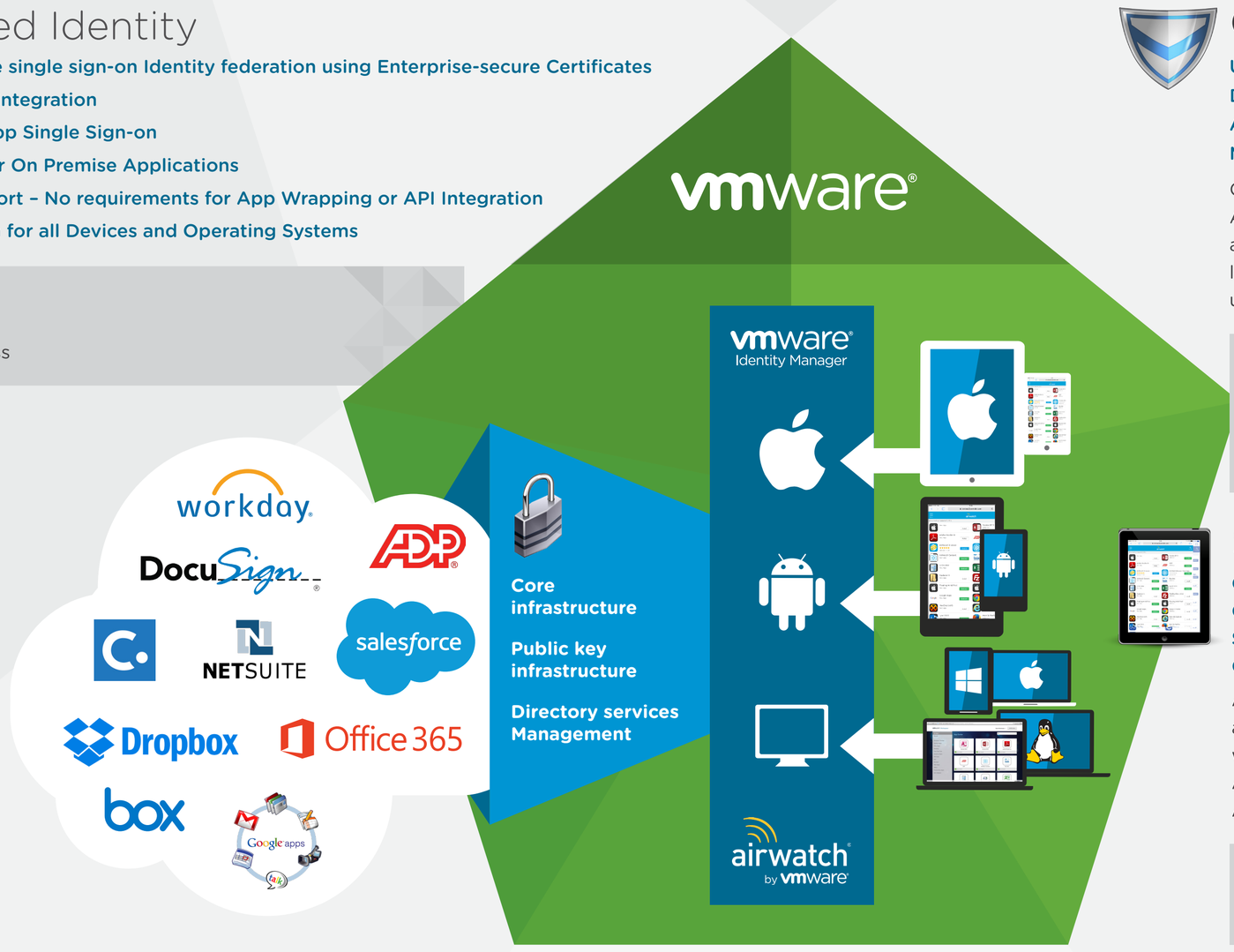
On-premises software

Delivered as a virtual appliance
Internal database makes deployment simple
Built from the same release train as cloud version (Updates are distributed less often)
Simple to build out highly available environment

Federated Identity

Secure Enterprise single sign-on Identity federation using Enterprise-secure Certificates
Active Directory Integration
Unified Mobile App Single Sign-on
Single Sign-on for On Premise Applications
Native App Support – No requirements for App Wrapping or API Integration
Optimized Log-in for all Devices and Operating Systems

Federated SSO
AD Federation
Adaptive Access



Conditional Access

User/Group
Device Type
App Type
Managed or Unmanaged Device

Optimize user experience and security with AirWatch Adaptive Access that leverages device enrollment as an additional factor of authentication (something you have) and enforcing local PIN screen lock/unlock policy (something you know) for managed and unmanaged devices.

SSO Mobile Experience
Self-service catalog
Native integration
One-touch mobile app access
(no passwords or logins required)

Secure Data on Device

Office 365 and
On-premises Exchange
SaaS Apps Data
On-premises Application Data

Allowing easier migrations and implementations to Office 365. This allows users one touch mobile access to the Office 365 environment without additional logins. Secures devices by encrypting devices using AirWatch EMM Integration and further security provided by leveraging AirWatch EMM for remote wipe of corporate data.

SSO Web Experience
Self-service catalog
Launcher

Why VMware Over Competing Solutions

Superior policy engine to improve user experience
Competing solutions set an authentication policy per application. VMware Adaptive Access can differentiate by device type and network, optimizing the user experience for iOS, Android, OSX, and Windows while maximizing security for untrusted or unmanaged devices

Eliminate app wrapping for mobile SSO
Other enterprise mobility management vendors require app-wrapping native mobile apps to be configured and protected. VMware and AirWatch support the ACE protocol that eliminates the need for wrapping and enable mobile SSO through the appropriate protocols based on device type eliminating the need to manage app lifecycle

OS neutrality and vendor relationships
Your mobility and identity management solution has to be optimized across every OS. VMware invests in relationships with all of the device and OS vendors and provides leadership in standard bodies to protect our customer's investment and to reduce complexity

In the cloud or behind the firewall
VMware Identity Manager and AirWatch enterprise mobility management are offered as cloud services or as packaged software you can install behind the firewall based on your requirements. On-premises connectors provide a bridge between your directory and the cloud

Industrial-grade enterprise architecture
VMware Identity Manager was built from the ground up on a multi-tenant cloud architecture by the industry pioneers in identity as a service. The services operate with state-of-the-art DevOps practices on vCloudAir, the same infrastructure enterprises choose for mission critical apps and disaster recovery

Optimized for VMware NSX virtual networking
As traditional perimeter security fails to protect external apps and data and leaves the core exposed once the perimeter is infiltrated, VMware NSX may be leveraged with VMware Identity Manager single sign-on and AirWatch per-app VPN to isolate and policy-manage services deep within the datacenter

Does your identity solution have the eight must-haves?

Single sign-on
Directory integration
Multi-factor authentication
Policy management
Application provisioning
Cross-device catalog and launcher
Analytics / Reporting
Meets security & compliance requirements

And does the solution have these attributes?

Mobile SSO
Leverage device-based certificate for authentication
Doesn't require application changes for SSO (no wrapping or API)
Conditional access based on managed or unmanaged devices
Optimize login experience for each OS
Automates and streamlines onboarding and revocation
Supports any type of device and OS
Support any type of application

Links and Resources

www.vmware.com/products/identity-manager

Setup and Configure in under 60 Minutes*