VMware Identity Manager and AirWatch Office 365 Migration

Five Common Challenges Customers are Facing with Office 365

Exchange

Exchange has reached its breaking point and Office 365 is the way out

A major driver of Office 365 adoption is the need to move off of on-premises Exchange architecture as scaling and managing exchange is extremely challenging, yet business-critical

Office 365 requires Azure Active Directory accounts

To implement Office 365 (Exchange Online, OneDrive, Office 365Office for mobile, etc.), an account on Azure Active Directory is required. Meanwhile, customers still require and prefer their own on-premises Active Directory as it integrates into many other business systems

Managing users in two places doesn't scale

Microsoft provides Active Directory Federation Services (ADFS) to try to bridge between the on-premises Active Directory and Azure, but most customers find this too complex and requiring too many changes to the on-premises environment. Third-party identity federation services are the best option

Proliferation of Office apps and documents on mobile devices requires more security

Adoption of Office 365 also means that access to email, apps, and files are more easily available, but that requires even more security for mobile devices.

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

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

Enterprise single sign-on
Identity federation — Allows for one or many Account management and provisioning

Provides identity and access management that applies single federated cloud identities tied to an organization's directory services. This unifies silos of user identities across applications, allowing access to on-premises Exchange and Office 365.

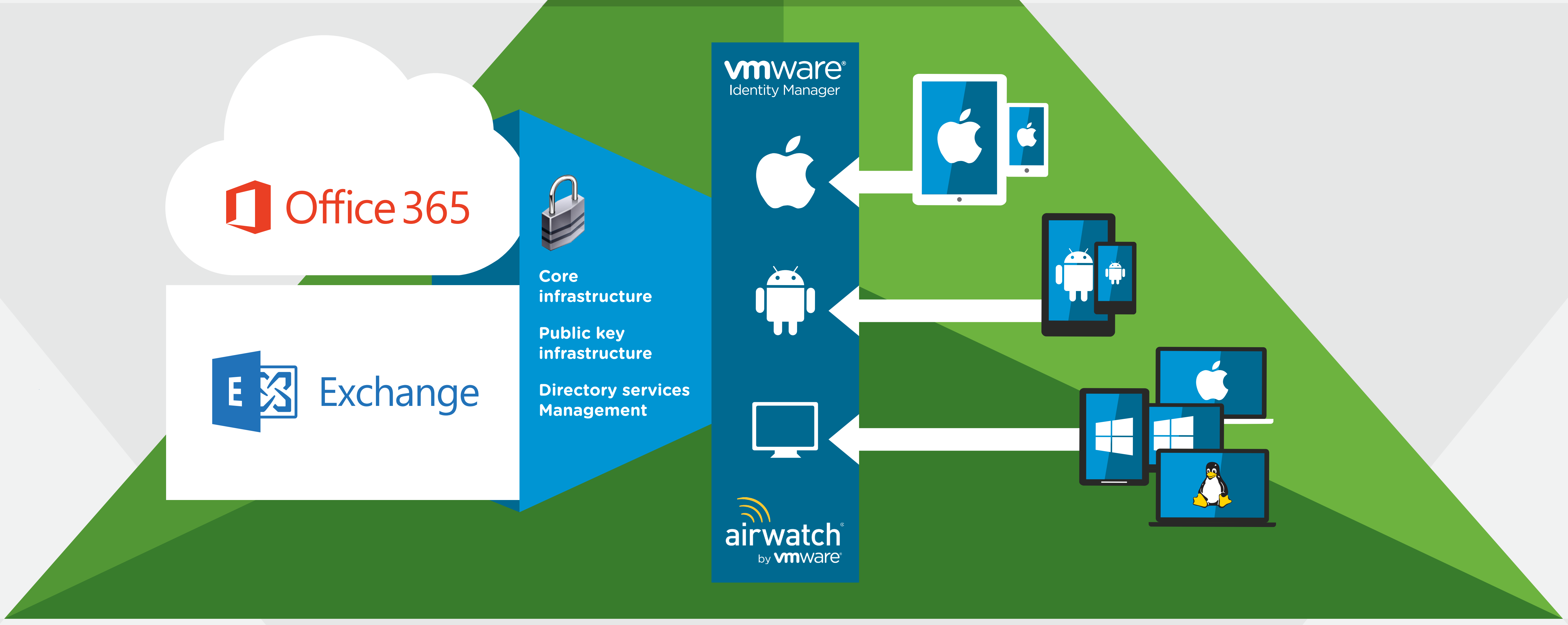
Allows integration with Active Directory services through the use of federation identities for SSO. Active Directory synchronization for changes in identities can be replicated from an organization's Active Directory. Changes sync in 30 minutes to Active Directory.

Conditional Access

User/Group
Device Type
App Type
Managed or Unmanaged Device
Domain or Network Scope

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.

vmware®



Secure Data on Device

Encrypt devices
Wipe application data

Allows IT to manage Office 365 and on-premises Exchange, 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.

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*

vmware®