Servium
delivering tomorrow's solutions today

Office 365 airwatch by vmware

vmware PARTNER ENTERPRISE SOLUTION PROVIDER

AirWatch - White Paper

Seven reasons to include AirWatch with every Office 365 migration

Tel: 0303 334 3344

hello@servium.com

Servium
delivering tomorrow's solutions today

Office 365 airwatch by vmware

vmware PARTNER ENTERPRISE SOLUTION PROVIDER

AirWatch - White Paper

Moving to Office 365 (O365) is an attractive alternative to the cost and complexities of on-premise email management. Add to this, pressure from users who demand an ever more mobile experience in order to remain productive on-the-go and it's difficult to see beyond the value adding potential O365 is capable of delivering.

However, swept along with the benefits that O365 presents, organisations often forget the considerations surrounding identity and mobile device management that accompany a migration. Without suitable measures in place, organisations will not be able to secure corporate content, especially as some O365 licenses permit users to install Office applications on up to ten different devices. Similarly, many of these devices will be mobile devices too, which present new and more difficult security challenges compared to traditional desktop apps.

We've helped a number of organisations make the move to O365 and security is always a concern. IT teams understand the security and access control mechanisms in place for on-premise email and apps, based on network and perimeter security models. Moving to the cloud however, everything changes. These models no longer work and new dynamic approaches are therefore required to ensure apps remain secure and only authorised users with compliant devices can obtain access.

The importance of Enterprise Mobility Management

Accordingly, every organisation seriously considering O365 migration also needs to be considering Enterprise Mobility Management. As far as we're concerned there are few better technologies than AirWatch for managing O365 applications on users' devices, whilst making sure those apps and the content within them are secure.

With this in mind, here are our top seven reasons for deploying the technology alongside O365:

1. Combat data proliferation across devices

O365 permits users to deploy multiple installs of the Office products across a host of devices. Whereas once corporate data only resided on a small selection of corporate owned devices, thanks to native apps it could now be on almost any device, potentially outside the control of IT policies.

Using AirWatch, only compliant devices can access O365 applications and in doing so data on the device is encrypted and policies are set to prevent data leakage, ensuring that O365 data can be remotely wiped from the device if lost or stolen. By deploying O365 apps through the AirWatch Catalog, AirWatch enforces containerisation of these applications to prevent data loss using the native platform controls. Using a variety of measures such as disabling data, sharing between business and personal apps through copy-paste restrictions and preventing email attachments from being opened in any other application other than Office, data is secured and transmission controlled.

2. Simpler access to mobile applications

To use cloud and native apps, users will need to log in to each Microsoft application. This can be frustrating for users and takes time. Instead, using AirWatch, IT teams can federate on-premise Active Directory infrastructure out to O365, therefore enabling users to use one secure, authenticated sign-on for all of their applications, regardless of the device they are using. This drives users to the AirWatch App Catalog, a web-based app deployment platform, where using their company credentials they can easily get access to all Office apps without having to re-enter credentials for each one. From here they can securely download native applications.

3. Contextual and conditional access control

Ensure only authorised users on authorised devices can access O365 services. By following the AirWatch enrolment process, trust is established between the user, device, mobile network, cloud and datacentre. Then by identifying the type of device being used, AirWatch can intelligently choose a method and strength of authentication that provides the best possible user experience while enforcing the policies set by IT. The authentication not only confirms the user identity but also validates that the device is compliant, according to AirWatch policy. If a user tries to connect to O365 from an unmanaged mobile device, access is denied.

4. Automate mobile email management

Centralising mobile email management with AirWatch can literally save weeks of manpower during O365 migration, by sending to each mobile device the necessary O365 settings and enabling automatic set up of the mail account for the user. Without this, changing user device settings becomes a highly manual task, especially if users are not savvy enough to make changes themselves. Automating in this way prevents helpdesk resources becoming consumed with repetitive support tasks to assist users with remediating problems inevitably encountered.

5. Enable self-service

Keep users happy and productive by enabling them to independently provision new devices. Self-enrolment facilities through AirWatch provide a seamless and automated experience, allowing users to set up devices quickly and begin using them securely. This also helps IT easily scale O365 across the organisation with minimal fuss.

6. Enhanced access and security

IT teams can set up conditional access to authorised users and devices. For example, policies can be established to deny jailbroken or rooted devices and administrators can even set rules for authentication based on how the user connects, such as different passwords for connection from an Android device versus a PC.

Likewise, AirWatch can also leverage digital certificates to automatically sign the user into O365, therefore providing passwordless authentication. Not only is the user experience superior, but security is enhanced by using certificates to authenticate rather than Active Directory passwords. Since AirWatch installs the certificate in a single secure location, all applications on the device can leverage this identity for authentication.

7. Remove the need for mobile OS knowledge

By using AirWatch, administrators do not need to have knowledge of every mobile operating system. Whenever Exchange Active Sync profiles are created in the AirWatch Administration Console, the process and settings remain the same regardless of the operating system. Accordingly, whenever a new device needs supporting, there is no need to determine specific device details or new settings, it simply gets supported alongside every other existing device.

Summary

In our opinion, AirWatch is the only technology that offers the robust content security and access measures businesses demand without adversely hampering the user experience. Equally, it brings noteworthy self-service opportunity and mitigates the need for high-touch IT support in rolling out O365, which both helps scale the benefits of the service and frees up precious IT resource for more demanding projects.

Any organisation looking to embark on an O365 migration would be advised to look closely at the technology. Organisations that have already made the move to O365, however, should not be deterred from exploring AirWatch solutions as there is no reason they cannot be introduced retrospectively.

Whilst this paper has discussed the relevance of AirWatch to O365, importantly the same architecture can be used to secure all company applications both cloud and on-premise, meaning investment in the technology has the potential to add value beyond the narrow application set considered here.

What next?

See it in action

Whether you're in flight with an O365 project or are simply evaluating your options, talk to one of our experts. We can arrange for a demonstration of AirWatch, or even a free trial of the technology.

To talk further email **hello@servium.com** or call **0303 334 3344**.

What is AirWatch?

AirWatch is the leader in enterprise mobility management, with a platform including industry-leading mobile device, email, application, content and browser management solutions. It provides the critical security features that are required to protect enterprise content on both corporate and employee-owned devices and ensure applications can only be accessed on managed and compliant devices.

About Servium

Servium provides IT infrastructure services for medium to large enterprises in both the private and public sector. We pride ourselves on delivering innovative solutions inspired by overcoming the day-to-day and strategic IT challenges of our customers. This is achieved by blending the best emerging technologies with professional customer service to answer these challenges and deliver economies previously not possible.

www.servium.com
Tel: 0303 334 33 44
hello@servium.com

@Servium_Ltd
www.linkedin.com/company/servium