# Introduction

Workspace one and the services that address business requirements are based on unique hybrid cloud architecture. Mobile device management and identity services are delivered via AirWatch and Vmware Identity Manager. The final key component to the architecture is a lightweight set of appliances that secure integration between cloud based and on-premises services.

Making it easier for end user to access apps increases the possibility of adoption. Workspace one provides one touch mobile Single Sign On (SSO). Mobile SSO allows user to sign in to application using their fingerprint providing password free and secure means of logging in to all apps that end user needs. Identity Manager is responsible for managing authentication using username/password, 2FA, certificate, kerberos, mobile SSO and inbound SAML from third party systems.

# Components and use cases

AirWatch => Enterprise Mobility Management

Identity Manager => Mobile Single Sign On

Workspace One => End user’s access to apps

Boxer => Secure Email app

AirWatch Browser => Secure Web Browser

Content Locker => Mobile Content Repository

Vmware Verify => 2FA [ technically multiple factory authentication ]

**Delving deeper**

Workspace one platform is comprised of Identity Manager and AirWatch. While each product can operate independently, integrating both of them is what integrates workspace one product to function. Identity Manager and AirWatch are available as either on-premises or cloud hosted solutions. Together they provide tight integration between user identity and device management.

Apart from the core components [ Identity Manager + AirWatch ] you can deploy a variety of other components depending on business need and use cases. For example: Secure Email Gateway (SEG) can be provided for secure email access while Unified Access Gateway (UAG) together with Content Locker can be used to provide secure access to corporate fileshare and web apps [ using Tunnel ].

The integration to enterprise backend is achieved through Enterprise System Connector. Enterprise System Connector is a windows based installer for 2 connectors 1) airwatch cloud connector and 2) identity manager connector.

**AirWatch Cloud Connector (ACC)** providers organizations the ability to integrate Airwatch with their backend enterprise system. It runs in the internal network, acting as a proxy that securely transmits requests from Airwatch to the internal network. This allows to integrate MDM capabilities together with user identity from LDAP and certificate authorities.

**Identity Manager** acts as a identity provider by syncing with AD to provide SSO across SAML based apps. IT is also responsible for authentication policy based on networks, applications or platform.

**Identity Manager Connector** is a windows installer packaged within Enterprise System Connector responsible for directory sync and authentication between an on-premise AD and the Identity Manager service.

**Mobile SSO** is a one touch SSO technology available for all platform that workspace one is supported on. The implementation on each OS is based on features provided by the underlying OS. For iOS it uses Key Distribution Center (KDC); for Android it uses Mobile SSO for android.

**Email Integration** is supported in 3 different ways:

1. Secure Email Gateway (SEG)
2. Powershell Integration
3. Google Apps for Work integration

SEG requires a server to be configured in the data center. Powershell communicates directly with Exchange ActiveSync on Exchance 2010+ or Office365. AirWatch integrates directly with Google services and does not need additional servers.

**Content Integration** is provided through few keys actions. First, an administrator uses AirWatch console to create , sync or enable a file repository. After configuration, this content is deployed on end user devices with Content Locker. Access to content can either be read only or read-write.

Both Identity Manager and AirWatch have their own compliance engine. When user registers their device into workspace one, it periodically sends data to AirWatch. The MDM can then run this data through compliance engine to determine the device posture. If device goes out of compliance , corresponding actions configured in AirWatch console are taken.

Identity Manager includes an access policy option that can be configured to check the AirWatch server for device compliance. Additionally, Identity Manager also has access to network the user is on, the OS they are using, or the application they are using. Identity Manager makes SSO decision based on these.

Vmware Verify is a multi-factor authentication solution that enables using an iOS, Android or Chrome Apps with a push notification, one time password, or SMS message as an additional factor when accessing resources through Identity Manager.

**Unified Access Gateway (UAG)** is a virtual appliance that allows Internet based access to internal web servers and contents.