vmware®

VMware Workspace ONE

Augment and Extend Microsoft 365

START

Microsoft 365 – Enterprise License

Which version of Microsoft 365 have you deployed?
Click to select.

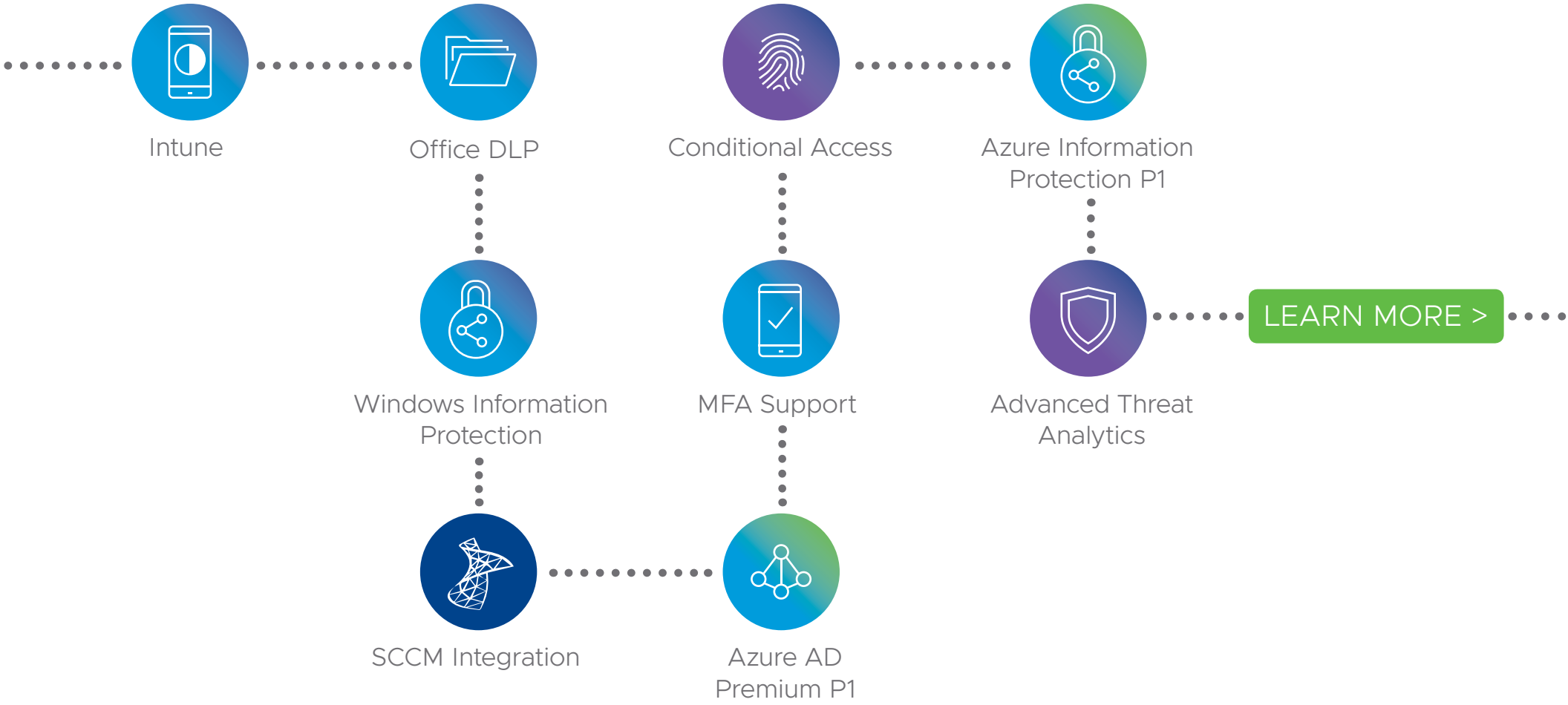
E3

E5

< BACK TO VERSION SELECTION

Microsoft 365 E3 – Understand the VMware Value

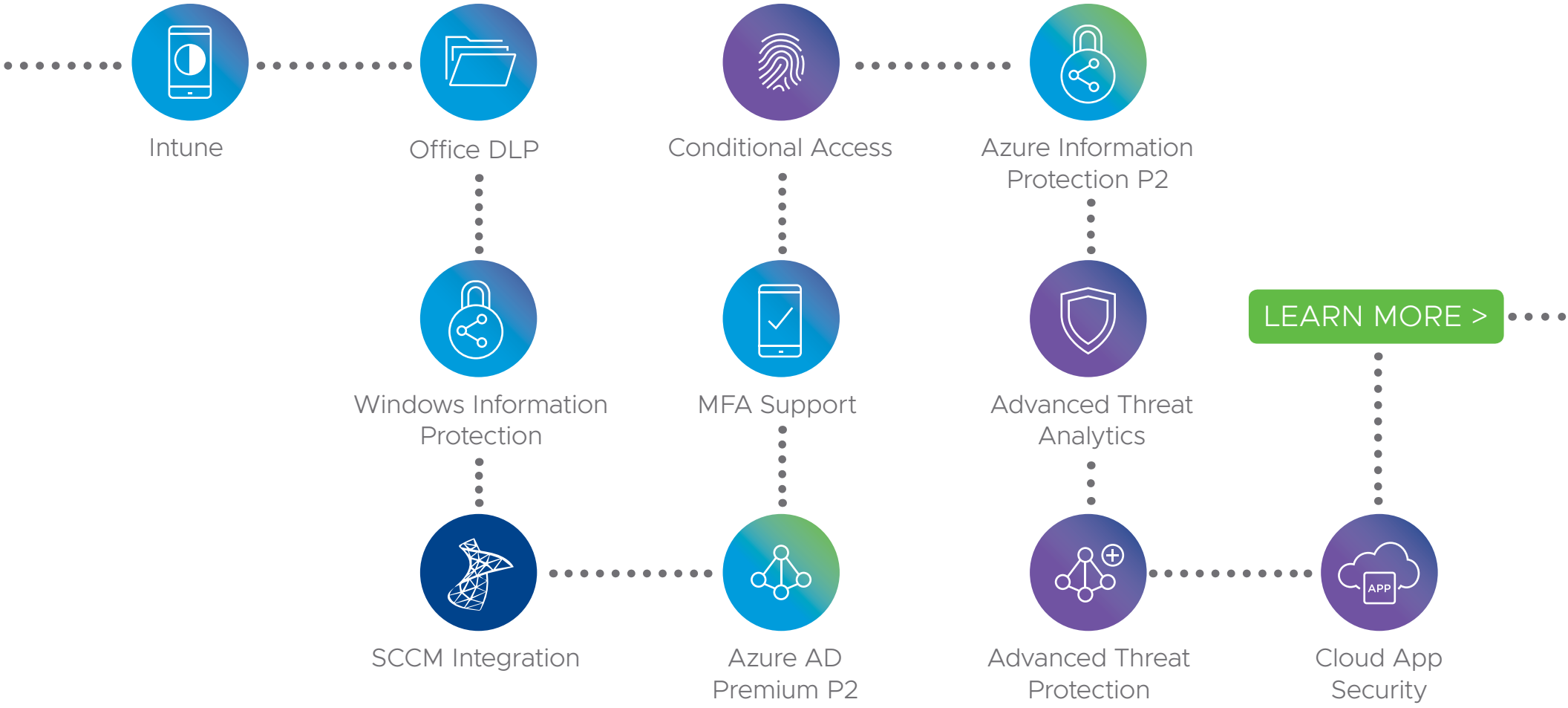
Click a topic below for more information.



< BACK TO VERSION SELECTION

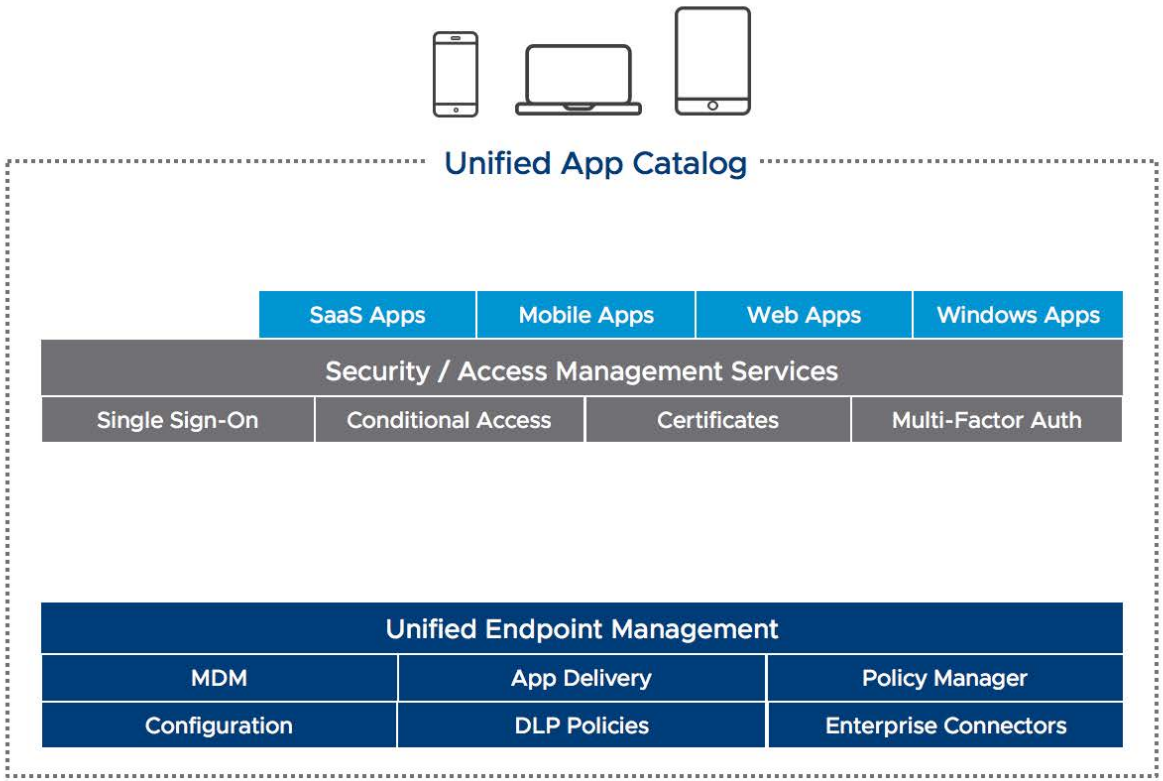
Microsoft 365 E5 – Understand the VMware Value

Click a topic below for more information.



The Digital Workspace

How a Digital Workspace is often positioned



SECTION CONTINUES

The Digital Workspace

The complete Digital Workspace

Trust Network Partners

McAfee Together is power.
Symantec
netskope
CYLANCE
Carbon Black.
Lookout
CROWDSTRIKE

Digital Workspace / Unified App Catalog

Mobile Flows + Notifications				
Content	Boxer	Secure Browser	People	
Virtual Apps	SaaS Apps	Mobile Apps	Web Apps	Windows Apps
Security / Access Management Services				
Single Sign-On	Conditional Access	Certificates	Multi-Factor Auth	
Intelligence				
Analytics	Trust Network	Automation		
Per App VPN	Unified Access Gateway	Enterprise Connectors		
Unified Endpoint Management				
MDM	App Delivery	Policy Manager		
Configuration	DLP Policies	Enterprise Connectors		

Integration Partners

Microsoft 365
slack
box
servicenow
salesforce
JIRA
Dropbox
G Suite

SECTION CONTINUES

Understanding the Value of Workspace ONE

Colleague experience and modern management

Deploy iOS, Android, Rugged Android, macOS, Chrome, and Windows 10 devices managed from a single pane of glass.

Full life-cycle application management and deployment for all supported operating systems.

Improve colleague experience with platform parity for onboarding, productivity, and lifecycle management.

Accelerate modernization of legacy applications using Workspace ONE mobile flows.

Drive business innovation by leveraging a common framework of management, security, and access.

Integration with Intune App Protection, Windows Information Protection, and Azure Information Protection.

Accelerate modern management adoption with SCCM integration for application deployment.

Gain powerful insights into end-user experience with app usage, adoption, and crash data.

Deploy and control native, cloud, and virtualized applications with identical end-user experience.

Deep integration with existing operating system DLP controls to containerize corporate data.

SECTION CONTINUES

< BACK TO VERSION SELECTION

Understanding the Value of Workspace ONE

Enhance security and secure access

Adaptive access secures data to only managed healthy devices.

Real-time reporting and analytics for patching and software updates.

Create automated remediation rules with Workspace ONE Intelligence.

Integration with service and help desk applications to provide support visibility

Seamless integration with conditional access policies to prevent access to secure data.

Create meaningful workflow to improve end-user experience through notifications.

Integration with micro-segmentation to control access to application data at the network layer through VMware NSX®.

Enhance visibility with historic data for application usage, patching lifecycle, and resource optimization.

Report at device hardware layer to interrogate the known exploits.

Integrate Intelligence with Trust Network partners to visualize, automate, and secure your devices and application data.

< BACK TO TOPIC SELECTION

Microsoft 365 – Azure AD Premium P1

VMware Workspace ONE value

VMware Workspace ONE® UEM extends the capability of Azure Active Directory (AAD) for the purposes of identity, compliance, and access with the following features:

- Integration with AAD for net-new users or synchronized users from AD
- Integrate with ONLY AAD for net-new users (not AD synchronized)
- Prevent unhealthy devices from connecting to AAD prior to authentication
- Enhanced conditional access policies for AAD P1
- Direct integration with AAD compliance flags
- Add contextual awareness with Workspace ONE Intelligence

< BACK TO TOPIC SELECTION

Microsoft 365 – Azure Information Protection P1

VMware Workspace ONE value

Workspace ONE integrates with Azure Information Protection (AIP) and Azure Rights Management (RMS), protecting documents and data by encrypting the content to only be editable or viewable by permitted recipients.

- RMS and integration with VMware Workspace ONE® Content
- Containerize email data with advanced DLP policies in VMware Workspace ONE® Boxer
- Integration with Intune App Protection policies
- Extend native email client with operating system DLP policies, for example, Open Into

< BACK TO TOPIC SELECTION

Microsoft 365 – E3 Conditional Access

VMware Workspace ONE value

VMware Workspace ONE enhances the capability of Microsoft E3 license with the following features:

- Prevent unhealthy devices from gaining access to applications
- Lock down applications based on Location and Network
- Ensure devices are patched to a minimum security requirement
- Risk-based policies and controls
- MFA support based on Location or Network
- Different policies for browser or native applications
- Understands the operating system of the device
- Integration with VMware Workspace ONE Intelligence

< BACK TO TOPIC SELECTION

Microsoft 365 – Azure AD Premium P2

VMware Workspace ONE value

Workspace ONE UEM extends the capability of Azure Active Directory (AAD) for the purposes of identity, compliance, and access with the following features:

- Integration with AAD for net-new users or synchronized users from AD
- Integrate with ONLY AAD for net-new users (not AD synchronized)
- Prevent unhealthy devices from connecting to AAD prior to authentication
- Direct integration with AAD compliance flags
- Add contextual awareness with Workspace ONE Intelligence

< BACK TO TOPIC SELECTION

Microsoft 365 – Azure Information Protection P2

VMware Workspace ONE value

Workspace ONE integrates with Azure Information Protection (AIP) and Azure Rights Management (RMS), protecting documents and data by encrypting the content to only be editable or viewable by permitted recipients.

- RMS and integration with Workspace ONE Content
- Containerize email data with advanced DLP policies in Workspace ONE Boxer
- Integration with Intune App Protection policies
- Extend native email client with operating system DLP policies, for example, Open Into

< BACK TO TOPIC SELECTION

Microsoft 365 – Advanced Threat Protection

VMware Workspace ONE value

Microsoft Azure Advanced Threat Protection (ATP) detects suspicious activities, primarily for the Windows operating system ATP, and requires third-party solutions for iOS, macOS, and Android. Workspace ONE Intelligence includes:

- Support for iOS, macOS, Windows 10, and Android
- Prevent unhealthy devices from accessing corporate resources
- Protect, detect, and remediate against malware
- Automatically ingest data from Trust Network Partners
- Security footprint that operates at every level, for example, OS, network, apps
- Audit application consumption and trend analytics
- Remediate risk through automated patching and software updates
- Integration with Trust Network Partners (CASB, malware, networks)

< BACK TO TOPIC SELECTION

Microsoft 365 – Cloud App Security

VMware Workspace ONE value

Workspace ONE Intelligence extends your CASB and malware infrastructure to ingest data from third-party vendors. Create effective automation rules to remediate issues in real time to ensure only healthy devices can connect to your cloud and on-premises applications.

- Support for iOS, macOS, Windows 10, and Android
- Prevent unhealthy devices from accessing corporate resources
- Protect, detect, and remediate against malware
- Security footprint that operates at every level, for example, OS, network, apps
- Audit application consumption and trend analytics
- Remediate risk through automated patching and software updates
- Integration with Trust Network Partners (CASB, malware, networks)

< BACK TO TOPIC SELECTION

Microsoft 365 – E5 Conditional Access

VMware Workspace ONE value

Conditional access permits the ability to consume traditional and cloud applications based on a variety of conditions such as Location, User, Device Health, and Risk.

VMware Workspace ONE enhances the capability of Microsoft E5 license with the following features:

- Prevent unhealthy devices from gaining access to applications
- Ensure devices are patched to a minimum security requirement
- Different policies for browser or native applications
- Create policies based on the operating system and management vs. unmanaged
- Integration with VMware Workspace ONE Intelligence

< BACK TO TOPIC SELECTION

Microsoft 365 – Microsoft Intune

VMware Workspace ONE value

VMware Workspace ONE provides extensive MDM support across a variety of operating systems and manufacturer APIs including:

- Manage Chrome OS and Chrome widget devices
- Broader support for Android rugged with deep API integration with vendors such as Samsung, Zebra, and Honeywell
- Native full application lifecycle management for macOS includes script support
- macOS compliance integration for device health and posture
- Support for wearables, for example, Google Glass, printers, and SLED devices
- Windows 10 over-the-air factory reset with apps (Device Guard)
- Native application deployment (Win32) without repackaging
- Sensors integration for device queries (Windows, macOS)

< BACK TO TOPIC SELECTION

Microsoft 365 – Azure Multi-Factor Authentication

VMware Workspace ONE value

VMware Workspace ONE helps to ensure that your data and applications are secure by leveraging industry-standard multi-factor authentication (MFA) solutions including:

- Support for any RADIUS or SAML-based MFA product, for example, RSA
- Integration with Azure multi-factor authentication
- Take advantage of existing deployed MFA products
- Enhance traditional MFA with policies based on:
  - Device ownership, for example, BYO vs. corporate
  - Target application and location
  - Device health and patch level
  - Integration with Workspace ONE Intelligence

< BACK TO TOPIC SELECTION

Microsoft 365 – Advanced Threat Analytics

VMware Workspace ONE value

Microsoft Advanced Threat Analytics (ATA) is designed to protect only on-premises systems from multiple types of security attacks and vulnerable systems based on compromised credentials. Workspace ONE enhances this capability to both on-premises and cloud systems:

- Secure both on-premises and off-premises devices
- Prevent unhealthy devices from connecting to on-premises infrastructure
- Over-the-air patch deployment for known security vulnerabilities
- Automated NIST CVE rules to protect cloud and on-premises systems
- Integration with existing help desk solutions to provide first line awareness
- Keep users up to date regarding the latest patches and common vulnerabilities
- Leverage the VMware Trust Network Partners to protect against 0 day exploits
- Utilize adaptive management to secure confidential data access

< BACK TO TOPIC SELECTION

Microsoft 365 – Office DLP Controls

VMware Workspace ONE value

Intune App Protection protects corporate data on mobile devices. This applies to the Office Application suite. Workspace ONE manages Intune App Protection policies alongside existing operating system DLP controls such as "Open Into" in iOS.

- Integration with Microsoft Graph API
- Single console for Intune App Protection policies
- Prevent users from being able to back up corporate data
- Restrict actions such as copy and paste
- Ensure app data is encrypted
- Allow only approved data storage locations
- Restrict web content to managed browser
- Integrates with existing OS-level DLP controls, for example, native email to Microsoft Word

< BACK TO TOPIC SELECTION

Microsoft 365 – Windows Information Protection

VMware Workspace ONE value

Built for Windows 10, Windows Information Protection (WIP) ensures that corporate data cannot be shared in unauthorized applications. VMware Workspace ONE integrates seamlessly with Windows Information Protection:

- Encrypt data with your corporate certificates
- Prevent accidental data leakage via third-party apps
- Extends to personal devices such as home PCs and laptops
- Identify and classify corporate data
- Integration with Azure rights management
- Separation of corporate and personal data
- Ability to enterprise wipe corporate data

< BACK TO TOPIC SELECTION

Microsoft 365 – SCCM Integration

VMware Workspace ONE value

Microsoft System Center Configuration Manager (SCCM) is designed to manage Windows, macOS, Unix, and Linux systems. VMware Workspace ONE® AirLift™ integrates with SCCM to synchronise collections, devices, and applications to Workspace ONE UEM:

- Remove costs associated with deploying applications with two technologies
- Hybrid mode to support existing Windows 7 and 10 systems managed by SCCM
- Silently deploy Workspace ONE UEM to existing Windows 10 devices
- Patching support via WSUS or Windows Updates as a Service
- Reporting and real-time analytics
- Pre 1710 Support for older versions of SCCM and Windows 10
- SCCM 2012 R2+

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com