

# Protect Microsoft Office 365 content with MaaS360



Microsoft Office 365 offers a user-friendly, fast and collaboration-friendly suite of applications (apps), which can be used on any device from anywhere. **However, there may be better solutions for securing Office 365 content than going “all-in” with Microsoft’s mobility, endpoint and identity management tools.**

Scroll onward and see:

- Common industry misperceptions—debunked
- Ways to secure Office 365 apps
- How IBM® MaaS360® with Watson™ can help you achieve your goals—with capabilities that far exceed those offered solely by Microsoft Intune



## Myth #1:

“To secure Office 365 on all our devices, we need to go ‘all-in’ with Microsoft.”

## It’s *not* all or nothing:

MaaS360 offers proven and robust built-in capabilities for managing devices running Office 365, supporting the complete ecosystem of Microsoft business products, including Microsoft Exchange, Microsoft SharePoint, Microsoft OneDrive for Business, Windows File Share, the Office 365 suite and Skype for Business.

**MaaS360 enables you to secure Office 365 apps and content on your smartphones, tablets, laptops and desktops.**

- Create, manage, deploy and assign policies, including Intune Mobile Application Management (MAM), to Office 365 apps with the Microsoft Graph application programming interface (API)
- Manage Copy/Paste and Save-In for Office 365 apps
- Secure access to SharePoint and OneDrive for Business content
- Establish conditional access, single sign-on (SSO), identity federation and multi-factor authentication
- Enable a secure document-editing experience across Office 365 apps
- Auto-quarantine ActiveSync-connected mailboxes based on policy and compliance

**Here’s what you can do *without an Intune license*:**

| If you need a way to...  | MaaS360 enables you to...  |
|--|--|
| Offer email, calendar and contacts on devices with auto-quarantine | <ul style="list-style-type: none"> <li>• Deploy secure mail</li> <li>• Enforce persona policies that enable connectivity to Office 365</li> <li>• Add certificate support for multi-factor authentication</li> </ul> |
| Offer mobile productivity tools                                    | <ul style="list-style-type: none"> <li>• Deploy content management controlled by persona policies</li> </ul>   |
| Provide content access using SharePoint and contain data           | <ul style="list-style-type: none"> <li>• Push a document container and/or secure browser</li> </ul>  |
| Stop data leakage from Office 365 apps                             | <ul style="list-style-type: none"> <li>• Apply content management data loss prevention (DLP) policies</li> </ul>   |



## Myth #2:

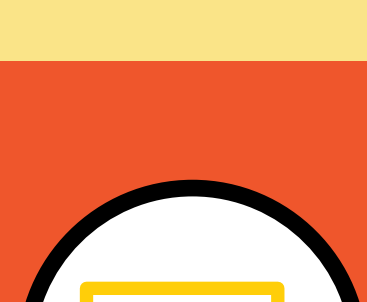
“Intune is free. I don’t need to buy mobile device management (MDM), enterprise mobility management (EMM) or unified endpoint management (UEM).”

## The “free” that may not include what you need:

Intune doesn’t support modern-day use cases beyond basic MDM and MAM. Of those that it does support, many demand an extra cost. MaaS360 satisfies modern enterprise use cases for endpoint and mobile.

**The following and more are available in MaaS360 basic packaging. Intune will either charge more for these features or does not have a way to support them.**

- **One window** to manage all of your smartphones, tablets and laptops
- **Patch and update management** for PCs and Apple Macs
- **Cognitive insights and contextual analytics** offered by integration with Watson
- **SSO and conditional access** to enterprise resources and apps like Office 365
- **Fast and easy deployments** for Apple iOS, Google Android and Microsoft Windows 10
- **A single, secure container** for email, app and content access, and DLP
- **Native-like app catalog experiences** for all major device platforms
- **Integration** with existing, non-Microsoft IT enterprise systems



## Myth #3:

“For strong identity management, I need to migrate to Microsoft Azure Active Directory and Microsoft identity solutions.”

## With MaaS360, there is no identity crisis:

MaaS360 provides seamless integration with Azure Active Directory, and robust identity and access management capabilities are available as a standard offering.

**Work with Azure Active Directory for directory integration, SSO and federation.**

Full Azure Active Directory integration helps you easily manage group memberships and policies with identity management solutions, including SSO and federation. And MaaS360 can be configured as your Office 365 identity provider to establish conditional access, including identity-based application entitlement, helping you block unmanaged devices or devices connecting to Office 365 services.

## GET THE BEST OF BOTH

Combine Office 365, Intune MAM and best-of-breed UEM to secure and manage your Office 365 apps and entitlements. Office 365 offers enterprise-grade collaboration and productivity across all endpoints. MaaS360 delivers mature, highly accredited, industry-leading UEM. So, use them in conjunction to satisfy all of your use cases.