IBM MaaS360 with Watson for Microsoft Windows 10

Enable cognitive unified endpoint management with the latest Microsoft operating system

Highlights

- Employ broad platform and operating system support to manage the full range of user endpoints
- Provide privileged identity management for data and application (app) access
- Use lockdown features to provide secure access for unprivileged users, or users with limited or short-term privileges
- Set and document security policies and distribute to users, groups or devices
- Manage apps by providing a sophisticated, unified app catalog or portal for users
- Deploy robust security features, including an IBM® MaaS360® Secure Browser for Microsoft Windows

Today's end-user devices comprise all form factors—everything from smartphones and tablets to laptops and desktops. They also cross all platforms, including Apple iOS and Apple macOS, Google Android, and every flavor of Microsoft Windows. Those versions include Microsoft Windows XP, Microsoft Windows 7, Microsoft Windows 8, and the latest releases of Microsoft Windows 10 and Microsoft Windows 10 Mobile. And the device landscape is ever-changing.

While many organizations long ago standardized on Windows 7 for laptops and desktops, an increasing number are moving to Windows 10. Studies show, in fact, that Windows 10 is now running on more than 500 million devices.[1] Why the change? In some cases, it's a normal part of the hardware upgrade process. In other instances, organizations are planning to migrate to Windows 10 as the end of extended support for Windows 7 approaches in 2020.[2] Organizations are also adapting to device form-factor change. Windows is now available on Microsoft Surface devices and original equipment manufacturer (OEM) touchscreen devices. Adding to the complexity, many are finding themselves supporting a wide range of devices on various operating systems.

IBM MaaS360 with Watson™, a cognitive unified endpoint management (UEM) solution, can help IT organizations face the challenges that today's divided endpoint landscape presents. It provides an intelligent single solution for deployment, management, security and monitoring of end-user devices, from Windows 7 desktops to the latest Windows 10 tablets—and everything in between.

Unify management with MaaS360

Because of the variety of form factors and platforms in use today, management of end-user devices in this divided landscape can require multiple point solutions that may or may not integrate, a situation that can increase security risk, create gaps in visibility and complicate management.

While some vendors offer only incomplete Windows support, MaaS360 supports Windows 7, Windows 8, Windows 10 and Windows 10 Mobile. And while other vendors also offer incomplete platform support, MaaS360 with Watson delivers cognitive UEM for iOS, Android, Windows and macOS devices. To manage the full gamut of device form factors and their associated operating systems, MaaS360 delivers client management functionality, application programming interface (API) management, or a combination of the two.

MaaS360 with Watson provides mobile device management (MDM), enterprise mobility management (EMM), and a comprehensive, cognitive UEM solution that addresses the pains of managing a heterogeneous pool of end-user devices, including those in bring-your-own-device (BYOD) environments. The solution gives IT and security leaders the power to see what happened, what can happen, and what should be done, all in the context of their environment. As organizations move to Windows 10, MaaS360 helps facilitate the transition by providing a single platform that brings all services under one management umbrella, eliminating dependencies on numerous point solutions.

Manage all types of end-user devices

Microsoft has provided APIs in an MDM style, making it much easier to onboard, manage and secure Windows 10 devices than with traditional client management tools. Now IT can simply support Windows 10 devices in the same way they manage iOS, macOS and Android devices.

IBM has the broad platform support required to help organizations manage end-user devices, while providing visibility into endpoints across the enterprise and facilitating the transition to Windows 10. MaaS360 leverages the best of both worlds by supporting the modern Windows 10 APIs as well as traditional client management tools for agent-based patching, operating system updates, and software distribution and configuration.

MaaS360 supports a wide range of management actions on Windows 10 devices enrolled via MDM, including Locate, Wipe, Selective Wipe, Change Policy, Reboot, Remove Control, Hide, and Request Data Refresh. MaaS360 also enables IT organizations to define maintenance windows and integrate IBM BigFix® to provide Microsoft security patches and updates along with updates to common Windows apps.

Manage identity and access across devices

The identity and access technology of MaaS360 represents a shift from a device-based context to a user-based context—one that takes multiple data points into account, including the user's identity, the data and apps they're accessing, and information about when they are accessing assets. It also represents a shift toward conditional access to enterprise assets, such as through integration with Microsoft Azure Active Directory.

In addition, MaaS360 provides privileged identity management capabilities for more secure access to apps and data such as mail, contacts and calendars. These capabilities include:

- Simplified and unified configuration for large rollouts across form factors
- Easier swipe- and gesture-based actions
- Easy access to folders
- Secure attachment viewing

MaaS360 gives you the ability to identify individual users, the device they are using, their location, and their access permissions for enterprise assets, apps and proprietary data.

IT administrators can also use lockdown features to provide secure access for users who do not have privileges or for users with limited or short-term privileges. An account designed to present a persistent locked-down state can be configured, too, in order to create a kiosk-type experience. When a device is accessed using the locked-down account, the device displays only the app that you specify.

Manage data and apps

With MaaS360, you can set security policies for documents and distribute them to users, groups or devices. Documents can be version-controlled, audited and secured through data loss prevention (DLP) and other options, such as Microsoft Windows Information Protection policies and app whitelisting and blacklisting via AppLocker on Windows 10 devices. MaaS360 also supports integration with Microsoft SharePoint, Microsoft Windows File Server and Microsoft OneDrive.

MaaS360 helps IT organizations manage apps by providing a sophisticated, unified app catalog or portal for users. This self-service app catalog can be used to provision all types of apps, including web and desktop apps, whether they are private or public, new or legacy, departmental or enterprise-wide.

Fine-grained app controls ensure that organizations allow only trusted apps to be accessed via the catalog. Specific apps can be blacklisted to boost security while still protecting privacy. App upgrades can be delivered to users as soon as they are available, helping to increase app security by facilitating the timely distribution of fixes.

MaaS360 unified app catalog support extends to Windows 10, allowing users to choose which apps they wish to install and when they want to install them. The app catalog supports APPX-format Universal Windows Platform (UWP) apps and bundles from Windows Store, installer packages (.MSIs) and executable files (.EXEs), in addition to home-grown apps. The apps available through the catalog can be featured, searched for, or sorted for easy user access.

Enhance security while boosting productivity

MaaS360 provides a robust collection of security features, especially for Windows 10 devices, including a MaaS360 Secure Browser and adaptive Windows 10 policies that cover pass-codes, device and network restrictions, ActiveSync and other security settings.

Your information protection needs

Device protection	Data separation	Leak protection	Sharing protection
Protect system and data when device is lost or stolen	Contain work apps, documents, and data, separating from personal device content	Prevent unauthorized users and apps from accessing and leaking data	Protect data when shared with others or shared outside of organizational devices and control

Providing security for data and apps is a critical function of an effective endpoint management solution.

MaaS360 helps IT administrators manage Windows 10 security policies, including:

- Security policies regarding encryption, unlocking and un-enrollment
- Restriction policies limiting the use of cameras, Cortana, location and telemetry, and more
- Network restriction policies such as for Wi-Fi, Bluetooth, data roaming and VPN
- ActiveSync policies such as for sync domain, contents, frequency and logging
- App whitelists/blacklists for desktop apps and UWP apps

Why IBM?

While alternative solutions provide incomplete coverage across computing platforms, MaaS360 delivers cognitive UEM across all endpoint types including smartphones, tablets, laptops, desktops, devices designed for the IoT, ruggedized devices and wearables. And while competing solutions provide incomplete coverage of Windows devices, MaaS360 can support the full spectrum, from Windows XP SP3 to Windows 10.

Traditional mobile device management systems were built in a simpler time for tactical purposes and disparate mobility projects. With the industry's first cognitive UEM platform, MaaS360 delivers a single, strategic productivity and security solution with powerful insights and analytics from Watson technology, IBM X-Force® Exchange threat intelligence and cloud-sourced benchmarking data from its platform to help drive your organization's digital business transformation.

For more information

To learn more about IBM MaaS360, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/maas360

[1] Tom Warren, "500 million machines are now running Windows 10," *The Verge*, May 10, 2017. https://www.theverge.com/2017/5/10/15604374/microsoft-windows-10-500-million-devices

[2] Microsoft Support, "Windows lifecycle fact sheet," *Microsoft*, January 2016. https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet

IBM Security
New Orchard Rd
Armonk, NY 10504

Produced in the United States of America
June 2017

WGD03112-USEN-00