IBM Security MaaS360 with Watson

Manage your organization's laptops with modern device management

Highlights
Manage devices with Windows

Manage devices with macOS

Manage patches

Manage device compliance and security

Thanks to modern hybrid work models, an increasing variety of devices and evolving cyber threats, administrators are being challenged to work with and synchronize separate applications. Modern unified endpoint management (UEM) solutions include laptop management and, as pointed out by IDC in their Worldwide UEM Software Vendor Assessment for 2022, "while UEM platforms today mostly manage smartphones and tablets, laptops and PCs (both Windows and Mac), as well as emerging Google Chrome OS devices, are increasingly critical for management with UEM."[1]

IBM Security® MaaS360® with Watson® combines and unifies modern device management and traditional client management to offer a robust, easy-to-use offering affecting key aspects of Windows and Mac devices. This solution is designed to help organizations improve their ability to enroll, configure, manage and report on laptops running macOS and Microsoft Windows alongside smartphones and tablets. With MaaS360 with Watson, organizations can extend the portal to become a hub for automated functions that are standalone or integrated with other management tools. This can help administrators maintain consistent security policies and profiles for both corporate and user-owned devices.

Manage devices with Windows
With more than 15 years of experience in delivering Microsoft solutions, MaaS360 is designed to help companies manage, integrate and extend their Microsoft ecosystem with the rest of their technology stack. MaaS360 covers multiple use cases of enrollment and management for Microsoft Windows 10 and 11.

Some of the main highlights of using IBM Security MaaS360 with Watson to help manage and protect laptops running Windows OS include:

- A new Windows 10+ device enrollment workflow that allows device users the option to enroll laptops running all editions of Windows 10 into the MaaS360 portal, thanks to the modern management capabilities built on the Windows 10+ mobile device management (MDM) APIs.
- The integration with Windows Out of Box Experience (OOBE) allows administrators to automatically enroll Windows devices into MaaS360 when a user registers with Microsoft Azure Active Directory (AD).
- Integration with Microsoft Azure AD, which allows administrators to pre-configure and enroll Windows endpoints with Windows Autopilot.
- The automated enrollment of a large quantity of Windows 10+ devices into the MaaS360 portal using the Windows 10+ bulk provisioning tool.
- The combination of mobile management and client management tools, such as Microsoft Endpoint Configuration Manager, allows IT administrators to have one single point of control for all laptops, desktops and mobile devices available in their organization.
- Real time actions such as start, stop, and restart services, which allow administrators to perform commands to reboot, locate, message and lock devices.
- Reports on hardware and software inventory showing Windows Store Apps, including APPX package formats and Win32 applications.
- A listing of existing endpoint security software, including versioning and latest service status.
- For customers who still use Windows 10+ devices that are enrolled in DTM mode, which is a traditional agent-based management that is best suited for Windows 7, MaaS360® now provides modern management capabilities built on the Windows 10+ MDM APIs This includes over-the-air enrollments and management, security policies and restrictions, and the ability to push profiles.
- The capability to leverage historical client management functions along with modern MDM API management.

Manage macOS devices with MaaS360 with Watson
macOS works in coordination with other Apple devices, running many of the same apps found on iPhone or iPad devices. In addition to analytics and robust security capabilities, MaaS360 with Watson provides laptop management capabilities designed for macOS as well as over-the-air enrollment and inventory management reporting on hardware, operating systems and software information. MaaS360 supports Mac OS X Tiger 10.4 and later versions.

Some of the key features MaaS360 offers regarding macOS management include:

- Integration with Apple Business Manager, allowing for the configuration of options from the UEM solution for streamlined enrollment.
- Device encryption support through configuration of FileVault 2 to encrypt macOS with XTS-AES-128 encryption, including the ability to create personal or institutional recovery keys.
- The ability to enforce Gatekeeper settings to allow the download of applications from anywhere or to limit downloads solely to the App Store and known developers.
- Consistent system configuration through restriction of the panes available to end users, establishing what can and cannot be adjusted on each macOS device.
- The capability to test OS version updates first, including the delay of automatic updates by up to 90 days.
- Interactive reporting and analysis for data security services including data encryption status, anti-virus, backup and recovery, personal firewall, and missing operating system patches through the endpoint security reporting module.
- Remote management of a number of device and user settings, including password, email, VPN, and wifi settings through the configuration management module.

With the help of IBM Security MaaS360 with Watson, organizations are able to help strengthen their security posture for all their laptops, no matter the type of OS, from one console.

Manage patches
OS patch management performs an install of patches, confirms installation of patches, and reports on the patch status for all devices, with minimal user intervention. All patches, including Microsoft operating system patches, are prepackaged and pretested, and include corrupt patch detection, patch rollback, bandwidth throttling and an audit of all installed Microsoft operating patches. For macOS, MaaS360 with Watson allows companies to remotely deploy the latest security patches and macOS updates to devices from the MaaS360 portal. Administrators can push macOS updates to individual devices or a group of devices that are enrolled in MaaS360.

When using the patch management system available in MaaS360 with Watson, IT teams can:

- View details about missing OS patches for Windows laptops in the patch management grid, including patch name, source category, source severity and devices missing patches.
- Natively find and report missing OS patches for managed Windows 10 devices, while allowing administrators the ability to install missing patches on a single or all devices.
- Distribute OS patches and app updates to devices by source category.
- View OS patches that are missing from a device, as well as the devices that are out of compliance for a specific patch.
- See OS patches and app updates that are missing from a Windows device or that have been distributed to specific devices from one page.

Manage device compliance and security
Whether they own laptops running an edition of Windows or Mac or both, with or without BYOD policies in place, organizations should consider a strategy that helps them put protections in place along with a consistent set of policies to drive compliance. With the help of IBM Security MaaS360 with Watson, organizations are able to help strengthen their security posture for their laptops, no matter the type of OS, from one console.

MaaS360 offers:

- Reporting on the service status, versions and definitions of installed anti-virus, antispyware, and similar software.
- Granular patch and update management as well as the ability to distribute applications, files or scripts.
- Automated out-of-compliance rules and actions for devices missing patches or running older versions of Windows 10.
- Proactive threat identification and remediation whether that means taking action when a user connects to risky networks, blocking a browser from ever hitting a phishing landing page or crypto jacking.
- The configuration of policy settings for macOS devices which includes restriction settings (such as Passcode, App Compliance and System Preferences settings), configuration settings (such as wifi, VPN, FileVault, Gatekeeper, and printing settings) and user settings.

Conclusion

IBM Security MaaS360 with Watson applies a modern device management concept to help organizations mix laptop management and mobile management under the same console. With MaaS360 with Watson, administrators have one point of control for Windows and macOS laptops, and are able to quickly enroll, set up and protect laptops with policies to help strengthen their security posture.

Why IBM?

IBM Security MaaS360 with Watson has advanced security features for endpoints, applications, and content, covering many major operating systems and device types. MaaS360 with Watson features AI and security analytics, data loss protection, mobile threat management and identity and access management, enabling organizations to strengthen policies and compliance rules while helping establish a more robust approach to their security framework.

For more information

To learn more about IBM Security MaaS360 with Watson, please contact your IBM representative or IBM Business Partner, or visit ibm.com/products/maas360.

Notes

1. IDC MarketScape: Worldwide Unified Endpoint Management Software 2022 Vendor Assessment, IDC, May 2022

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
November 2022