IBM Security

Baking Apple macOS support into your endpoint management approach

IBM MaaS360 with Watson unifies management of all device platforms, including macOS

IBM Security White Paper

A new endpoint management paradigm

Look at any enterprise today and you're likely to see a wide range of end-user devices under management—as well as some that are running under the radar. Users now demand flexibility in both form factor and platform, whether that means an Apple MacBook Pro running Apple macOS, a hybrid tablet enabled with Microsoft Windows 10, a Google Android smartphone, an Apple iOS device, or all of the above. Bring-your-own-device (BYOD) policies can help reduce the burden for IT of provisioning specific devices to meet every user's need, but it doesn't help reduce the burden of managing those devices. In fact, it can make endpoint management, including security, far more difficult.

That's the beauty of unified endpoint management, or UEM—the next evolution in a set of capabilities that began with mobile device management (MDM) and enterprise mobility management (EMM).

With the right UEM solution, IT organizations can manage all types of devices—laptops, desktops, tablets, hybrids and smartphones—with one solution, whether they're running Microsoft Windows, Android, iOS (including Apple iPhone and Apple iPad) or macOS (including the Apple Mac Mini, Apple Mac Pro, Apple MacBook, and Apple MacBook Air).

Not only does UEM consolidate and streamline the management of disparate device types, it's paving the way for a new endpoint management paradigm—one that empowers both IT administrators and end users while strengthening endpoint, application (app), content and data security. By leveraging application programming interfaces (APIs) for the platforms, over-the-air (OTA) enrollment and management policies, app catalogs, and other features, IT can take a lightweight, low-touch approach to managing end-user devices. In addition, IT can apply the same approach to all devices, from laptops to smartphones—whether personal or company-owned.

"UEM has the potential to offer several benefits: efficiency via a single endpoint security and management system, simplicity via a single set of policies for all end-user devices, and unified visibility into all connected endpoints."

—Eric Parizo, Current Analysis[1]

Read more in this blog about the increasing focus on UEM.

[1] Eric Parizo, "Ubiquitous Mobility and the Coming Transition from EMM to UEM," *Current Analysis,* March 30, 2016.

The challenges of a mixed-device environment

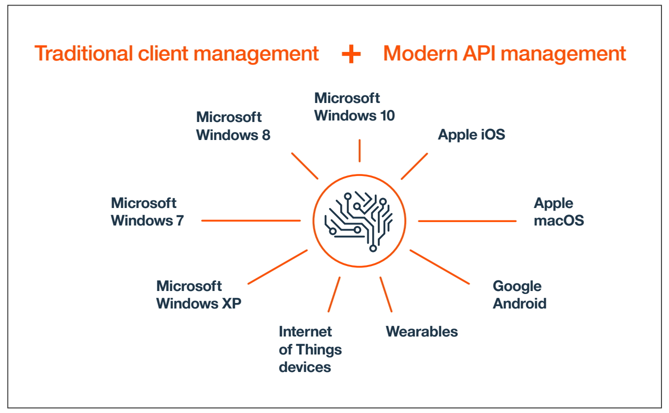
Whether BYOD is in play or not, IT organizations are now on the hook to manage virtually every type of end-user device. Adding to the stress, the MDM and EMM solutions they've invested in are incapable of managing every form factor and platform—let alone offering the granular security functionality needed for every operating system version. This is especially true when it comes to macOS devices, which have traditionally made up a lower percentage of enterprise laptops and desktops in most industries.

Mixed-device environments pose other challenges as well:

- Some platforms offer greater native security safeguards than others. Organizations need a solution that understands each device and operating system in detail and can help mitigate the associated risks.
- Some devices are running outside the control of IT. Organizations need to be able to find all the devices that are accessing data and resources, no matter the type.
- IT teams don't have time to touch every device or walk users through a lengthy enrollment process, or to keep track of patches, upgrades, encryption and anti-virus status, and other details for every type of device, platform and operating system version in use.

As a result of these challenges, the more powerful management controls afforded by UEM are replacing those of MDM, EMM, and traditional client management tools—leveraging platform API sets for more robust management of device security and configurations, including those of macOS devices.

Click image to enlarge. Click again for original size.



An effective UEM solution must support a wide range of endpoints and platforms.

Learn more about UEM use cases in this online article.

Apple’s slice of the pie is growing in the enterprise

Although Apple Macs have long been used extensively in fields such as education and graphic design, they are now gaining more traction in enterprises across all industries due to strong user adoption and preference. More organizations are giving employees their choice of platform, and more employees, including those who use Apple products for personal use, are requesting them at work. Apple has a reputation for delivering consumer-centric products, and Macs currently account for nearly 10 percent of all personal computers.[1] While certainly not the majority of market share, it’s a percentage that IT organizations can’t afford to ignore.

Apple continues to provide innovative enhancements to its products, and organizations that support Apple products need to position themselves to take advantage of those enhancements and keep up to date with the latest releases—without expending unnecessary resources or stifling the special features baked into these devices. The right UEM solution can leverage robust Apple API sets to help organizations manage macOS devices throughout the device lifecycle, from initial enrollment to device deprovisioning, including security configuration, app provisioning, and ongoing deployment of patches and updates—as well as managing the ad hoc challenges of lost and stolen devices.

But Apple is still just one of the manufacturers in the mix. Organizations need a solution that can support updates and operating system versions from Apple as well as all of the other device manufacturers on the day those changes become available, facilitating management of desktops and laptops as easily as tablets and smartphones.

“Mac has been slowly gaining on the rest of the market for the past decade or more.”

—Paul Thurrott[1]

Read more about the increase in Mac usage.

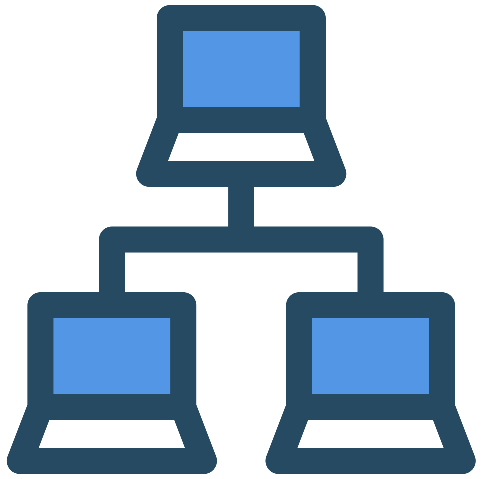
[1] Paul Thurrott, “Mac Nears 10 Percent Usage Share,” *Thurrott,* May 3, 2016.

Managing the Apple device lifecycle

Fortunately for enterprises that support a mixture of devices, Apple provides a robust set of APIs and management features that make it easier than ever to manage laptops, tablets and smartphones running macOS and iOS, boosting endpoint security while reducing administrative overhead. Using IBM® MaaS360® with Watson™, a cognitive UEM solution, you can intelligently manage macOS devices (including Mac Mini, Mac Pro, MacBook, MacBook Pro, and MacBook Air) alongside other laptop and desktop systems—from initial procurement through end-of-life, including:

- User enrollment
- Hardware and software inventory
- Security policy configuration and deployment
- App distribution and catalog management
- Email configuration
- Energy management
- Operating system patching and third-party updates
- Remote locating, locking and wiping of devices
- Reporting and analytics
- Deprovisioning

Apple API sets and features help enable the new endpoint management paradigm, equipping IT organizations with comprehensive yet lightweight tools that provide the control and visibility required to stay on top of endpoints and mitigate threats. From access controls and anti-virus protection to data encryption and media restrictions, Apple security features can help reduce the risk of a costly data breach at every point in the device lifecycle. Organizations can enjoy more efficient and effective device management thanks to dynamic security policies and automated enforcement actions, while employees can stay productive using the devices they prefer.



MaaS360 macOS device management enables set-and-distribute security policies for device restrictions, email configuration and network connectivity.

Learn more from IBM on the web about cognitive UEM for macOS.

Getting started with macOS devices

MaaS360 makes enrollment processes for macOS and iOS devices equally straightforward. Users receive an email notification or text, click on the enrollment URL and then enter the unique passcode provided. And with the Apple Device Enrollment Program (DEP) for corporate-owned devices, deployment is no longer a manual configuration process for IT. Users can be fully set up right out of the box, enabling seamless large-scale deployments of Macs, iPads and iPhones alike.

Upon enrolling any macOS device, IT can immediately access key information on its hardware, software/app inventory, and security settings, including:

- Operating system username
- Last-known location and location history
- Custom asset number
- Model
- Apple serial number
- Unique device identifier (UDID)
- Operating system
- Physical memory installed
- Free space on the system drive
- Network MAC address
- Gateway and DNS servers
- Anti-virus status and details
- Personal firewall status and details
- Encryption status and details
- Critical security patches that are missing
- Software inventory
- Change history

OTA enrollment can be a critical capability in simplifying and speeding device configuration and provisioning.

Learn more from IBM about mobile device management.

Setting up comprehensive security controls for macOS

Apple provides comprehensive native security and compliance controls for macOS devices, all of which can be managed through MaaS360 alongside iOS and other devices. Security controls for macOS include:

- Passcode enforcement
- Restrictions on email movement between email accounts
- Wi-Fi and virtual private network (VPN) profiles
- Proxy settings
- Service set identifier (SSID) auto-join
- User and group management
- Guest user restrictions
- Operating system restrictions
- Disablement of specific settings, such as those for Bluetooth
- Usage restrictions on external media and Apple AirPlay
- Certificates integration

For added data protection, Apple offers automatic full-disk encryption for macOS through FileVault, which uses XTS-AES-128 encryption with a 256-bit key to help prevent unauthorized access to data on startup disks. FileVault requires that users log in every time their Mac starts up, and no account is permitted to log in automatically.

Remote configuration of the login window, email accounts, printers and other enterprise necessities help make it easy to begin using these devices productively and securely in any corporate environment.

MaaS360 provides comprehensive tools to manage macOS security tools, from networking and wireless settings to account privileges.

Learn more from Apple on the web about FileVault encryption.

Ongoing management actions for macOS devices

When it comes to day-to-day as well as ad hoc device management activities, Apple provides the tools necessary to simplify the tasks that keep macOS users productive and secure, including OTA tools for:

- Locating lost devices
- Locking lost devices at the BIOS level
- Wiping all data from stolen devices
- Deploying operating system patches and updates
- Deploying third-party app updates
- Providing analytics reporting
- Removing control from retired devices

In addition, macOS actions include applying, changing or removing a wide range of macOS policies, such as those for device restrictions, device configuration, energy savings, login settings, and email configuration, including Microsoft Exchange ActiveSync.

Apple also provides features for facilitating the distribution of macOS apps, whether executed through a package, by package copy or by custom command. For each distribution, settings can be established for execution behavior, installation criteria, restart behavior and distribution timing.

MaaS360 works with macOS tools to minimize time for provisioning, patching, and upgrading macOS devices.

Get a quick tour of UEM basics via this For Dummies video.

With Watson, IBM MaaS360 provides cognitive UEM for macOS

MaaS360 with Watson provides a cloud-based, cognitive UEM solution that enables organizations to see what happened, what can happen, and what should be done, all in the context of their environment—and intelligently manage disparate device types, including Apple products, from a single platform.

While some vendors offer only incomplete operating system support, MaaS360 delivers UEM for iOS, macOS, Android, and Windows devices, including Microsoft Windows XP, Microsoft Vista, Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 10 and Microsoft Windows 10 Mobile. This convergence allows IT organizations to pursue a new, more lightweight endpoint management paradigm.

MaaS360 also provides the single-console view that organizations need to have consistent endpoint visibility, reporting and analytics across all device types—from desktops and laptops to tablets and smartphones—as well as a single management console that consolidates endpoint management inventory and tasks.

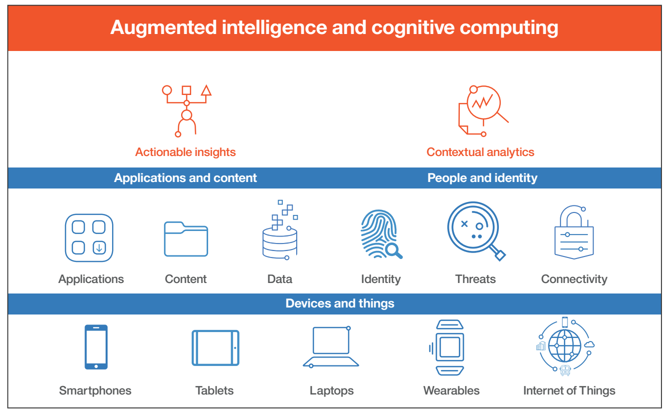
- Start a 30-day, no-charge trial of MaaS360.
- Learn how to take a cognitive approach to UEM.

These cognitive UEM capabilities include:

- Augmented intelligence that provides cognitive insights into contextual best practices, productivity enhancements and emerging threat alerts
- Device management from one console that provides visibility and control across endpoints
- Identity and access management built on a comprehensive, user-based context
- Data and app management, including fine-grained app controls
- Content editing and collaboration on-the-go
- Robust security policies, including an engine for automated rule enforcement and containment for data loss prevention (DLP)

By consolidating management of end-user devices across the enterprise with UEM, MaaS360 with Watson can help organizations increase the security of the IT infrastructure—shoring up endpoints that might otherwise be vulnerable to attackers. At the same time, IT organizations can manage the sea of devices more efficiently, reducing IT management costs while helping to keep users productive. A consolidated approach can also enhance the end-user experience, no matter which devices they use.

Click image to enlarge. Click again for original size.



Augmented intelligence and cognitive computing

Actionable insights

Contextual analytics

Applications and content

People and identity

Applications

Content

Data

Identity

Threats

Connectivity

Devices and things

Smartphones

Tablets

Laptops

Wearables

Internet of Things

MaaS360 provides a full range of capabilities with cognitive unified endpoint management.

The IBM MaaS360 with Watson difference

While some solutions provide only partial coverage across computing platforms, MaaS360 delivers cognitive UEM across the full range of endpoint types—from smartphones, tablets and laptops to desktops, devices designed for the Internet of Things, ruggedized devices and wearables. And while some solutions provide incomplete coverage of Windows-based 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. In providing the industry's first cognitive UEM platform, MaaS360 delivers a single, strategic productivity and security solution. MaaS360 enables powerful insights and analytics from Watson technology, IBM X-Force Exchange threat intelligence and cloud-sourced benchmarking data to help drive your organization's digital business transformation.

MaaS360 is delivered from a best-in-class cloud on a mature, trusted platform with ISO 27001 certification since 2016, US Federal Information Security Management Act (FISMA) certification since 2011 and SOC 2 Type II certification since 2007. MaaS360 was the first UEM solution authorized by the Federal Risk Authorization Management Program (FedRAMP). Gaining this recognition required an extensive security review of IBM controls.

Start a

30-day, no-charge trial

of MaaS360.

Read the three-part IBM blog series to find out how MaaS360 with Watson can help your enterprise achieve digital transformation.

For more information

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

IBM MaaS360
With
Watson™

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned X-Force research, provides security intelligence to help organizations holistically protect their infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

IBM Security
New Orchard Rd
Armonk, NY 10504

Produced in the United States of America
July 2017

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.