IBM Security

A smarter approach to enable endpoints, end users and everything in between

Use IBM MaaS360 with Watson for cognitive unified endpoint management

IBM Security White Paper

The road to unified endpoint management

Today's enterprises support an assortment of end-user devices, including laptops and desktops (both PCs and Macs), tablets and hybrid devices, and, of course, smartphones. Not only do employees use a variety of form factors, but they run a variety of platforms on those devices, including:

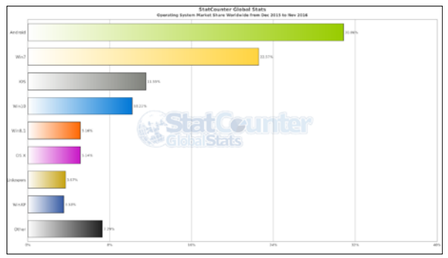
- Apple iOS and Apple macOS
- Google Android
- Microsoft Windows

To complicate the situation further, they run different versions of those platforms—for example, Microsoft Windows XP SP3, Microsoft Windows 10 or anything in between. In addition, IT is being tasked more and more with managing and securing wearables, ruggedized devices and the Internet of Things (IoT).

As tempting as it may sound, few organizations can standardize on one or two types of devices that all run the same operating system (OS), especially if they have a bring-your-own-device (BYOD) policy in place. Users now demand extraordinary flexibility, and organizations that can accommodate these user preferences can see dramatic increases in employee productivity. At the same time, a flexible infrastructure has multiple moving parts, making it difficult for many IT organizations to manage. Security can be particularly challenging, especially considering that security threats can change from one moment to the next.

With these factors considered, many organizations rely on various point solutions to get the job done—for example: a combination of mobile device management (MDM) and client management tools. These tools, however, generally lack integration, consolidated views of security status and user activity, and the ability to consistently apply and enforce management policies. Unified endpoint management (UEM) can relieve these shortcomings.

Click image to enlarge. Click again for original size.



Source: "Operating System Market Share Worldwide from Dec 2015 to Nov 2016," *StatCounter Global Stats,* December 2016.

Read more about IBM solutions for managing devices and ensuring their security.

The evolution of MDM

What started out as MDM has evolved over time to include mobile application management (MAM), application security, content management, threat management and many other capabilities that comprise enterprise mobility management (EMM). Simple MDM features are no longer sufficient in meeting today's complex enterprise data security requirements. And as the lines between smartphones, tablets and other endpoints continue to blur, UEM allows IT administrators to consolidate management of all device types, regardless of form factor, platform or OS version.

Thanks to application programming interface (API) sets from platform vendors such as Apple, Google, and Microsoft, UEM is easier than ever before. API sets allow UEM solutions to easily provide the functions needed to manage configurations and device security without the overhead of an agent sitting on the client. With API sets for iOS, macOS, Android and Windows 10, managing those devices is far more efficient than the agent-based client management of the past.

Legacy devices, platforms and applications—including Windows XP SP3 and Microsoft Windows Vista desktops, laptops running Microsoft Windows 7 (an OS whose extended support will be ending in 2020[1]), Microsoft Windows Phones that predate Windows 10 Mobile, and Win32 applications and software that are still being supported—will require the agent-based approach to ensure that they stay patched, updated and securely under IT control.

"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*[2]

Read more in this blog about the emergence of UEM.

1 "Windows lifecycle fact sheet," *Microsoft*, January 2016.

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

Unified endpoint management—converging API sets and agents

Device management demands the use of API sets to manage some endpoints and agent-based methods for others. API sets provide robust management of security and configurations; agents enable efficient patching and OS updates. Instead of deploying separate point solutions to address each of these use cases, the most effective approach is to employ a unified solution that offers IT administrators the best of both options.

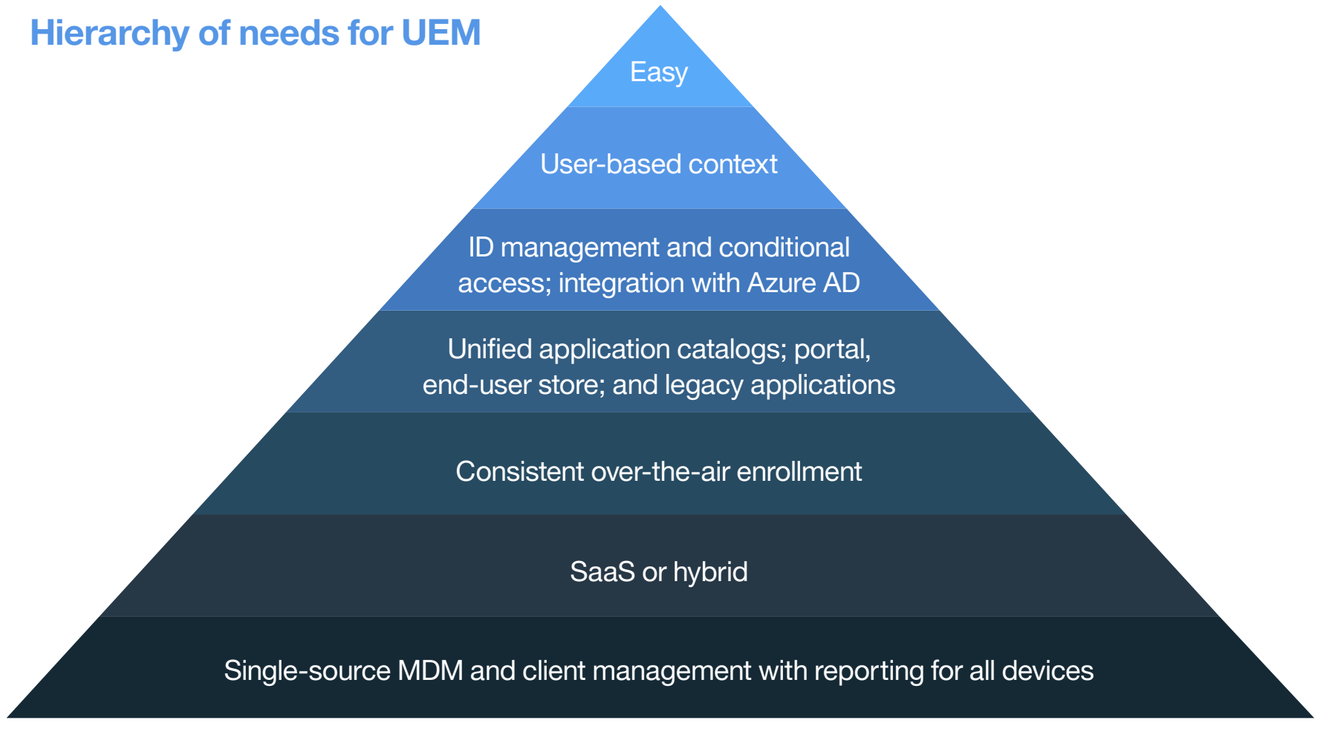
Synergy emerges when you combine the management and security of current and legacy technologies on one UEM platform for consistent device management. For organizations supporting legacy devices such as Windows 7 laptops, but have plans to migrate to Windows 10, a converged UEM solution allows IT to make the transition smoother. For this reason, it's important to choose a UEM platform designed to help make the migration seamless—even across a wide range of devices.

A converged UEM solution allows IT managers to use:

- API sets to manage today's mobile devices and OS versions
- Agent-based management for legacy devices and platforms
- A true unified approach for devices that support both API sets and agents
- A single tool that optimizes migration from legacy platforms

Learn more in this UEM for Dummies video.

Hierarchy of needs for UEM



Preparing for your Windows 10 migration

Preparing your organization to migrate from legacy Microsoft platforms such as Windows 7 to Windows 10 is a special case that is worth a closer look. Many organizations have a standard practice of exclusively supporting Windows 7 laptops and desktops. However, an increasing number are either moving to Windows 10 as part of the hardware upgrade process or are planning to complete their migration in the near future as the end of extended support for Windows 7 quickly approaches in 2020.[1]

The first question to cross most IT administrators' minds: will Windows 10 migration also require an investment in new device management tools, on top of everything else? Fortunately, the answer is no. With the right management solution in place, organizations can seamlessly transition from traditional agent-based device management to API-based device management, with help from Microsoft APIs for Windows 10.

In the meantime, many organizations find themselves supporting wide ranges of devices and operating systems, even as they prepare to transition to Windows 10. A UEM solution can help IT organizations face the challenges that today's fragmented device landscape presents. It can provide a single solution for deployment, management, security and monitoring of end-user devices, from Windows desktops to the latest Apple iPhones. And as more organizations make plans to migrate to Windows 10, the right UEM platform can support laptops, desktops and mobile devices across the gamut of operating systems, bringing all devices under one management umbrella, regardless of where they are in the migration process.

Windows 10 is now running on more than 400 million devices.[2]

Learn more about UEM for Windows 10 on SecurityIntelligence.com.

1 "Windows lifecycle fact sheet," *Microsoft*, January 2016.

2 Chuck Brown, "Windows 10: Here to stay in a big way," *Security Intelligence*, November 2, 2016.

Managing wearables, ruggedized devices and the IoT

Enterprises must consider endpoints that are growing dramatically in type and in number. Wearables, ruggedized devices and the IoT are all valuable when used efficiently, but can bring problems with security and management.

Wearable devices—from smart watches to body-worn cameras and heads-up displays—have increasing usefulness and technical capabilities, incorporating GPS receivers, cameras and other sensors for unprecedented utility. But they can break traditional patterns about how to secure mobile devices with strongly limited interfaces, proprietary connection types and unclear security implications. All of these factors make wearables complicated to manage.

Ruggedized devices, even ones that are essentially identical in function to existing devices such as laptops or tablets, may require a different approach to management, in part because of the environments where they are likely to be used, such as hardhat areas. Ruggedized devices are often deployed in places where they may be physically unreachable (or only occasionally reachable), making maintenance or management tasks that require accessing the device itself either impossible or expensive.

From the point of view of a security team responsible for managing and securing them, IoT devices share many qualities with wearables and ruggedized devices; they combine sensing and communications tools in a package that may be difficult to physically access, have limited management channels, and represent a security risk if left unsecured.

By anticipating change and implementing a flexible device model, IBM® MaaS360® is ready to help survey, update and secure modern, advanced endpoints alongside conventional desktops, laptops, smartphones and tablets.

Intelligent automation, safety initiatives, miniaturization and ever-improving communication channels mean networked devices will become the rule and not the exception.

- Learn how companies can use managed IoT devices to enhance worker safety.
- Read how IBM can help you use wearable devices to keep employees safer.

Choosing the right UEM solution

The following criteria should be considered by your organization in its search for a UEM solution that meets modern day requirements:

- A single console that consolidates endpoint management activities across all device types, including smartphones, tablets, laptops, desktops, wearables, ruggedized devices and IoT
- Multiplatform support, including iOS and macOS, Android, Windows 10 and Windows 10 Mobile
- Broad legacy Windows OS support: Windows XP SP3, Windows Vista, Windows 7 and Microsoft Windows 8
- Granular control over operating system and software patching policies, allowing IT administrators to customize maintenance and management of legacy devices
- Augmented intelligence capabilities that provide cognitive insights, contextual best practices, productivity improvement opportunities and emerging threat alerts
- Robust security capabilities for all types of devices and their data, including an engine for automated rules enforcement and containment capabilities for data loss prevention (DLP)
- Secure productivity applications to enable email, web browsing and content editing for on-the-go users
- A means to detect, analyze and automatically remediate enterprise malware and other advanced threats on endpoints
- Consistent endpoint visibility across all device types, regardless of whether they are managed by API sets or agents
- Reporting, analytics and inventory capabilities for devices as well as their applications and content
- A positive user experience throughout the lifecycle of the device, from deployment and onboarding through management, security enforcement and end-of-life
- A software-as-a-service (SaaS) delivery model that speeds up implementations and streamlines upgrades while reducing the hardware expenses, operating costs and management overheads that are synonymous with on-premises systems

With UEM, you can manage the full range of endpoints from a single console.

Learn more about common use cases in this UEM for Dummies e-book.

IBM MaaS360 with Watson for cognitive UEM

MaaS360 with Watson® is the industry's first cloud-based, cognitive UEM solution that addresses the pains of managing and securing a heterogeneous pool of endpoints, end users, and everything in between—including their applications, content and data. Used with IBM Watson and backed by the industry-leading security intelligence of IBM X-Force® Exchange, MaaS360 is a trusted advisor designed to help organizations unlock opportunities, amplify security and optimize efficiency with augmented intelligence and cognitive insights.

MaaS360 cognitive UEM capabilities include:

- Support across all major mobile platforms—affording organizations total visibility and control over their iPhones, iPads, Android devices, Windows 10 Mobile devices, and even Windows and macOS laptops and desktops
- Comprehensive support for legacy Windows platforms, including Windows XP SP3, Windows Vista, Windows 7 and Windows 8
- IBM MaaS360 Advisor, to provide IT with augmented intelligence for cognitive insights, contextual best practices, and emerging threats from structured and unstructured data
- Identity and access management (IAM) that allows a shift from a device-based context to comprehensive, user-based context
- Data and application management, including a user-friendly encrypted content container, fine-grained application controls, bulk application purchase and distribution capabilities, and intuitive enterprise application catalog
- Security policies and analytics that provide actionable intelligence reducing security and compliance risk without negatively impacting user productivity
- Detection and defense against malware and advanced threats with automated remediation capabilities
- Management and security of specialized use cases for wearables, ruggedized devices and the IoT

By consolidating management of end-user devices across the enterprise with UEM, MaaS360 can improve the overall security posture of the IT infrastructure by increasing the security of its endpoints, while enhancing employee productivity, increasing organizational efficiency and reducing management costs. A consolidated approach also enhances the end-user experience, including for new Windows 10 users.

IBM MaaS360

With Watson™

MaaS360 with Watson delivers a cognitive unified endpoint management platform.

Learn more about cognitive insights and analytics from MaaS360 with Watson.

Why organizations select IBM MaaS360 for UEM

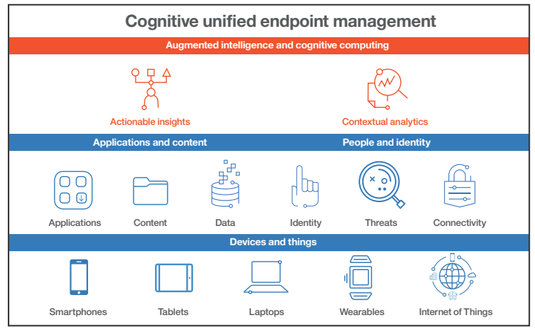
MaaS360 provides customers of all sizes, across all industries, with consistent endpoint visibility, manageability, security, reporting and analytics across all endpoints—whether they use APIs or agents—delivered from a single management console.

This single solution is particularly beneficial as organizations transition from legacy platforms to their new replacements—including Windows 7 to Windows 10 PC migration. Since MaaS360 unifies the management and security of all endpoints, there's no ripping and replacing required, nor is there a need to run multiple solutions in tandem. Even if you were to complete your migration tomorrow, you could continue using the same MaaS360 solution to:

- Secure and manage all associated endpoints
- Deploy, manage and secure your applications
- Enable content and control access
- Protect data across emails, content, and applications, helping to prevent leaks
- Seamlessly authorize identities and enforce authentication
- Establish context to facilitate security analysis and alerts
- Use MaaS360 Advisor to discover, define, assess and act on opportunities and issues

An exclusively SaaS offering, MaaS360 helps organizations get up and running faster, minimize their IT management footprint, and ensure that their endpoints are always running the latest software versions, including updated code as platform vendors release expanded APIs.

Click image to enlarge. Click again for original size.



MaaS360 provides a single platform to manage and secure all endpoints.

Get more insight into MaaS360 UEM by viewing this on-demand webinar.

IBM MaaS360 product editions

The MaaS360 UEM product editions offer a broad range of solutions that provide organizations with comprehensive endpoint management and security capabilities across all types of devices. The product is made up of the following product editions: Essentials, Deluxe, Premier and Enterprise.

In addition, as part of the IBM Security portfolio, MaaS360 provides key technology integrations, including with IBM BigFix®, IBM Security Access Manager, IBM QRadar® SIEM and IBM Trusteer® solutions, to boost the value of your IT investments. MaaS360 integrates with many leading technology solutions, so you can leverage your current IT investments to mobilize your organization.

MaaS360 with Watson insights and analytics can help organizations realize ROI faster by identifying and leveraging mobile opportunities, increasing the productivity of the mobile workforce, boosting the efficiency of IT operations, minimizing security risks and helping the business make more informed mobility decisions, including spending decisions. Insights and analytics include actionable intelligence and education that is tailored to the organization, cloud-sourced mobile benchmarking data, and a mobile security scorecard.

Click image to enlarge. Click again for original size.

Solution	Essentials	Deluxe	Premier	Enterprise
Device Management iOS, Android, Windows Mobile, Windows & macOS	✓	✓	✓	✓
App Management iOS, Android, Windows Mobile, Windows & macOS	✓	✓	✓	✓
Patch and Update Management	✓	✓	✓	✓
Identity Management	✓	✓	✓	✓
Advisor	✓	✓	✓	✓
Container App	✓	✓	✓	✓
Mobile Expense Management	✓	✓	✓	✓
Secure Mobile Mail		✓	✓	✓
Secure Mobile Chat		✓	✓	✓
OS VPN			✓	✓
Secure Browser			✓	✓
Gateway for Browser			✓	✓
Content Management			✓	✓
Gateway for Documents			✓	✓
App Security			✓	✓
Gateway for Apps			✓	✓
Mobile Document Editor				✓
Mobile Document Sync				✓
Mobile Threat Management				✓

For more information about Maas360 editions, visit the IBM Marketplace.

- Take a quick tour of the MaaS360 home page via this IBM video.

Why IBM?

While alternative solutions provide incomplete coverage across computing platforms, MaaS360 delivers cognitive UEM across all endpoint types including smartphones, tablets, laptops, desktops, 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 for a simpler time for tactical purposes and disparate mobility projects. With the industry's first cognitive UEM platform, MaaS360 with Watson delivers a single, strategic management and security solution to drive your organization's digital business transformation.

And this is just the beginning. As cognitive capabilities are added, MaaS360 with Watson builds greater knowledge and context, for a smarter approach to securing and enabling endpoints, end users and everything in between. These capabilities create a valuable, trusted advisor and partner in the digital transformation of business.

In addition, MaaS360 is:

- Comprehensive, with a full suite of management, security and productivity solutions
- Delivered from a best-in-class cloud on a mature, trusted platform
- Trusted worldwide to provide enterprise security and focused on providing fast time-to-value
- Known for its exceptional customer experience, from its 30-day trial through full deployment
- Capable of securely integrating with IBM Notes®, Microsoft Exchange, Microsoft Active Directory/LDAP, certificate authorities and other IT systems in an easy, plug-and-play fashion
- Non-intrusive and does not sit in the critical path of your emails
- Certified to comply with ISO 27001, Federal Information Security Management Act (FISMA), SOC 2 Type II and Federal Risk and Authorization Management Program (FedRAMP)

Visit UnifiedEndpointManagement.com for a 30-day trial of MaaS360 at no charge.

For more information

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

About IBM Security

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.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
March 2017

WGW03287-USEN-00