IBM MaaS360 with Watson for Apple macOS

MaaS360 unifies management of all device platforms, including macOS

Highlights

- Utilize single-console management for consistent endpoint visibility, reporting and analytics across all device types
- Manage Apple macOS devices alongside smartphones, tablets, laptops, desktops, wearables and the Internet of Things (IoT)
- Strengthen endpoint security by helping reduce the risk of a costly data breach at every point in the device lifecycle

Unified endpoint management, or UEM, enables IT organizations to manage all types of devices with one solution, and paves the way for a new endpoint management paradigm—one that empowers administrators and end users. Leveraging features such as application programming interfaces (APIs), over-the-air (OTA) enrollment and management policies, and application catalogs for business software, IT can apply the same approach to all devices, from laptops to smartphones, user-supplied or company-owned.

macOS features facilitate this trend across the device lifecycle. And with comprehensive, cloud-based UEM capabilities provided by IBM® MaaS360® with Watson™, you can easily manage macOS devices, from initial procurement through deprovisioning.

MaaS360 can help organizations increase the security of the IT infrastructure—shoring up endpoints that might otherwise be vulnerable. At the same time, IT organizations can manage the sea of end-user devices more efficiently, reducing IT management costs while helping to keep users productive.

The challenges of a mixed-device environment

IT organizations are now on the hook to manage virtually every type of end-user device—but they don't have time to touch every device or walk users through a lengthy enrollment process. And legacy mobile device management (MDM) and enterprise mobility management (EMM) can't manage every form factor and platform—let alone offer security protection for every operating system.

Although they have traditionally made up a lower percentage of enterprise endpoint infrastructure, Apple Macs are gaining more traction across industries as more organizations are giving their employees the ability to choose which platforms they use for work. Building on a reputation for delivering consumer-centric products, Macs currently account for nearly 10 percent of all personal computers.[1]

Managing the Apple device lifecycle

Apple provides a robust set of APIs and management features to simplify managing smartphones, tablets and laptops running Apple iOS and macOS, providing control and insight from enrollment through retirement, and boosting endpoint security while reducing administrative overhead.

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.

Getting started with macOS devices

Enrollment processes for Apple iPads, Apple iPhones and Macs are equally straightforward, especially through MaaS360. With the Apple Device Enrollment Program (DEP) for corporate devices, deployment is no longer a manual configuration process for IT. Users can be set up right out of the box, for seamless large-scale deployments of iOS and macOS devices.

Apple also provides comprehensive security and compliance controls for macOS devices, all of which can be managed through MaaS360 alongside iOS and other devices. Security controls for macOS range from passcode enforcement to guest user restrictions to usage restrictions on external media and Apple AirPlay.

Ongoing management 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, from locating lost devices to wiping data from stolen devices to removing control from retired devices.

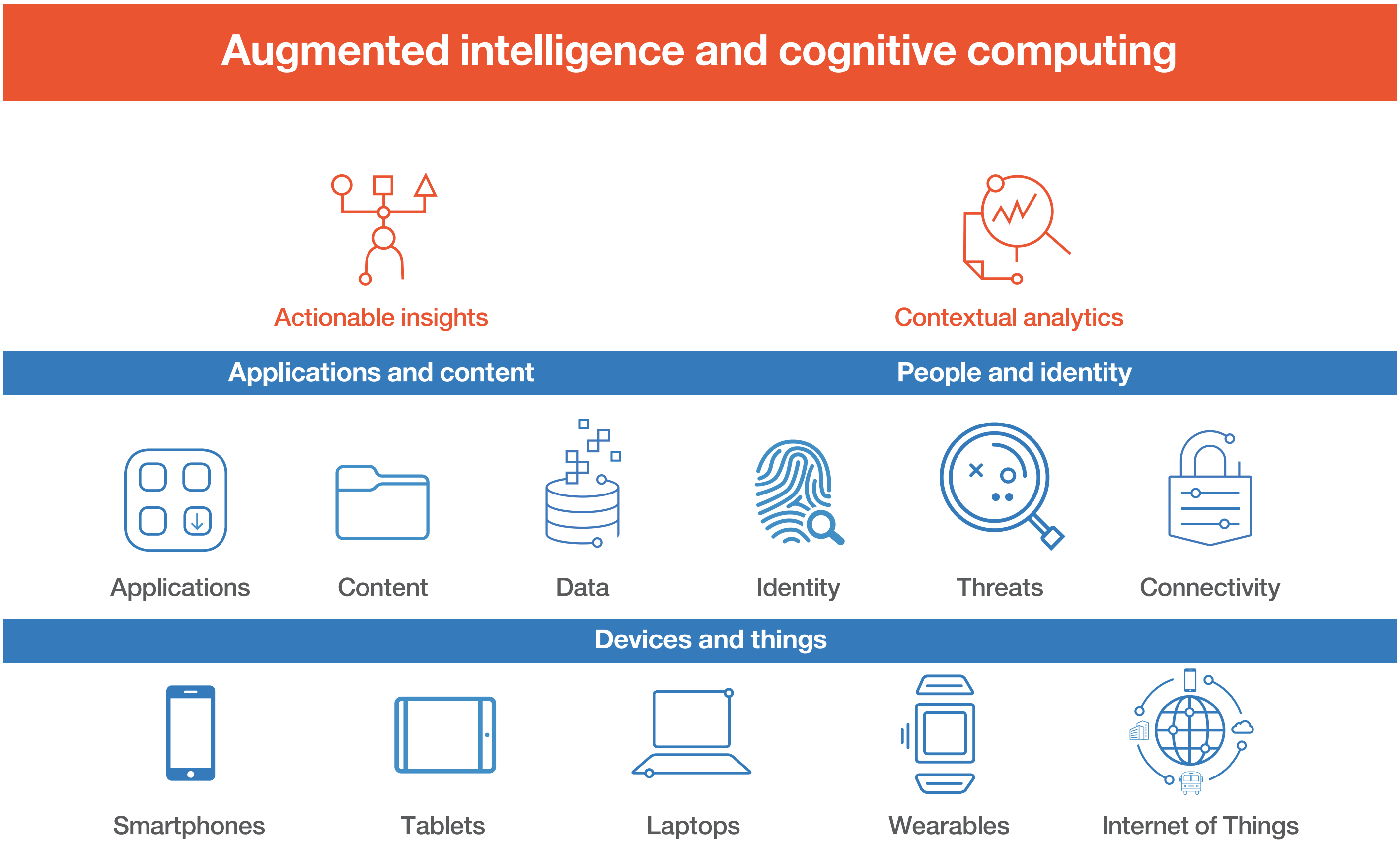
Additionally, specific actions can be taken to control a wide range of policies for macOS devices, including restrictions, configuration controls, passcode settings, and email setup—including Exchange ActiveSync. Apple also provides features for facilitating the distribution of macOS applications, whether executed through a package, by package copy or by custom command.

UEM for macOS with MaaS360

MaaS360 delivers UEM for iOS, macOS, Google Android, as well as Microsoft Windows devices, including support for Microsoft Windows 7 through Microsoft Windows 10.

MaaS360 also provides the single console that organizations need for consistent endpoint visibility, reporting and analytics across device types, as well as a management console that consolidates endpoint management inventory and tasks. It enables:

- Device management that provides visibility and control across endpoints from one console
- Identity and access management built on a comprehensive, user-based context
- Data and application management, including fine-grained application controls
- Content editing and collaboration with data leak prevention (DLP)
- Policies and analytics that provide actionable intelligence



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

Why IBM?

IBM is a trusted IT partner worldwide with a focus on enabling enterprise security, offering a powerful security software and services portfolio as well as exclusive IBM Watson cognitive technology and the industry-leading security intelligence of IBM X-Force® Exchange. Now MaaS360 with Watson elegantly and efficiently delivers UEM to a full spectrum of end-user devices, including smartphones, tablets, laptops and desktops. MaaS360 also provides an exceptional user experience from a 30-day no-cost trial through full deployment.

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 Federal Risk and Authorization Management Program (FedRAMP)-authorized EMM solution, which entailed an extensive security review of IBM controls.

For more information

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

IBM Security
New Orchard Rd
Armonk, NY 10504

Produced in the United States of America
June 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 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.

[1] Paul Thurrott, “Mac Nears 10 Percent Usage Share,” *Thurrott*, May 3, 2016. https://www.thurrott.com/hardware/66933/mac-nears-10-percent-usage-share

Please Recycle