

---

# Mobility insights and analytics with IBM Watson

Left in the dark with dim MDM? Brighten your day  
with IBM MaaS360 with Watson for cognitive UEM

# Are you drowning in mobile minutiae?

Today's mobile landscape looks very different than it did just a few years ago. In fact, with 7.9 million mobile applications downloaded every month<sup>1</sup> and 387 new malware threats identified every minute,<sup>2</sup> the landscape can change overnight. In an ever-evolving mobile world, organizations are actively struggling to maintain security while keeping their workers productive each day. Leveraging mobile data to add business value also can be a tall order.

While working to maintain tactical control of the mobile environment, IT managers often find themselves drowning in minutiae. Overwhelmed by the number of moving parts, they're unable to stay abreast of the latest threats, let alone extract meaning from or make decisions based on the mountains of data now being collected. With limited IT resources dedicated to mobile technology tools that facilitate reactive rather than proactive management—and limited

visibility into mobile intelligence across the organization—many managers have had to choose between security and productivity as the focus of their efforts.

Given the importance of mobile computing in keeping businesses competitive, it's more important than ever that organizations strike the appropriate balance between security and productivity—and tap into the vast potential business value that mobility represents. With proactive delivery of rich insights, organizations can transition from a purely tactical management approach to one that is strategic; informed by industry data and best practices, optimized for IT efficiency, and appropriate to the organization and each user. This new paradigm is the difference between a legacy mobile device management (MDM) solution and a new, smarter approach with cognitive unified endpoint management (UEM).

**472:** Average number of applications managed by heavily mobile organizations.<sup>3</sup>

▶ [See the latest statistics](#) on mobile security in this IBM infographic.

<sup>1</sup> Jeremy Sacco, "[App downloads soar in October](#)," *The Fiksu Blog*, November 24, 2015.

<sup>2</sup> "[McAfee Labs Threat Report](#)," *McAfee Labs*, February 2015.

<sup>3</sup> "[The Massive Mobile Migration](#)," *IBM*, April 27, 2016.



# Insights and analytics from IBM MaaS360 with Watson

Click image to enlarge. Click again for original size.

Thanks to a massive migration to mobile platforms, what began as mobile device management (MDM) evolved over time into enterprise mobility management (EMM) technology, encompassing MDM and the capabilities needed to manage and secure applications, content, bring-your-own-device (BYOD) environments and much more.

The next step in the evolution accounts for all device varieties—smartphones, tablets, laptops, desktops, wearables, and devices designed for the Internet of Things (IoT)—hence the term unified endpoint management (UEM). IBM® MaaS360® has unleashed a unique approach to UEM that does more than manage and secure endpoints, users, groups, and their applications, content and data. MaaS360 goes not just a step, but a leap, to leverage the deep insights that big-data analytics and cognitive computing can provide for a given organization's IT environment—or even for an entire industry.

Keeping with IBM leadership in ushering in the new cognitive era, MaaS360 is now available with deep insights and cloud-based

analytics. With IBM Watson® technology, backed by the industry-leading security intelligence of IBM X-Force® Exchange, MaaS360 insights and analytics can help organizations accelerate and maximize the return on investment (ROI) from their mobile strategies by:

- Identifying and leveraging digital transformation opportunities
- Reducing security risks
- Increasing the productivity of their workforce
- Boosting the efficiency of IT operations
- Helping the business make more informed decisions, including spending decisions

MaaS360 with Watson includes three key capabilities:

- [Advisor](#), which provides actionable intelligence that is tailored to the organization
- [Mobile Security Index](#), which provides the industry's first publicly available mobile security scorecard
- [Mobile Metrics](#), which provides the industry's first cloud-sourced mobile benchmarking data

**MaaS360 with Watson ushers in a new era of enterprise mobility with cognitive unified endpoint management.**

▶ [Learn more](#) about what it means to take a cognitive approach to UEM.



## MAAS360 ADVISOR:

# Actionable intelligence, tailored to your environment

Click image to enlarge. Click again for original size.

With Watson, MaaS360 Advisor is a powerful cognitive engine that provides contextual information based on industry best practices as well as relevant alerts on emerging threats. This actionable intelligence is sourced from both structured and unstructured data, and is customized based on your organization's industry, its size and its mobile environment, including the type of devices, platforms and applications used across the organization.

MaaS360 Advisor provides insights and recommendations that empower you to:

- **Discover** best practices for user productivity, recommendations for IT optimization and potential security threats—delivered right to your MaaS360 dashboard
- **Define** what the insight is and why it is important for your organization
- **Assess** the impact of best practices or security risks to your devices, users, applications and more
- **Act** on the intelligence to unlock business opportunities or remediate security threats

▶ [Learn more](#) about cognitive unified endpoint management.

Examples of insights you can expect from MaaS360 Advisor include:

- Information on upcoming operating system (OS) releases for Apple iOS, Google Android, Microsoft Windows and products from other original equipment manufacturers
- Best practices for security rules and policies
- Recommendations based on IT optimization models
- Policy changes and other remediation steps you can take based on recent vulnerabilities and detailed risk exposure information
- Visibility into specific at-risk devices
- Information on relevant security programs such as Samsung Knox, Apple VPP/DEP, Android and others
- Mobile application recommendations based on application use and sentiment analysis of the current application catalog
- Other recommendations based on insights gathered from peers in your industry

MaaS360 Advisor leverages feedback mechanisms, learning models and automation to enhance productivity, increase IT efficiency and reduce risk exposure over time. It also provides recommendations to facilitate end-user notification and education, maximizing the value of the insights to the organization.

**With Watson, MaaS360 Advisor delivers augmented intelligence and actionable insights.**

## MOBILE SECURITY INDEX:

# Where do you stand?

Click image to enlarge. Click again for original size.

The MaaS360 Mobile Security Index is the industry's first publicly available mobile security scorecard. And because it is available at no cost to customers and non-customers alike, it will offer the first view organizations have into MaaS360 insights and analytics.

This scoring index, which takes industry and geography into account, is designed to provide administrators with a mobile security rating for their organization based on current industry configuration data and best practices. It then provides a benchmark as a point of comparison against other similar organizations based on criteria such as industry, region or size. These comparisons are based on massive amounts of data from existing MaaS360 implementations.

The Mobile Security Index also provides specific recommendations and best practices for improving the organization's overall security posture. The end goal is to foster mobile security best practices across companies and industries worldwide.

In addition to an overall score, the Mobile Security Index provides scores across four categories:

- Secure connectivity
- Device security
- Application security
- Data security

To generate a score from the Mobile Security Index, organizations need only to complete a brief online self-assessment—providing answers to a series of questions about their mobile security implementation. Those completing the assessment are queried on their organization's approach to mobile devices, platforms, applications and policies.

**MaaS360 Mobile Security Index is the first step to assess and improve your organization's approach to mobile security.**

▶ Get your organization's [Mobile Security Index](#) now.

## MOBILE METRICS:

# Benchmarking data and best practices

Click image to enlarge. Click again for original size.

MaaS360 Mobile Metrics leverages the aggregated data of more than 12,000 MaaS360 customer implementations worldwide to provide the industry's first cloud-sourced mobile benchmarking data. This data, which reflects a wide range of organization types and their mobile implementations, allows customers to compare their security configurations and usage data with peers across similar industries, sizes and other criteria.

Mobile Metrics provides a clearer view into mobile environments, enables more informed decision-making and gives organizations a larger context for evaluating their security policies. For example, customers can compare their password requirements with those of other organizations in their industry, the number of applications they've blacklisted, or the number of devices on a given platform.

With forecasts and predictive models, Mobile Metrics can also help companies predict adoption rates of new mobile applications based on the experiences of similar organizations, or identify other potential opportunities to improve user productivity.

Mobile Metrics allows you to compare your environment against benchmarks on health, compliance and security, including:

- Deployment
- Devices
- Applications
- Security

**MaaS360 Mobile Metrics enables benchmarking across industries and company sizes.**

▶ [Learn more](#) about Mobile Metrics from the SecurityIntelligence.com blog post.





# Why IBM?

MaaS360 with Watson delivers an industry-first set of productivity and security solutions for cognitive unified endpoint management, made possible through technologies and intelligence available exclusively from IBM. With Watson, MaaS360 insights and analytics are informed by the aggregated cloud-sourced data of more than 12,000 MaaS360 implementations and backed by the IBM X-Force Exchange security community.

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.

**IBM MaaS360** cognitive unified endpoint management combines device application and content management with strong security through one platform, allowing customers to enhance user productivity and maximize security without compromising the user experience. IBM feeds data aggregated from implementations worldwide back into MaaS360 to continue the cycle of providing contextual and meaningful intelligence.

**IBM Watson** is a cognitive technology that can analyze and interpret all types of data, including unstructured text, images, audio and video. It utilizes machine learning to grow its subject matter expertise in applications and systems. The natural language and data mining capabilities provided by Watson have been used to address a wide range of difficult problems, from cancer diagnosis and treatment decisions to weather forecasting. Watson has now partnered with MaaS360 to enlighten unified endpoint management for business transformation.

**IBM X-Force Exchange** is a cloud-based threat intelligence sharing platform that facilitates research on security threats, the aggregation of security intelligence, and collaboration with peers. X-Force Exchange combines content from IBM, open-source projects and other third parties to provide relevant and detailed information about vulnerabilities, IP addresses, domains and web applications in real time. It is supported by IBM X-Force, one of the most recognized security research teams in the world.

## IBM MaaS360



## IBM X-Force Exchange





# For more information

To learn more about IBM MaaS360, please contact your IBM representative or IBM Business Partner, or visit: [ibm.com/maas360](https://ibm.com/maas360)

## 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.

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](https://ibm.com/financing)

© Copyright IBM Corporation 2017

IBM Security  
Route 100  
Somers, NY 10589

Produced in the United States of America  
March 2017

IBM, the IBM logo, ibm.com, IBM Watson, MaaS360, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at [www.ibm.com/legal/copytrade.shtml](https://www.ibm.com/legal/copytrade.shtml)

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.

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.