



---

## Highlights

- Eine smarte Möglichkeit, Endgeräte, Endbenutzer und alles dazwischen zu schützen und zu unterstützen
  - Effizientes Management verschiedener Geräte, einschließlich Laptops, Desktops, Smartphones, Tablets, IoT-Geräten (Internet der Dinge) und sonstigen mobilen Geräten
  - Unterstützung aller wichtigen Plattformen, einschließlich Apple iOS und macOS, Google Android und Microsoft Windows
  - Bereitstellung umfassender Unterstützung für Microsoft, vom traditionellen Microsoft Windows XP SP3 zum modernen Microsoft Windows 10
  - Vereinheitlichung von Endgeräte-transparenz, -management und -sicherheit mit einer einzigen Konsole
  - Identifizierung von Risiken und Geschäftschancen mit Erkenntnissen und Analysen aus kognitiver Technologie von IBM Watson und Bedrohungsdaten von IBM X-Force
- 

# IBM MaaS360 mit Watson

## *Ein kognitives Konzept für Unified Endpoint Management*

Es mag zwar wünschenswert sein, Endbenutzer auf einer oder zwei Arten von Geräten mit demselben Betriebssystem zu standardisieren, jedoch sieht die Realität in den meisten Unternehmen anders aus. Benutzer verlangen heute höchste Flexibilität sowie höchsten Komfort – das heißt, die meisten Unternehmen unterstützen die verschiedensten Endgeräte, z. B. Laptops und Desktops (PCs und Macs), Tablets und Hybridgeräte, Smartphones und IoT-Geräte.

Mitarbeiter nutzen nicht nur die verschiedensten Geräte, sondern auch viele verschiedene Plattformen darauf, wie z. B. iOS und macOS, Android und Windows.

Um die Situation noch zu verkomplizieren, nutzen sie verschiedene Versionen dieser Plattformen, also beispielsweise Windows XP SP3, Windows 10 oder Versionen, die dazwischen liegen.

Beim Versuch, diese heterogenen Geräteumgebungen besser zu kontrollieren, verlassen sich viele Unternehmen auf verschiedene Einzellösungen (z. B. eine Kombination aus Mobile-Device-Management- (MDM) und Client-Management-Tools). Diese Tools können normalerweise nicht kombiniert eingesetzt werden, bieten keine konsolidierte Ansicht des Sicherheitsstatus der Geräte und der Benutzeraktivität und erlauben es IT-Administratoren auch nicht, Managementrichtlinien durchgängig anzuwenden und umzusetzen. Die Lösung? Unified Endpoint Management (UEM) – mit einem smarten Konzept, das es IT-Administratoren erlaubt, das Management aller Arten von Geräten zu konsolidieren, unabhängig von Gerät, Plattform oder Betriebssystemversion.



## **IBM MaaS360 mit Watson für kognitives UEM**

IBM MaaS360 bietet eine Cloud-basierte, umfassende UEM-Lösung, die es IT-Abteilungen ermöglicht, einen heterogenen Pool von Endgeräten, Endbenutzern und allem dazwischen zu verwalten und zu schützen, einschließlich ihrer Anwendungen, Inhalte und Daten.

MaaS360 stellt leistungsfähige UEM-Funktionen für alle wichtigen IT-Plattformen wie iOS-, macOS-, Android- und Windows-Geräte zur Verfügung. Und in Fällen, in denen die Lösungen der Mitbewerber die traditionellen Microsoft-Plattformen nur mangelhaft unterstützen, bietet MaaS360 Unterstützung für Windows XP SP3, Microsoft Windows Vista, Microsoft Windows 7, Microsoft Windows 8, Windows 10 und Microsoft Windows 10 Mobile. Diese Funktionen umfassen Folgendes:

- Identitäts- und Zugriffsmanagement, das den Wechsel von einem gerätebasierten Kontext zu einem umfassenderen benutzerbasierten Kontext ermöglicht
- Anwendungsmanagement, einschließlich eines intuitiven, universellen Anwendungskatalogs für iOS, macOS, Android und Windows, erweiterter Bundling- und Promotion-Features, Funktionen für Mengenerwerb und -verteilung von Anwendungen sowie differenzierter Datensteuerung
- Einen benutzerfreundlichen, verschlüsselten Container zur Sicherung unternehmensweiter E-Mail-, Web-Browsing- und Anwendungsdaten
- Erkenntnisse und Analysen aus kognitiver Technologie von IBM Watson und Bedrohungsdaten von IBM X-Force

- Erkennung und Abwehr von Malware und erweiterten Bedrohungen durch automatisierte Korrekturfunktionen
- Management und Sicherheit für spezialisierte Anwendungsfälle für mobile Geräte, widerstandsfähige Geräte und IoT-Geräte

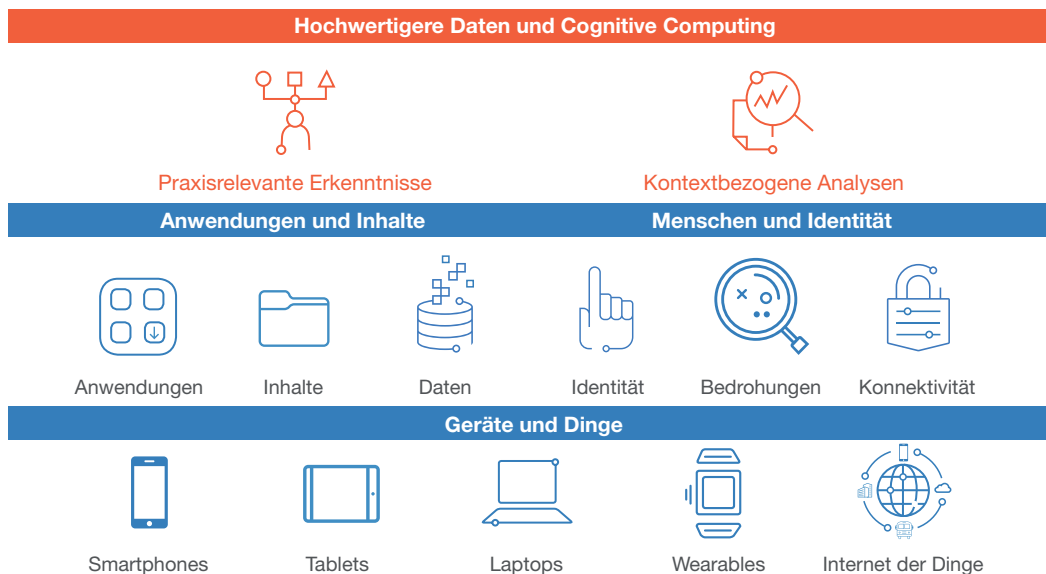
MaaS360 bietet nicht nur eine verlässliche Lösung für durchgängige Endgerätetransparenz, Berichterstellung und Analysen für verschiedene Geräte, sondern auch eine einzige Managementkonsole, die Endgerätemanagementaufgaben für alle Geräte konsolidiert, unabhängig davon, ob das Management über API-Sets, Agenten oder beides erfolgt.

MaaS360 bietet zudem Folgendes:

- Leistungsfähige Sicherheitsfunktionen, einschließlich Regelengine für die automatisierte Umsetzung
- Dashboards für die Berichterstellung und Inventarisierungsfunktionen für Endgeräte und deren zugehörige Anwendungen
- Differenzierte Steuerung von Patching-Richtlinien für Betriebssystem und Software, damit IT-Administratoren Wartung und Management traditioneller Geräte anpassen können

MaaS360 vereinfacht als ausschließlich Cloud-basiertes Angebot die schnelle Bereitstellung, trägt dazu bei, Speicherbedarf und Kosten für das Endgerätemanagement zu minimieren und stellt sicher, dass immer die neuesten Softwareversionen und aktualisierter Code vorliegen, sobald Plattformanbieter erweiterte APIs herausgeben.

## Kognitives Unified Endpoint Management



### Konvergierende APIs und Agenten

Dank der API-Sets für iOS, macOS, Android und Windows 10 ist das Management der Geräte mit diesen Plattformen erheblich einfacher und effizienter als das traditionelle agentenbasierte Client-Management. Jedoch ist für traditionelle Geräte und Plattformen nach wie vor das agentenbasierte Konzept erforderlich, um sicherzustellen, dass sie unter Kontrolle der IT immer die notwendigen Patches erhalten, aktualisiert werden und geschützt sind. In einigen Fällen ist es am effizientesten, beide Methoden kombiniert zu verwenden – eine Hybridlösung aus API-Sets und Agenten. MaaS360 führt beide Methoden zusammen und bietet Unternehmen damit die Möglichkeit, für das Management aller Endgeräte eine einzige Lösung zu nutzen.

Für alle Verantwortlichen im Bereich IT-Management und IT-Sicherheit, die weiterhin traditionelle Windows-Geräte wie Windows 7-basierte Laptops unterstützen, ermöglicht MaaS360 einen einfachen, nahtlosen Übergang zu Windows 10, ohne die Verwendung alter Management-Tools einzustellen und diese durch neue zu ersetzen. Dank Microsoft-APIs für Windows 10 können Unternehmen MaaS360 nutzen, um die Migration von traditionellem agentenbasiertem Geräte-management zu API-Geräte-management zu vereinfachen – mit einer einzigen Plattform.

## So macht IBM MaaS360 mit Watson den Unterschied

Während alternative Lösungen die IT-Plattformen nur unvollständig abdecken, bietet MaaS360 kognitives UEM für alle Endgerätetypen, z. B. Smartphones, Tablets, IoT-Geräte und sonstige mobile Endgeräte. Und während die Lösungen der Mitbewerber Windows-Geräte nur unzureichend unterstützen, bietet MaaS360 Unterstützung für das gesamte Spektrum von Windows XP SP3 bis Windows 10.

Traditionelle Mobile-Device-Management-Systeme wurden in einer einfacheren Zeit zu taktischen Zwecken und für unterschiedliche Mobilitätsprojekte erstellt. MaaS360 mit Watson stellt mit der ersten kognitiven UEM-Plattform der Branche eine einzige Lösung für strategisches Management und Sicherheit zur Verfügung, um die digitale Transformation Ihres Unternehmens voranzutreiben.

MaaS360 bietet wertvolle Erkenntnisse und Analysen aus der kognitiven Technologie von Watson, Bedrohungsdaten von IBM X-Force Exchange sowie Benchmarkingdaten aus der Cloud über die MaaS360-Plattform.

Dank der Erkenntnisse und Analysen aus MaaS360 mit Watson können Unternehmen den Return-on-Investment ihrer mobilen Strategien maximieren und schneller realisieren, indem sie Geschäftschancen identifizieren, die Mitarbeiterproduktivität steigern, die Effizienz des IT-Betriebs verbessern, Sicherheitsrisiken minimieren und Unterstützung bieten, damit fundiertere

Endgeräteentscheidungen, einschließlich Entscheidungen bezüglich Ausgaben, möglich sind. Erkenntnisse und Analysen aus MaaS360 umfassen drei wichtige Funktionen:

- **Advisor** – mit praxisrelevanten Erkenntnissen im Kontext des jeweiligen Unternehmens
- **Mobile Security Index** – mit der ersten öffentlich verfügbaren Scorecard für mobile Sicherheit der Branche
- **Mobile Metrics** – mit den ersten Cloud-basierten Benchmarkingdaten für Endgeräte der Branche

MaaS360 ermöglicht als Teil des umfangreichen IBM Security-Portfolios auch den kombinierten Einsatz wichtiger IBM Technologie mit Lösungen wie IBM BigFix, IBM QRadar SIEM, IBM Trusteer und IBM Security Access Manager, um das Maximum aus den IT-Investitionen herauszuholen.

---

# IBM MaaS360



---

MaaS360 mit Watson bietet das erste kognitive Konzept für Unified Endpoint Management der Branche.

Lösung	Essentials	Deluxe	Premier	Enterprise
Device Management <small>iOS, Android, Windows Mobile, Windows &amp; macOS</small>	✓	✓	✓	✓
App Management <small>iOS, Android, Windows Mobile, Windows &amp; macOS</small>	✓	✓	✓	✓
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				✓

Die MaaS360-Lösungsversionen sind auf den Bedarf Ihres Unternehmens zugeschnitten.

### MaaS360-Lösungsversionen

Die MaaS360-Produktfamilie bietet eine breite Palette an Lösungsversionen, die Unternehmen umfassende, sichere und effiziente Unified-Endpoint-Management-Funktionen bereitstellen, um deren Bedarf am besten gerecht zu werden. Die Lösung steht in den folgenden Versionen zur Verfügung: Essentials, Deluxe, Premier und Enterprise – weitere Details finden Sie in [IBM Marketplace](#).

### Warum IBM?

MaaS360 ermöglicht die Verwendung einer Plattform für das Management sämtlicher Geräte dank eines kognitiven Konzepts unter Verwendung von Watson. Ganz gleich, ob APIs oder Agenten verwendet werden, vereinheitlicht MaaS360 die Managementaktivitäten für alle Geräte im gesamten Unternehmen und unterstützt ggf. gleichzeitig einen Hybridansatz. MaaS360 schützt Endgeräte sowie deren Anwendungen, Inhalte und Daten, um das allgemeine Sicherheitsniveau der IT-Infrastruktur zu verbessern, während gleichzeitig die betriebliche Effizienz gesteigert und IT-Managementkosten reduziert werden. Durch einen konsolidierten Ansatz kann auch die Nutzung durch den Endbenutzer von der ersten Bereitstellung bis zur Stilllegung des Geräts verbessert werden.

## Weitere Informationen

Wenn Sie mehr über IBM MaaS360 erfahren möchten, wenden Sie sich an Ihren IBM Ansprechpartner oder IBM Business Partner oder besuchen Sie uns unter: [ibm.com/maas360](http://ibm.com/maas360)

## Informationen zu IBM Security

IBM Security bietet ein innovatives und integriertes Portfolio von Produkten und Services für die Unternehmenssicherheit. Das durch weltbekannte X-Force-Forschungsarbeit unterstützte Portfolio bietet Sicherheitsdaten, um Unternehmen dabei zu unterstützen, ihre Infrastrukturen, Daten und Anwendungen umfassend zu schützen, sowie Lösungen für Identitäts- und Zugriffsmanagement, Datenbanksicherheit, Anwendungsentwicklung, Risikomanagement, Endgerätemanagement, Netzwerksicherheit und mehr. Mit diesen Lösungen können Unternehmen ein effektives Risikomanagement betreiben und integrierte Sicherheit für mobile, Cloud-, Social-Media- und andere unternehmensspezifische Geschäftsarchitekturen implementieren. IBM verfügt über eine der weltweit größten Organisationen für Forschung und Entwicklung im Bereich Sicherheit, überwacht 15 Milliarden Sicherheitsereignisse pro Tag in über 130 Ländern und hält mehr als 3.000 Sicherheitspatente.

Darüber hinaus bietet IBM Global Financing verschiedene Zahlungsoptionen, um Sie bei Investitionen in Technologie zu unterstützen, die Sie für das Wachstum Ihres Unternehmens brauchen. Wir kümmern uns auch um das vollständige Lebenszyklusmanagement von IT-Produkten und Services – vom Kauf bis zur Entsorgung. Weitere Informationen finden Sie unter: [ibm.com/financing/de](http://ibm.com/financing/de)



### IBM Deutschland GmbH

IBM-Allee 1  
71139 Ehningen  
[ibm.com/de](http://ibm.com/de)

### IBM Österreich

Obere Donaustraße 95  
1020 Wien  
[ibm.com/at](http://ibm.com/at)

### IBM Schweiz

Vulkanstrasse 106  
8010 Zürich  
[ibm.com/ch](http://ibm.com/ch)

Die IBM Homepage finden Sie unter:  
[ibm.com](http://ibm.com)

IBM, das IBM Logo, [ibm.com](http://ibm.com), IBM Watson, BigFix, MaaS360, QRadar, Trusteer und X-Force sind eingetragene Marken oder Marken der IBM Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicennamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information“ unter [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

Microsoft und Windows sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Dieses Dokument ist zum Datum seiner Erstveröffentlichung aktuell und kann jederzeit von IBM geändert werden. Nicht alle IBM Angebote sind in jedem Land, in welchem IBM tätig ist, verfügbar.

Die Informationen in diesem Dokument werden auf der Grundlage des gegenwärtigen Zustands (auf „as-is“-Basis) ohne jegliche ausdrückliche oder stillschweigende Gewährleistung zur Verfügung gestellt, einschließlich, aber nicht beschränkt auf die Gewährleistungen für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck oder die Freiheit von Rechten Dritter. Für IBM Produkte gelten die Gewährleistungen, die in den Vereinbarungen vorgesehen sind, unter denen sie erworben werden.

Der Kunde ist für die Einhaltung der geltenden Gesetze und Verordnungen selbst verantwortlich. IBM erteilt keine Rechtsberatung und gibt keine Garantie bzw. Gewährleistung bezüglich der Konformität von IBM Produkten oder Services mit den geltenden Gesetzen und gesetzlichen Bestimmungen.

**Erklärung zu geeigneten Sicherheitsvorkehrungen:** Zur Sicherheit von IT-Systemen gehört der Schutz von Systemen und Informationen in Form von Vorbeugung, Erkennung und Reaktion auf unbefugten Zugriff innerhalb des Unternehmens und von außen. Unbefugter Zugriff kann dazu führen, dass Informationen geändert, gelöscht, veruntreut oder missbräuchlich verwendet werden. Ebenso können Ihre Systeme beschädigt oder missbräuchlich verwendet werden, einschließlich zum Zweck von Attacken. Kein IT-System oder Produkt kann umfassend als sicher betrachtet werden. Kein einzelnes Produkt, kein einzelner Service und keine einzelne Sicherheitsmaßnahme können eine unbefugte Verwendung oder einen unbefugten Zugriff mit vollständiger Wirksamkeit verhindern. IBM Systeme, Produkte und Services werden als Teil eines gesetzeskonformen, umfassenden Sicherheitskonzepts entwickelt, sodass die Einbeziehung zusätzlicher Betriebsprozesse erforderlich ist. IBM übernimmt keine Gewähr dafür, dass Systeme, Produkte oder Services vor zerstörerischen oder unzulässigen Handlungen Dritter geschützt sind oder dass Systeme, Produkte oder Services Ihr Unternehmen vor zerstörerischen oder unzulässigen Handlungen Dritter schützen.

© Copyright IBM Corporation 2017



Bitte der Wiederverwertung zuführen