



Principali benefici

- Protezione delle app aziendali mediante inserimento in Container sicuro
 - Incremento della produttività e del grado di soddisfazione dei dipendenti
 - Gestione centralizzata delle app mobili con una console di tipo web
 - Supporto sicuro delle iniziative di BYOD
 - Riduzione del rischio di perdita di dati sensibili
 - Applicazione del controllo degli accessi su dispositivo e della conformità a norme e regolamenti
 - Cancellazione selettiva del catalogo delle app e delle app gestite
 - Impiego di controlli amministrativi granulari e report grafici interattivi
 - Riduzione del carico di rete e incremento delle performance e della scalabilità delle app
-

IBM MaaS360 Mobile Application Management

Per distribuire, gestire e proteggere le app mobili con la massima semplicità

Accesso protetto alle app

Smartphone e tablet stanno trasformando le aziende incrementandone la produttività, migliorando le efficienze e aumentando il grado di soddisfazione dei clienti. La proliferazione dei dispositivi mobili non può però restare incontrollata senza un'adeguata protezione dei dati aziendali sensibili, specialmente nell'era del BYOD (bring your own device).

Non si tratta più semplicemente di controllare l'e-mail e gestire i dispositivi. Le app stanno svelando le autentiche potenzialità dei dispositivi mobili.

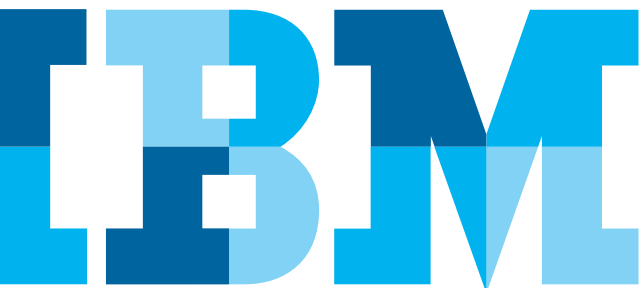
Sono però sempre più fonte di vulnerabilità di sicurezza a causa di procedure di archiviazione dei dati inefficienti, malware, accessi non autorizzati, mancanza di crittografia e perdite di dati derivanti dalla sincronizzazione.

I vostri dipendenti possono installare e utilizzare sui propri smartphone e tablet oltre un milione di app mobili diverse.¹

Le imprese devono poter distribuire, gestire e proteggere le app mobili essenziali per il business su dispositivi personali e di proprietà dell'azienda.

IBM® MaaS360® Mobile Application Management semplifica la gestione delle applicazioni offrendo un catalogo di app aziendali di grande intuitività con solide funzioni di sicurezza e gestione del ciclo operativo delle app.

“Entro il 2017, il 25% delle imprese disporrà di un app store aziendale per la gestione di app approvate su PC e dispositivi mobili”² – Gartner



Catalogo di applicazioni aziendali

- Catalogo di app aziendali intuitivo e personalizzabile, pensato per dispositivi iOS, Android e Windows Phone
- Eccezionale esperienza utente
- Possibilità immediata per gli utenti di visualizzare le app disponibili, installarle e ricevere notifiche di eventuali aggiornamenti
- Distribuzione di una selezione di app pubbliche e aziendali
- Impiego di una console web protetta per la gestione e la distribuzione di app



Figura 1: Esempio di catalogo di app aziendali su dispositivo mobile

Gestione del ciclo di vita delle applicazioni mobili

- Impiego di flussi di lavoro di gestione delle app mobili basati su best practice
- Distribuzione di app e monitoraggio dell'installazione over-the-air (OTA) per tutti gli utenti, i gruppi di utenti o i singoli dispositivi
- Pubblicazione di aggiornamenti delle app
- Report di inventario delle app continuamente aggiornati
- Integrazione con app store pubblici quali Apple App Store, Google Play e Windows Phone Store per flussi di lavoro privi di inconvenienti.

App	Name	Type	Category	Device Type	VPP Codes	Installations
Skype	View Distribute Delete More...	Apple	Social Networking	Tablet, Smartphone		1
Cisco WebEx Meetings	View Distribute Delete More...	Android	Business	Smartphone		1
Salesforce Mobile	View Distribute Delete More...	Android	Business	Smartphone		1
iBooks	View Distribute Delete More...	Apple	Book	Tablet, Smartphone		1
iTunes U	View Distribute Delete More...	Apple	Education	Tablet, Smartphone		0
AnyConnect iOS+	View Distribute Delete More...	Android	Business	Smartphone		0
ADME ERP	View Distribute Delete More...	Apple	Internal Apps	Tablet, Smartphone		0
CDW Events	View Distribute Delete More...	Apple	Social Networking	Tablet, Smartphone		0
LinkedIn	View Distribute Delete More...	Android	Social	Smartphone		0

Figura 2: Esempio di catalogo di app sul portale MaaS360

IBM® MaaS360® Mobile Application Security

- Impiego di un semplice app wrapper o Software Development Kit (SDK) come componente aggiuntivo di sicurezza di MaaS360 Mobile Application Management
- Autenticazione degli utenti prima dell'accesso alle app
- Applicazione dei controlli di conformità dei dispositivi
- Limitazione delle operazioni di copia e incolla e dei backup di dati locali e su cloud
- Ricezione di avvisi in tempo quasi reale delle violazioni della conformità
- Tunneling a livello di app per l'accesso protetto ai dati aziendali senza la necessità di una VPN tra i dispositivi

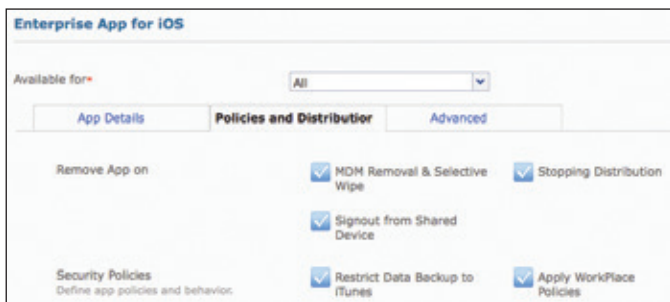


Figura 3: Esempio di opzioni di sicurezza impostabili per un'app

Conformità delle app mobili

- Creazione di blacklist, whitelist e set di app necessarie
- Limitazione delle app native su dispositivo (ad es. YouTube)
- Limitare l'accesso ai dispositivi sottoposti a jailbreaking o rooting
- Configurazione di azioni automatiche per l'imposizione della conformità
- Esecuzione di azioni istantanee tramite l'automazione o l'intervento manuale mirato a bloccare l'accesso alle email, limitare le risorse di rete (ad es. escludendo le VPN) ed eseguire cancellazioni remote
- Visualizzazione di report grafici di cronologia delle operazioni di sicurezza e conformità

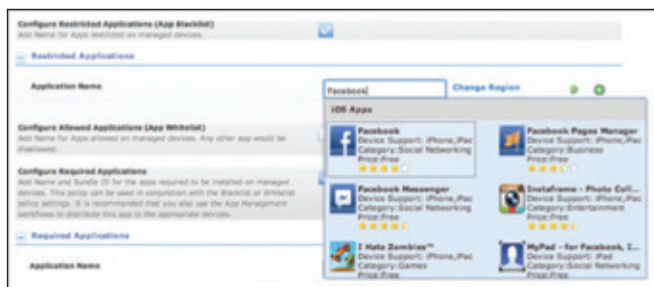


Figura 4: Esempio di come sia possibile inserire un'app in una blacklist per impedirne l'installazione su un dispositivo

Container di app mobili aziendali

MaaS360 Mobile Application Management semplifica la gestione delle applicazioni offrendo un catalogo di app aziendali di grande intuitività con solide funzioni di sicurezza e gestione del ciclo operativo delle app.

Catalogo di applicazioni aziendali

Catalogo di app aziendali intuitivo e personalizzabile, pensato per iOS, Android e Windows Phone.

Gestione del ciclo di vita delle applicazioni mobili

Piattaforma progettata per distribuire, aggiornare e proteggere app mobili pubbliche e aziendali.

MaaS360 Mobile Application Security

Container di applicazioni mobili per app aziendali con gestione della sicurezza integrata come funzione opzionale aggiuntiva di MaaS360 Mobile Application Management.

Conformità delle app mobili

Policy di sicurezza per blacklist, whitelist e set di app necessarie. Regole di applicazione automatiche per avvisare gli amministratori, bloccare l'e-mail, limitare le risorse di rete ed eseguire cancellazioni remote.

IBM® MaaS360® Content Service

Opzione per l'hosting e la distribuzione di app mobili aziendali su una rete globalmente ottimizzata.

Programma di Volume Licensing

Supporto di Volume License per dipendenti.

Per maggiori informazioni sulle soluzioni di prevenzione delle frodi IBM Security, contattate il vostro rappresentante o Business Partner IBM di fiducia o visitate il sito Web al seguente indirizzo: ibm.com/security.



© Copyright IBM Corporation 2016

IBM Italia S.p.A
Circonvallazione Idroscalo
20090 Segrate (Milano)
Italia

Documento redatto negli Stati Uniti d'America,
gennaio 2016

IBM, il logo IBM, ibm.com e X-Force sono marchi di International Business Machines Corp., registrati in molte giurisdizioni del mondo. BYOD360™, Cloud Extender™, Control360®, E360®, Fiberlink®, MaaS360®, MaaS360® e dispositivo, MaaS360 PRO™, MCM360™, MDM360™, MI360®, Mobile Context Management™, Mobile NAC®, Mobile360®, Secure Productivity Suite™, Simple. Secure. Mobility.®, Trusted Workplace™, Visibility360® e We do IT in the Cloud.™ e il dispositivo sono marchi o marchi registrati di Fiberlink Communications Corporation, una società IBM. Altri nomi di prodotti e servizi possono essere marchi registrati di IBM o dei rispettivi titolari. Un elenco dei marchi IBM è disponibile sul Web nella sezione delle informazioni sul copyright e sui marchi, all'indirizzo ibm.com/legal/copytrade.shtml

Apple, iPhone, iPad, iPod touch e iOS sono marchi o marchi registrati di Apple Inc., negli Stati Uniti e in altri Paesi.

Microsoft, Windows, Windows NT e il logo Windows sono marchi di Microsoft Corporation negli Stati Uniti e in altri paesi.

Questo documento è aggiornato alla data iniziale della pubblicazione e può essere modificato da IBM in qualsiasi momento. Non tutte le offerte sono disponibili in ogni Paese in cui IBM opera.

I dati sulle prestazioni e gli esempi dei clienti citati vengono presentati a puro scopo illustrativo. Le prestazioni effettive possono variare in base alle specifiche configurazioni e condizioni operative. È responsabilità dell'utente valutare e verificare il funzionamento di qualsiasi prodotto o programma con i prodotti e i programmi IBM.

LE INFORMAZIONI PRESENTI IN QUESTO DOCUMENTO VENGONO FORNITE COSÌ COME SONO, SENZA ALCUNA GARANZIA, ESPRESSA O TACITA, DI ALCUN TIPO, INCLUSE TUTTE LE GARANZIE DI COMMERCIALIZZABILITÀ, IDONEITÀ PER UN FINE PARTICOLARE O NON VIOLAZIONE DI DIRITTI DI TERZI. I prodotti IBM sono garantiti secondo i termini e le condizioni dei contratti in base ai quali vengono forniti.

Il cliente ha la responsabilità di garantire la conformità alle normative e ai regolamenti applicabili. IBM non fornisce consulenze legali né garantisce che i suoi servizi o prodotti assicurino la conformità del cliente a normative o regolamenti.

Qualsiasi riferimento alle future intenzioni di IBM e al suo orientamento è soggetto a modifica o ritiro senza preavviso e deve intendersi unicamente come obiettivo prefissato dell'azienda.

Dichiarazione relativa alla validità delle procedure di sicurezza: la sicurezza dei sistemi IT implica la protezione dei sistemi e delle informazioni tramite la prevenzione, il rilevamento e la gestione degli accessi non autorizzati provenienti dall'interno e dall'esterno dell'azienda. L'accesso non autorizzato può determinare la modifica, la distruzione o l'uso inappropriato delle informazioni o causare danni o utilizzi impropri dei sistemi, con eventuali attacchi ad altri. Nessun sistema o prodotto IT può essere considerato assolutamente sicuro e nessun prodotto o misura di sicurezza può essere totalmente efficace per la prevenzione dell'accesso non autorizzato. I sistemi e i prodotti IBM sono progettati come parte integrante di un approccio esaustivo alla sicurezza, che implica necessariamente altre procedure operative e può richiedere altri sistemi, prodotti o servizi per garantire la massima efficacia. IBM non garantisce che sistemi e prodotti siano immuni da condotte dannose o illegali perpetrate da qualsiasi altro soggetto.

1 Numero di app disponibili nei principali app store dal mese di luglio 2014, Statista, <http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/>

2 "Gartner Says That by 2017, 25 Percent of Enterprises Will Have an Enterprise App Store", comunicato stampa di Gartner Group, 12 febbraio 2013, <http://www.gartner.com/newsroom/id/2334015>



Riciclare