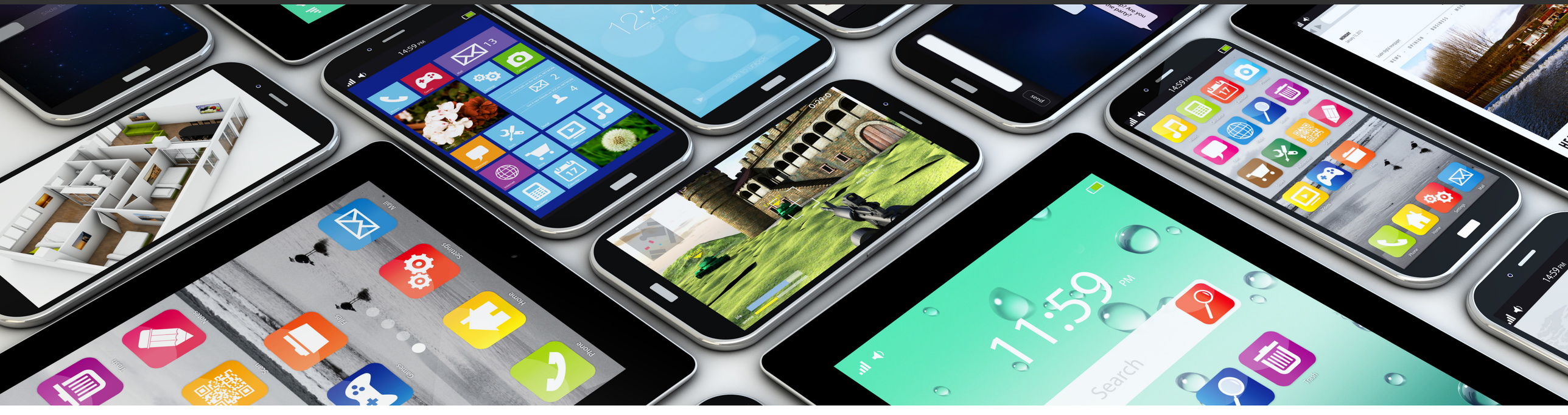
IBM MaaS360 | With Watson

IBM Security

IBM



White Paper di IBM Security Thought Leadership

11 best practice per la MDM (mobile device management – gestione dei dispositivi mobili)

Come gestire e proteggere i dispositivi mobili nell'azienda

Restare a galla nella marea di dispositivi mobili

I dispositivi sono entrati a far parte così profondamente delle nostre vite – personali e lavorative – che è quasi impossibile tornare con la mente ad un tempo in cui non erano a nostra disposizione. Le aziende di oggi e i loro dipendenti si affidano ai dispositivi per un numero così grande e un assortimento talmente vasto di casi di utilizzo che l'importanza di una loro efficace gestione non è mai stata più rilevante.

I moderni leader di IT e sicurezza stanno affrontando la difficoltà di fornire, gestire e proteggere i dispositivi mobili nei rispettivi ambienti aziendali. Ora, grazie all'utilizzo sul posto di lavoro di smartphone, tablet, PC e Mac, l'IT ha bisogno di un'unica piattaforma, in grado di gestire tutti i dispositivi – indipendentemente dal tipo.

Anche se potrebbe sembrare complesso, l'approccio da adottare per la gestione di questi dispositivi è relativamente semplice. Attieniti a questi 11 passi e sarai sulla strada giusta per gestire in modo efficace la tecnologia mobile nella tua azienda.

11 best practice per l'MDM

1. Stai attento a quello che fai
2. Non devi fare tutto da solo
3. Prova prima di acquistare
4. La conoscenza è potere
5. Andare dalla visione d'insieme al succo della questione
6. Automatizza, segnala e correggi
7. Blocca il dispositivo
8. Solo le app giuste
9. Politiche: Il sale della vita
10. 'Quanti dati hai utilizzato?!'
11. Fa gioco di squadra

1

Stai attento a quello che fai

Prima di iniziare a pensare ai vari modi in cui gestirai i tuoi dispositivi, innanzitutto devi capire quali tipi di dispositivi sono in uso nel tuo ambiente. Ecco alcune domande a cui tutti i professionisti IT dovrebbero rispondere durante la loro valutazione iniziale:

- **Quali tipi di dispositivi sto gestendo?**
  - Apple iOS o macOS? Google Android? Microsoft Windows?
- **Quanti dispositivi sono in uso nel mio ambiente?**
  - Dove devo rivolgermi per ottenere il numero definitivo?
- **Quali sono i casi di utilizzo relativi ai miei dispositivi?**
  - Di quali applicazioni (app) specifiche ho bisogno per determinate attività?
- **A cosa si connettono internamente i miei dispositivi?**
  - Microsoft Exchange ActiveSync? Microsoft Active Directory? Google Apps? EWS? IBM Notes Traveler?

Solo dopo aver risposto a queste domande è possibile iniziare a pianificare i passi successivi per l'implementazione della soluzione MDM.

2

Non devi fare tutto da solo

Prima di intraprendere realmente i passi iniziali nel percorso verso l'adozione della tecnologia mobile, quello che ci aspetta può apparire scoraggiante. Sei sotto pressione perché devi assicurarti che tutti i dispositivi siano documentati e funzionino correttamente – ma non sei sicuro di come terrai traccia di tutti questi dispositivi.

Assicurati di valutare uno strumento MDM che abbia una valida rete di partner, su cui contare al momento dell'esecuzione della tua strategia – o che sia dotata di un framework in grado di supportarti prima di iniziare l'implementazione.

Un valido provider di MDM potrà contare su rivenditori, MSP (managed service provider – provider di servizi gestiti), gestori e partner di altro tipo con cui potrai collaborare strettamente per valutare i tuoi obiettivi e assicurarti che i passi per raggiungerli vengano eseguiti correttamente.

Se il tuo team IT si rimboccherà le maniche e si occuperà direttamente della gestione, assicurati di collaborare con un vendor che includa supporto pre e post-vendita complementare – e che sia preparato a offrirti assistenza dall'inizio alla fine.

Un programma di servizi per l'esito positivo dell'adozione di dispositivi mobili non dovrebbe essere considerato un bonus aggiunto; dovrebbe essere un'aspettativa. Assicurati che la tua soluzione MDM disponga di vari pacchetti di servizi tra cui scegliere, che ti consentiranno di realizzare il massimo ROI (return on investment-rendimento dell'investimento). Assicurati di collaborare con persone che abbiano già raggiunto questi obiettivi, che sappiano cosa stai cercando di realizzare e che possano, quindi, aiutarti ad ottenerlo.

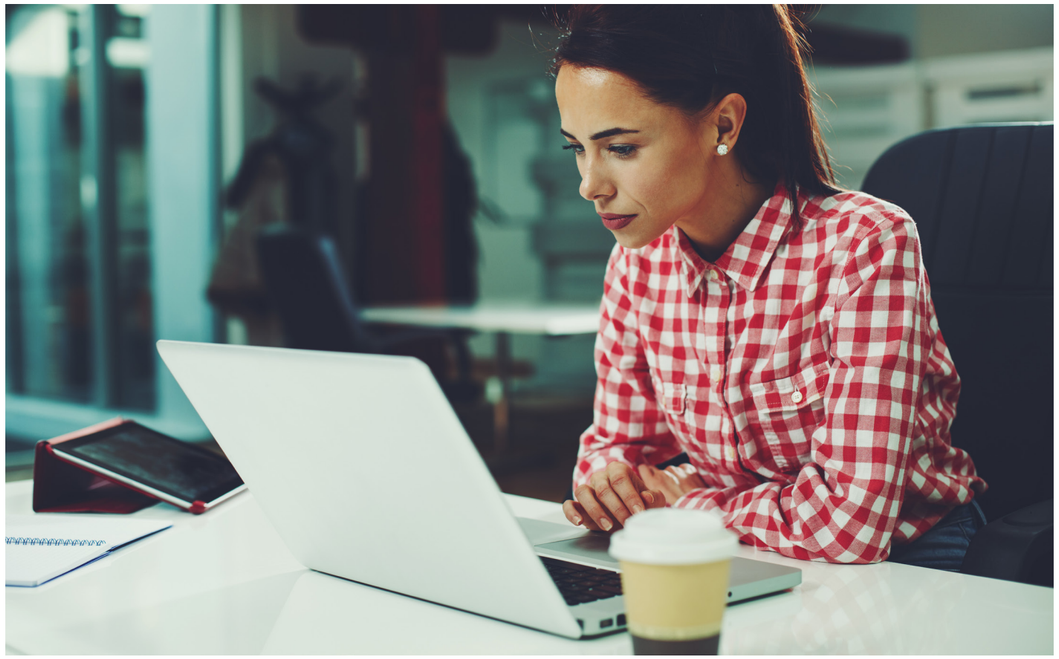
3

Prova prima di acquistare

In ogni caso, dovrebbe essere facile iniziare a utilizzare la tua soluzione MDM. Assicurati che la tua offra accesso gratuito a un portale di produzione completa (non 'lite' o limitato), dove potrai iniziare a registrare i dispositivi e sottoporre a test le funzioni nel giro di pochi minuti. Per maggiore comodità, assicurati che il portale abbia un modello di distribuzione cloud, così potrai iniziare a utilizzarlo direttamente dal tuo browser preferito.

Una volta creato l'account ed effettuato l'accesso al portale, la registrazione dei dispositivi dovrebbe essere un processo lineare. Assicurati che sia semplice:

- **Registrare il tuo primo dispositivo**
  - Sia che si tratti di un iPhone o iPad Apple, di un Android o di un tablet Windows 10,dovresti riuscire a predisporre e configurare rapidamente il dispositivo.
- **Configurare e pubblicare la tua serie iniziale di politiche**
  - I tuoi dispositivi dovranno essere protetti mediante passcode? Desideri che le fotocamere vengano disabilitate? La connessione Wi-Fi è importante? Le opzioni di personalizzazione dovrebbero essere complete.
- **Escludere alcune app**
  - Tornando ai casi di utilizzo, quali app fanno parte integrante del tuo ambiente? Inizia per prima cosa da queste.



Una volta acquisita una certa familiarità con il portale e iniziato a svolgere specifiche azioni, assicurati anche di chiudere il cerchio con i dispositivi sottoposti a test.

- Il processo di registrazione risulta rapido, facile e privo di interruzioni?
- Le politiche che hai configurato ed emesso stanno entrando in vigore?
- È facile trovare, accedere e utilizzare le app mobile che sono state distribuite nei dispositivi?

4

La conoscenza è potere

Sia che tu abbia già qualche esperienza o che tu stia adottando per la prima volta una soluzione MDM, il processo di apprendimento dovrebbe essere rapido, intuitivo e interessante. Dal momento che ogni soluzione ha una configurazione differente, il processo potrebbe essere un po' disorientante, quando si passa da una soluzione alla successiva. La cosa migliore è condurre un'adeguata valutazione, per stabilire quali risorse sono a propria disposizione. Quando si esaminano le funzionalità del supporto tecnico per una soluzione, ci si dovrebbe porre le seguenti domande:

- **Che tipo di supporto ho a disposizione?**
  - Come minimo, alla soluzione dovrebbe essere assegnato un numero di help desk dedicato oppure una funzione di chat online, che consentirà di parlare immediatamente con un rappresentante del supporto.
- **Esiste un manuale per il proprietario?**
  - Le guide e la documentazione relative al portale, che spiegano come ricavare il massimo dalla propria esperienza, sono essenziali per l'esito positivo dell'implementazione.
- **Sono disponibili video illustrativi, nel caso non si abbia il tempo di leggere il manuale per il proprietario?**
  - Sia che tu preferisca apprendere visivamente o che tu sia molto impegnato, i supporti didattici video possono rappresentare il modo più semplice per ottenere la guida dettagliata di cui si ha bisogno e dovrebbero essere inclusi nella propria offerta di soluzione.

Non si dovrebbe mai avere la sensazione di rimanere all'oscuro e dovrebbe esserci una grande quantità di aree da visitare per ottenere spiegazioni sull'MDM. Fai domande – ottieni risposte. Non dovrebbe mai essere più difficile di così.

5

Andare dalla visione d'insieme al succo della questione

L'azienda è piena di endpoint differenti – di qualsiasi tipo: smartphone, tablet e laptop, dispositivi indossabili e dispositivi IoT (Internet of Things). Non dimentichiamo varie integrazioni per email, utenti directory e accesso sicuro ai documenti. Di qualunque cosa si debba tenere traccia, la propria soluzione MDM dovrebbe consentire l'accesso tramite una singola console nella quale si possano visualizzare endpoint, utenti finali e tutti i dispositivi necessari a connetterli.

Ecco tre best practice da prendere in considerazione nella scelta della propria soluzione MDM, basate sulle necessità essenziali:

- Assicurarsi che il proprio strumento di reportistica e inventario sia in grado di consolidare tutti i dispositivi registrati e le informazioni associate all'interno di report di facile consultazione. Si arriverà a fare affidamento su aggiornamenti quotidiani, quindi, dovrebbero essere generati automaticamente, senza input manuale.
- Oltre ai vantaggi dell'accessibilità immediata offerti dall'MDM su cloud, non dovrebbero essere necessari l'acquisto, l'installazione o la manutenzione di hardware – quindi, nessuna tariffa associata. La piattaforma dovrebbe essere aggiornata automaticamente con le nuove funzioni disponibili.
- La capacità di ricercare con facilità qualsiasi cosa è fondamentale per una soluzione basata sul cloud. Dovresti essere in grado di accedere ai tuoi dispositivi, integrazioni, report, app e documenti protetti con un semplice clic del mouse.

6

Automatizza, segnala e correggi

La protezione dei dati aziendali è una delle massime priorità per i moderni leader dell'IT e della sicurezza – e, non è una sorpresa, anche una delle maggiori difficoltà. La soluzione MDM dovrebbe essere dotata di valide funzionalità di sicurezza, facili da utilizzare.

Con dati sensibili sui dispositivi sia aziendali che dei dipendenti, dovrebbe essere possibile rilevare e controllare gli accessi effettuati. Gli strumenti di segnalazione devono fornire informazioni approfondite sull'inventario dei dispositivi, sui rischi per la sicurezza e sulla conformità. Ecco alcuni aspetti da prendere in considerazione quando si tratta di segnalazioni:

- I dispositivi possono segnalare le rispettive posizioni per un periodo di tempo, in modo da poter sapere dove sono stati.
- Se un dispositivo non è conforme alle politiche aziendali, segnalazioni e avvisi possono essere generati e inviati immediatamente allo staff IT.
- La correzione in caso di violazioni dovrebbe essere repentina e automatica e includere il blocco del dispositivo, la cancellazione selettiva o gli interventi aziendali appropriati da parte del reparto delle Risorse umane. Tutti questi punti possono essere visualizzati in un semplice report, che può essere esportato per l'archiviazione aziendale.

7

Blocca il dispositivo

Con l'emergere delle iniziative BYOD (bring-your-own-device), le organizzazioni corrono il rischio di esporre le informazioni aziendali sui dispositivi personali dei dipendenti. Tuttavia, la tua soluzione MDM dovrebbe prevedere una qualche forma di isolamento dei dati aziendali. L'idea è quella di separare il lavoro dal tempo libero, così il tuo team IT avrà maggiore controllo sui dati a cui l'utente ha accesso – e, in modo più specifico, chi ha accesso ai dati su quel determinato dispositivo. La tua soluzione MDM dovrebbe essere in grado di fornire specifiche linee guida per l'accesso ai dati protetti e dovrebbe intraprendere delle azioni nel caso di una potenziale violazione, ad esempio perdita o furto di un dispositivo.

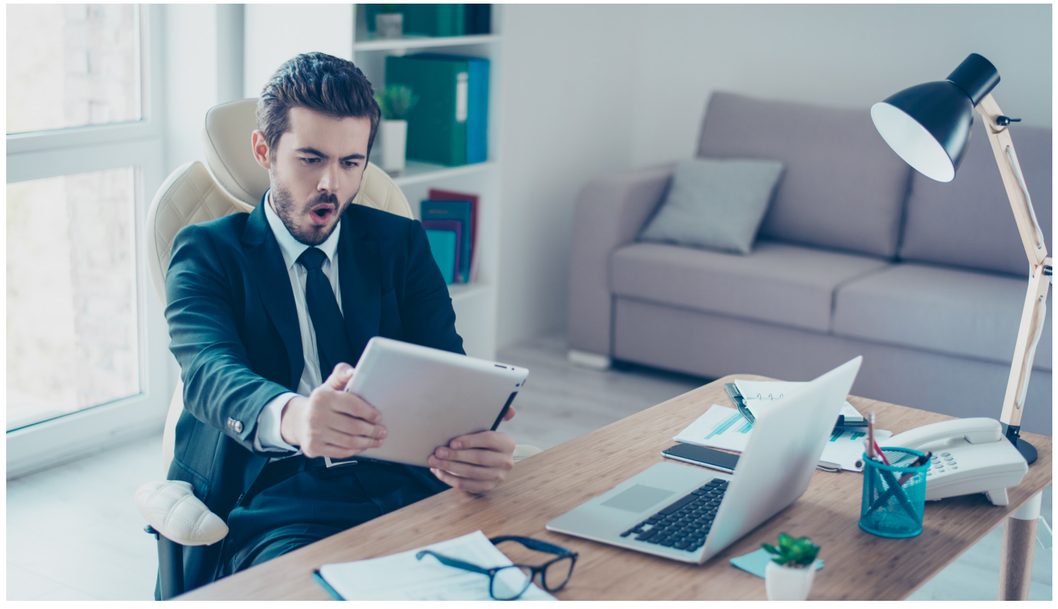
Quando si valuta un isolamento sicuro, è opportuno chiedersi:

- **Cosa dovrei fare se un dispositivo viene perso o rubato? Come posso proteggere i dati della mia organizzazione?**
  - La tua soluzione MDM dovrebbe essere in grado di localizzare da remoto, bloccare un dispositivo e cancellarne il contenuto. Alcune soluzioni offrono una funzione di 'cancellazione selettiva', che interesserà solo i dati e le impostazioni distribuiti sul dispositivo e lascerà inalterate le informazioni personali.
- **Come posso bloccare i miei dati aziendali?**
  - La procedura per bloccare i dati è semplice. Nella maggior parte dei casi, è possibile impostare la sicurezza dei dati aziendali tramite una politica e applicarla all'utente e/o al dispositivo. La sicurezza può includere protezione mediante passcode per l'app MDM e restrizioni basate sul tempo riguardo alla possibilità di accesso da parte degli utenti ai dati aziendali, tra cui email e documenti.

8

Solo le app giuste

Con l'avvento di una schermata home personalizzata, l'organizzazione può decidere quali app verranno visualizzate sui dispositivi aziendali e vietare agli utenti app non essenziali. I dispositivi Android e iOS possono abilitare un 'chiosco' del dispositivo, dove gli utenti possono visualizzare solo le app approvate dall'azienda e niente altro. Limitare l'accesso alle app significa per un utente minore probabilità di violare la politica aziendale; con il risultato di rendere più facile la gestione del dispositivo. Inoltre, quando sul dispositivo non sono installati giochi o app non approvate dall'azienda, gli utenti saranno più produttivi.



9

Politiche: Il sale della vita

Quando si definisce la propria strategia MDM, è opportuno tenere a mente di che tipo di politiche per i dispositivi si avrà bisogno. Una soluzione MDM dovrebbe offrire una politica personalizzabile, che possa essere basata su precedenti iterazioni – per non parlare della possibilità di adattare un numero illimitato di politiche. In questo modo, si potrà avere una serie di politiche completamente personalizzate per le esigenze specifiche della propria azienda, con un preavviso minimo. Come bonus aggiunto, la tua soluzione MDM dovrebbe offrire funzionalità di benchmarking con origine nel cloud, che consentiranno di confrontare le proprie configurazioni con quelle di altre aziende delle stesse dimensioni e nello stesso settore d'industria.

- **Perché vengono consigliate molteplici politiche?**
  - Le politiche possono essere applicate a un singolo utente/dispositivo, a un gruppo definito o a chiunque nell'azienda. Molteplici politiche possono anche essere utilizzate se e/o quando un dispositivo risulta non conforme e devono essere applicate misure di sicurezza.
- **Cosa dovrei cercare in una politica?**
  - Dovresti essere in grado di modificare facilmente aspetti dettagliati del funzionamento del dispositivo, per soddisfare le esigenze della tua organizzazione. Dovresti anche essere in grado di impostare profili per funzionalità Wi-Fi, email e VPN (virtual private network).

10

‘Quanti dati hai utilizzato?!’

Troppo spesso, uno dei principali punti dolenti, per quanto riguarda i dispositivi aziendali, è rappresentato dall’utilizzo dei dati presenti sul cellulare. Con l’ascesa dei servizi di video e musica in streaming, si può perdere il controllo dell’utilizzo dei dati in modo abbastanza rapido, così che la bolletta sarà più gravosa. La propria soluzione MDM dovrebbe essere in grado di integrarsi con tutti i principali gestori della zona.

L’organizzazione ha la possibilità di impostare dei limiti di dati, per avvisare utenti e staff nel caso si stiano avvicinando, o stiano superando, la rispettiva assegnazione mensile. Insieme a questi avvisi, sono previste azioni automatiche, che è possibile intraprendere nei confronti degli utenti, in caso di necessità. La cosa migliore è discutere con il proprio gestore di tecnologia wireless su cosa si può fare per impedire agli utenti di eccedere nell’uso dei dati.

- Scopri in che modo il tuo gestore può aiutarti a contenere le eccedenze dei dati.
- La tua soluzione MDM dovrebbe essere in grado di integrarsi con il tuo gestore.
- I report sull’utilizzo dei dati dovrebbero fare parte della tua offerta di soluzione.

11

Fa gioco di squadra

La tua soluzione MDM dovrebbe essere in grado di integrarsi con le soluzioni dei produttori di dispositivi mobili, ad esempio profili di lavoro Android, Samsung Knox, Apple’s Device Enrollment Program (DEP) e Apple’s Volume Purchase Program (VPP). Queste integrazioni saranno i fattori principali del successo dell’MDM, possono semplificare la gestione complessiva e fare risparmiare tempo, denaro e stress.

Informazioni su IBM MaaS360 con Watson

Migliaia di organizzazioni di tutte le dimensioni, in tutti settori d'industria, si affidano a IBM MaaS360 con Watson come base per la loro trasformazione digitale con endpoint e dispositivi mobili. Come prima e unica piattaforma UEM (unified endpoint management – gestione endpoint unificata) cognitiva, MaaS360 mette a disposizione intelligence aumentata, analytics contestuale e controlli di sicurezza avanzati di utenti, dispositivi, app e contenuto per supportare implementazioni di endpoint e dispositivi mobili. Fornito dal migliore IBM Cloud della categoria su una piattaforma affidabile e consolidata, MaaS360 aiuta a gestire un'ampia gamma di dispositivi per più utenti, da un'unica console e consente l'integrazione con soluzioni offerte da Apple, Google, Microsoft e altri fornitori di strumenti di gestione. IBM collabora con questi fornitori, non solo per consentire l'integrazione, ma anche per garantire che tale integrazione possa realizzarsi non appena siano disponibili nuovi strumenti o aggiornamenti.

Per ulteriori informazioni

Per ulteriori informazioni su MaaS360 e per iniziare una versione di prova gratuita per 30 giorni, visitare: **ibm.com**/it/maas360-trial

Informazioni sulle soluzioni di IBM Security

IBM Security offre una delle più avanzate ed integrate serie di prodotti e servizi per la sicurezza aziendale. Il portafoglio, supportato da esperti di ricerca e sviluppo IBM X-Force, notissimi in tutto il mondo, fornisce intelligence di sicurezza per aiutare le organizzazioni a proteggere a 360 gradi il proprio personale, le infrastrutture, i dati e le applicazioni, offrendo soluzioni per la gestione di identità ed accessi, la sicurezza del database, lo sviluppo delle applicazioni, la gestione dei rischi, la gestione degli endpoint, la sicurezza della rete ed altro ancora. Queste soluzioni consentono alle organizzazioni di gestire in modo efficace i rischi e di implementare la sicurezza integrata per dispositivi mobili, cloud, social media ed altre architetture di business aziendali. IBM rappresenta una delle più vaste organizzazioni di ricerca, sviluppo e distribuzione di soluzioni per la sicurezza nel mondo, monitora al giorno 30 miliardi di eventi legati alla sicurezza, in oltre 130 paesi e detiene oltre 3.000 brevetti di sicurezza.

Inoltre, IBM Global Financing fornisce numerose opzioni di pagamento per facilitare l'acquisto della tecnologia necessaria per espandere il proprio business. Forniamo gestione dell'intero ciclo di vita dei prodotti e dei servizi IT, dall'acquisto allo smaltimento. Per ulteriori informazioni, visitare il sito: **ibm.com**/it/financing/it

IBM MaaS360

With Watson™

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

La home page di IBM Italia si trova all'indirizzo:
ibm.com

WGW03350-ITIT-00