IBM Security
White paper sulla leadership di pensiero

Mobilizzazione delle applicazioni e dei contenuti aziendali

Come mettere a disposizione delle imprese una modalità di collaborazione mobile semplice e protetta

IBM

La strategia mobile per una nuova era

D: Ha adottato una strategia mobile efficace?

R: Strategia mobile? Vuole sapere se i nostri dipendenti possono accedere alle e-mail dai loro dispositivi mobili? Sì, abbiamo una strategia mobile.

Se questa è la vostra risposta, sappiate che non siete gli unici a pensarla così. Molte aziende sono ancora dell'idea che la posta elettronica sia il mezzo di comunicazione migliore per i dipendenti fuori ufficio. Lo è stato fino a un paio di anni fa. Ma non possiamo certo sostenere che controllare la propria casella di posta e rispondere ai messaggi quando si è fuori sede sia "lavorare", tutt'al più si tratta di "attività di facciata". Oggi la collaborazione mobile ha il potere di sbloccare la vera produttività e facilitare concretamente il lavoro in tempo quasi reale, ma molte aziende devono ancora accettare, pianificare e implementare una strategia mobile efficace, che permetta di utilizzare tutta la potenza della mobilità con un accesso semplice e protetto alle risorse aziendali.

In questo documento discuteremo di come sia possibile applicare il monitoraggio continuo a computer portatili, computer desktop e altri dispositivi endpoint.

In questo white paper, vedremo come:

- Abilitare un accesso mobile protetto ai dati aziendali, senza l'utilizzo di VPN sul dispositivo
- Utilizzare in mobilità SharePoint, la condivisione file di Windows e i siti intranet
- Proteggere i dati aziendali sensibili con efficaci criteri di sicurezza e controlli DLP
- Fornire l'accesso mobile senza modificare la configurazione di sicurezza della rete o del firewall
- Consentire agli utenti in viaggio di collaborare utilizzando i propri dispositivi personali

Continuate a leggere per sapere come fare per consentire ai dipendenti di accedere alle risorse protette dal firewall, salvaguardando i dati con criteri di autorizzazione, crittografia e containerizzazione.

Accesso semplice e sicuro

Ecco una sfida semplice: costruire una casa perfettamente sicura, in grado di proteggere tutti i vostri oggetti di valore. Che approccio scegliete? Potreste optare per una casa senza finestre né porte, priva di qualunque ingresso o uscita. Si tratta certamente di una soluzione sicura, ma non molto utile nella vita reale. Oppure potreste costruire una casa con finestre e porte dotate di serrature inattaccabili ed efficienti sistemi di sicurezza, per ottenere lo stesso livello di sicurezza offerto dalla prima opzione, e in più la possibilità di entrare, uscire, accogliere i visitatori e far passare l'aria senza mettere a rischio i vostri beni.

La vostra strategia mobile potrebbe assomigliare a una casa senza finestre né porte. Oppure a una casa con porte e finestre che non si chiudono. Dovete proteggere i contenuti aziendali, ma dovete anche renderli disponibili, affinché gli utenti possano essere produttivi. Elenchi di contatti clienti, dati dei pazienti, informazioni finanziarie, file di Risorse umane, applicazioni aziendali o verbali delle sedute del consiglio di amministrazione: il numero di informazioni a cui i vostri collaboratori vogliono accedere cresce ogni giorno e bloccarne l'accesso non ha più senso. Porte e finestre sono necessarie, così come un sistema di sicurezza che garantisca il passaggio solo a coloro che ne hanno diritto.

Cosa succede se in ufficio un utente scarica i contatti commerciali sul proprio smartphone o tablet personale? E se invia i rapporti finanziari al proprio indirizzo e-mail di casa, per poter lavorare la sera, dopo che i bambini sono andati a dormire? E che dire dei fornitori? Condividere i contenuti e le applicazioni permette di collaborare in modo più efficiente, ma cosa succede una volta terminato il progetto?

Queste situazioni sono all'ordine del giorno. Le persone trovano sempre il modo di ottenere le informazioni di cui hanno bisogno, mettendo però spesso a repentaglio la sicurezza dei dati aziendali. Occorre consentire loro di usare un metodo sicuro, affidabile e semplice per ottenere ciò di cui hanno bisogno.

Considerazioni sui contenuti

I contenuti aziendali vengono archiviati su reti aziendali tramite la condivisione file di Windows, SharePoint, i siti intranet e le applicazioni Web. Le informazioni necessarie per collaborare con colleghi, partner e clienti e svolgere il proprio lavoro sono bloccate in unità interne e archivi dati, knowledge base, wiki interne, ERP, SCM, HRM, CRM e altri sistemi o processi di gestione.

Come comportarsi con i lavoratori fuori sede, che necessitano di un accesso in mobilità, molto spesso da dispositivi che non sono quelli aziendali?

Oltre a proteggere i dati e le reti interne, le condivisioni di file e i sistemi di archiviazione, occorre tenere presente anche le seguenti considerazioni al momento di decidere quale strategia mobile adottare. Alcune possono sembrare ovvie, ma vale comunque la pena soffermarcisi.

1. I contenuti devono essere accessibili on-demand agli utenti attraverso un approccio di tipo “push” o “pull”
2. Ogni utente deve avere accesso solo ai contenuti di cui ha bisogno, in base al contesto e all'identità
3. I dati devono essere aggiornabili e sincronizzati tra i vari dispositivi
4. Il processo di accesso ai dati non deve essere oneroso per l'utente
5. La gestione della sicurezza non deve essere costosa, pur trattandosi di un investimento importante
6. La gestione della sicurezza non deve rubare troppo tempo all'IT
7. I dati in movimento devono essere crittografati e protetti
8. I dati non devono lasciare l'organizzazione senza autorizzazione
9. I dati creati e memorizzati nelle app devono essere salvaguardati
10. Dal momento che i dispositivi personali non sono di proprietà dell'organizzazione, c'è un limite al controllo che può essere esercitato

Uno degli obiettivi più importanti di qualsiasi legislazione sulla sicurezza informatica deve essere quello di consentire a chi si difende di agire con la stessa rapidità dei malfattori che attaccano i sistemi.

Tecnologie correnti

Diamo uno sguardo alle tecnologie in uso oggi e ad alcune delle questioni inerenti alla sicurezza e la produttività.

Posta elettronica

La posta elettronica è l'applicazione d'elezione per la collaborazione, ma è solo uno dei tanti strumenti.

Non è progettato per la collaborazione. La posta elettronica supporta un tipo di comunicazione “da uno a uno” o “da uno a molti”, ma non l'interazione “da molti a molti” di cui gli utenti hanno bisogno per essere veramente produttivi. Questo approccio facilita l'accumulo di informazioni non smaltite tra gruppi che dovrebbero lavorare insieme.

Le informazioni inviate per posta elettronica possono facilmente diventare vecchie; chi continua a lavorare su un foglio di calcolo ricevuto per e-mail, ad esempio, potrebbe non rendersi conto che il foglio è stato sostituito da una copia più attuale.

Il problema maggiore è che i dati possono essere tagliati, incollati e inoltrati a destinatari che non dovrebbero riceverli.

VPN

Il ricorso a una VPN è una scelta comune per fornire un accesso protetto dal firewall.

Purtroppo, l'obbligo all'accesso deteriora l'esperienza utente. Dovendo scegliere tra contenuti nuovi ma difficili da raggiungere e i contenuti di vecchi allegati e-mail, non più aggiornati ma facili da raggiungere, la tentazione di optare per la strada più semplice è molto forte.

Le VPN richiedono licenze per ogni dispositivo, il che comporta un aumento dei costi mensili che nel tempo potrebbe pesare. Inoltre, è stato dimostrato che l'accesso a una VPN scarica più rapidamente la batteria del dispositivo mobile.

Poiché i dispositivi mobili utilizzano la tecnologia wireless per la connessione, la crittografia è importante. Tuttavia, c'è la questione dell'accesso in roaming. In genere, le soluzioni che si basano sulla crittografia di alto livello diventano inutili quando gli utenti effettuano il roaming tra i punti di accesso. Per fortuna esistono soluzioni a questo problema.

Virtualizzazione dei desktop

Alcune applicazioni consentono di visualizzare un desktop sui dispositivi mobili. In questo modo, tutti gli elementi accessibili dal desktop sono disponibili anche sullo smartphone o sul tablet. Si tratta però di un'opzione generalmente costosa, caratterizzata da un'esperienza utente insoddisfacente. Con questo approccio, la disponibilità e le prestazioni dipendono dalla connettività di rete. Le dimensioni e la risoluzione dello schermo rappresentano un altro problema, soprattutto sugli smartphone con display piccoli. Le applicazioni ottimizzate per un ambiente desktop possono essere accessibili su un dispositivo mobile tramite la virtualizzazione desktop, ma questo non significa che siano utilizzabili.

Un'altra considerazione importante è che i server e le risorse di rete devono essere in grado di supportare la connessione contemporanea di numerosi dispositivi.

Condivisioni di file di terze parti

Le condivisioni di file di terze parti consentono di conservare i file nel cloud. Uno dei maggiori problemi in questo caso è l'assenza di controllo da parte dell'utente. Il contenuto può essere inviato a chiunque, può essere accessibile da chiunque e si possono avere problemi di controllo della versione.

Per non parlare della cattiva esperienza utente. Agli utenti non piace essere costretti a imparare a utilizzare un nuovo software solo per poter accedere ai contenuti di cui hanno bisogno; inoltre, è importante anche tenere in considerazione il tempo necessario all'apprendimento.

Le condivisioni di file di terze parti possono anche essere costose: l'aggiunta di nuovi utenti comporta l'aggiunta di licenze, e potrebbe non essere possibile utilizzare gli investimenti esistenti, come le app e gli archivi di contenuti.

App di terze parti e personalizzate

Se ricorrete a uno sviluppatore esterno per le vostre app dipenderete dal fornitore. La prevenzione di perdita di dati (DLP) potrebbe non essere integrata nell'app.

Potete cercare di sviluppare le vostre app, ma in tal caso dovrete disporre del personale necessario per supportarle e apportare le eventuali modifiche rese necessarie dall'introduzione di nuovi tipi di dispositivi, aggiornamenti del sistema operativo, ecc.

Molti esperti di sicurezza, i migliori funzionari di sicurezza informatica del governo e i leader politici si auspicano che venga posta una maggiore enfasi sul monitoraggio continuo, sugli strumenti di monitoraggio automatico e sulla capacità di reazione rapida agli attacchi sferrati ai sistemi informatici.

L'importanza dei criteri di sicurezza

Se avete intenzione di consentire agli utenti di accedere alle risorse aziendali con i loro dispositivi personali, dovrete creare dei criteri che regolamentino il modo in cui i dati vengono resi accessibili e utilizzabili.

Potreste richiedere l'inserimento di una password per poter accedere ai dati importanti.

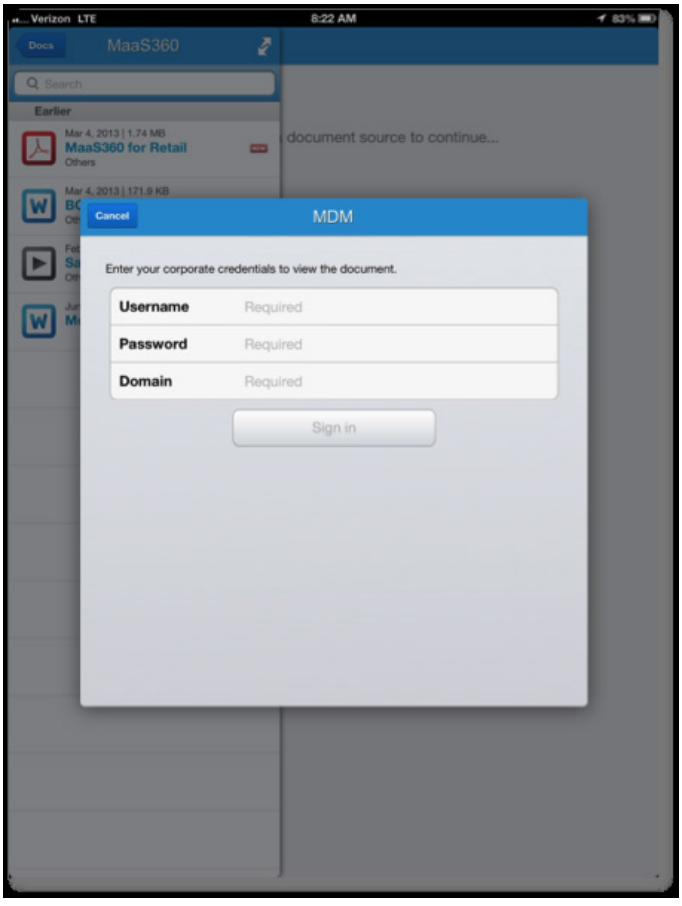

Figura 1 - Una richiesta di autenticazione

Potreste limitare la funzione di taglia e incolla dei documenti.

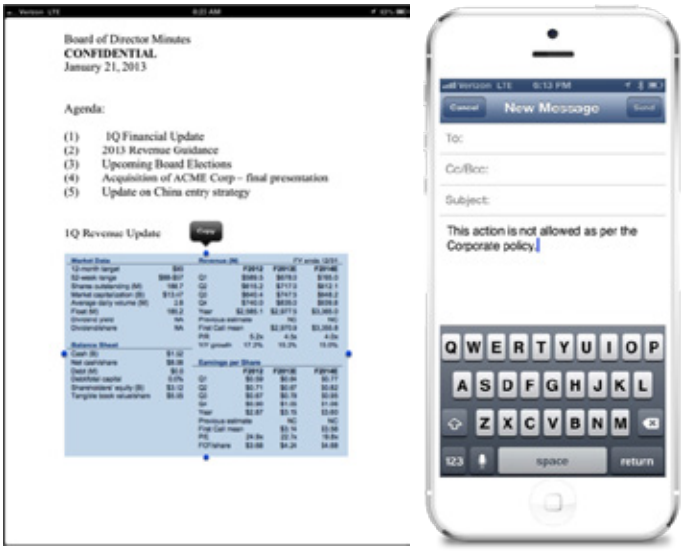

Figura 2 - Controlli per impedire le perdite di dati, come ad esempio l'imposizione di restrizioni sulle operazioni di copia e incolla

IBM® MaaS360® Productivity Suite

MaaS360 Productivity Suite contribuisce a superare le sfide poste dalle tecnologie attuali, perché è stata progettata per consentire diverse possibilità di accesso sicuro e protezione dei dati a riposo:

1. IBM® MaaS360® Secure Mobile Mail
2. IBM® MaaS360® Mobile Application Security
3. IBM® MaaS360® Secure Mobile Browser

MaaS360 utilizza un “contenitore”, ospitato in un'area protetta del dispositivo, per consentire l'approccio “dual persona” a dati, app e contenuti. Siete voi a decidere quali controlli adottare per l'area protetta, in modo che l'accesso a e-mail, contatti, calendari, app (e relativi dati), documenti e pagine Web sia sicuro.

Figura 3 - MaaS360 Productivity Suite e MaaS360 Content Suite

MaaS360 Productivity Suite utilizza criteri personali per specificare i livelli di sicurezza che saranno adottati su tutti i dispositivi dell'utente. I criteri vengono creati nel portale MaaS360 e distribuiti via etere a tutti i dispositivi registrati, in modo tale che non sia necessario agire fisicamente sui dispositivi.

Quando un dispositivo non è più conforme, o il progetto è terminato e si è concluso il rapporto con il fornitore, è possibile eliminare il “container” da remoto e di conseguenza tutti i dati e le app.

Il “container” è dotato di funzioni di sicurezza integrata, tra cui la conformità FIPS 140-2 e la crittografia AES-256. È possibile chiedere agli utenti di inserire un codice di accesso. È, inoltre, possibile configurare le impostazioni in modo che il “container” venga completamente rimosso in caso di dispositivi soggetti a jailbreak o root oppure se i dispositivi non hanno risposto al controllo entro un determinato periodo di tempo.

È, inoltre, possibile impedire che i file presenti nel “container” vengano spostati, copiati o stampati, o che file esterni vengano importati nel “container”.

IBM® MaaS360® Content Suite

MaaS360 Content Suite fornisce un “container” crittografato e strumenti di produttività con i quali distribuire, visualizzare, creare, modificare e condividere documenti sui dispositivi mobili, offrendo alle organizzazioni il controllo di cui hanno bisogno e ai dipendenti l'accesso che chiedono:

1. IBM® MaaS360® Mobile Content Management
2. IBM® MaaS360® Mobile Document Editor
3. IBM® MaaS360® Mobile Document Sync

MaaS360 Mobile Content Management offre un “container” di documenti mobile per la collaborazione sui contenuti con un set completo di funzionalità di gestione del ciclo di vita per la distribuzione, l'aggiornamento, la gestione e la protezione dei documenti. Gli amministratori IT possono imporre l'autenticazione, impedire il copia/incolla e autorizzare la sola visualizzazione. Gli utenti possono accedere a repository di file e contenuti aziendali distribuiti come SharePoint, DropBox e Google Drive.

MaaS360 Mobile Document Editor è progettato per impedire le perdite di dati aziendali e consentire agli utenti di creare, modificare e salvare i dati. Gli utenti possono collaborare sui file di Word, Excel, PowerPoint e di testo dai loro dispositivi mobili mentre sono in viaggio.

MaaS360 Mobile Document Sync permette agli utenti di sincronizzare facilmente i contenuti di tutti i dispositivi mobili gestiti per continuare a creare o modificare i file senza interruzioni. Il reparto IT può applicare criteri di protezione come la limitazione del copia/incolla e il blocco dell'apertura o della condivisione di applicazioni non gestite. I controlli possono essere applicati a tutti i documenti, a un gruppo di documenti o a singoli documenti e offrono la flessibilità necessaria per proteggere i preziosi dati aziendali.

I casi di condivisione di contenuti protetti sono numerosi in tutti i reparti di un'organizzazione, dalle vendite al marketing, dalle operazioni al finanziario:

- Visualizzare e condividere le modifiche apportate all'ultimo minuto a una presentazione di vendita, giusto prima dell'incontro con il cliente
- Collaborare sugli ultimi dati finanziari in un foglio di calcolo prima di imbarcarsi su un aereo

- Creare messaggi di marketing e condividerli con i colleghi mentre si è seduti al tavolino di un bar
- Distribuire i documenti finanziari trimestrali al Consiglio di Amministrazione e impostare la scadenza del documento dopo la conclusione della riunione
- Condividere i materiali dei prodotti in tempo quasi reale con i venditori, in modo che non debbano affannarsi per trovare la scheda dati o le più recenti informazioni sulla concorrenza
- Assicurarsi che i tablet in vendita nei negozi abbiano le informazioni di inventario e prodotto più recenti

IBM® MaaS360® Gateway Suite

MaaS360 Gateway Suite è una componente fondamentale per rendere tutto questo possibile. Protegge i dati in movimento, fornendo un accesso continuo e sicuro ai contenuti aziendali e all'intranet dai dispositivi mobili:

- Fornisce un accesso mobile semplice e protetto ai dati, senza una VPN on-device; non è necessario accedere alla VPN ogni volta che occorrono delle informazioni
- Rende disponibili SharePoint, le condivisioni di file di Windows, i siti intranet e le app Web anche in mobilità
- Protegge i dati con criteri di sicurezza affidabili e controlli DLP
- Non richiede la modifica delle impostazioni di rete o di sicurezza del firewall

Figura 4 - I flussi di dati con MobileFirst Gateway

Potete configurare le opzioni dei criteri per gestire il modo in cui MaaS360 Productivity Suite interagirà con i dispositivi degli utenti. Ad esempio, potete specificare gli URL dei wiki aziendali, i sistemi di tracciamento dei bug o le cartelle aziendali in MaaS360 Gateway, che saranno visualizzati come segnalibri in MaaS360 Secure Mobile Browser. Potete, inoltre, specificare se l'accesso a queste posizioni richieda l'autenticazione.

MaaS360 Gateway determina ciò che gli utenti delle risorse aziendali vedranno quando accedono al "container" dati dai loro dispositivi.

Non comprate mai niente senza provarlo

MaaS360 è facile e veloce da provare e il tempo investito nella sua configurazione per le vostre esigenze è tempo ben speso. Quando vi sarete resi conto che MaaS360 è la soluzione giusta per la vostra organizzazione, l'ambiente di prova diventerà il vostro ambiente live!

Per provare gratuitamente e senza impegno MaaS360, fate clic qui:. Potete iniziare immediatamente, senza complicate impostazioni o modifiche delle infrastrutture esistenti. Provate MaaS360 oggi stesso!

Figura 5 - I prodotti MaaS360

Informazioni su IBM MaaS360

IBM MaaS360 è la piattaforma di gestione della mobilità aziendale per consentire produttività e protezione dei dati in base al modo in cui le persone lavorano. Migliaia di organizzazioni fanno affidamento su MaaS360 come base per le loro iniziative di mobilità. MaaS360 consente la gestione globale con validi controlli di sicurezza su utenti, dispositivi, applicazioni e contenuti per supportare qualsiasi applicazione mobile. Per saperne di più su IBM MaaS360 e iniziare con una versione di prova gratuita di 30 giorni, visitate il sito Web www.ibm.com/maas360

Informazioni su IBM Security

La piattaforma di sicurezza di IBM offre funzionalità di security intelligence per aiutare le aziende a proteggere olisticamente utenti, dati, applicazioni e infrastrutture. IBM offre soluzioni per la gestione delle identità e degli accessi, la gestione degli eventi e delle informazioni di sicurezza, la sicurezza dei database, lo sviluppo di applicazioni, la gestione dei rischi e degli endpoint, la protezione dalle intrusioni di nuova generazione e così via. IBM gestisce una delle più grandi organizzazioni di ricerca, sviluppo e realizzazione di soluzioni nel campo della sicurezza. Per maggiori informazioni, visitate il sito www.ibm.com/security

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

Documento redatto negli Stati Uniti d'America,
marzo 2016

Si prega di riciclare

WGW03111-ITIT-01