

L'ENTERPRISE MOBILITY MANAGEMENT E LA SOLUZIONE DI BLACKBERRY





Note sull'autore

Gaetano Di Blasio è giornalista professionista dal 1997. Da oltre 25 anni segue il settore dell'ICT. Attualmente è Direttore

Responsabile delle riviste SOLUTIONS e Security & Business di Reportec, di cui è socio e cofondatore

Avvertenze

Pubblicato nel 2014

Tutti i marchi contenuti in questo white paper sono registrati e di proprietà delle relative società. Tutti i diritti sono riservati. Va notato che le informazioni contenute possono cambiare senza preavviso; le informazioni contenute sono reputate essere corrette e affidabili anche se non sono garantite. La descrizione delle tecnologie non implica un suggerimento all'uso dell'una o dell'altra così come il parere espresso su alcuni argomenti da parte di Reportec è puramente personale. La vastità dell'argomento affrontato e la sua rapida evoluzione possono avere portato a inaccuratezze di cui Reportec non si ritiene responsabile, pur avendo espletato i possibili controlli sulla correttezza delle informazioni medesime; il white paper non rappresenta una presa di posizione a favore di una o l'altra delle tecnologie, standard o prodotti ivi riportati né garantisce che le architetture, apparati, prodotti hardware e software siano stati personalmente verificati nelle funzionalità espresse; le descrizioni delle architetture, delle piattaforme, dei servizi e dei dati aziendali sono stati elaborati in base alle informazioni fornite dalle aziende, con le quali gli stessi sono stati analizzati e ridiscussi.

Copyright Reportec – 2014

www.reportec.it

L'ENTERPRISE MOBILITY MANAGEMENT E LA SOLUZIONE DI BLACKBERRY

Un mondo business sempre più mobile

La mobilità è sempre stata un elemento chiave per il progresso della società umana. Tutti i momenti che hanno caratterizzato un balzo in avanti nell'evoluzione industriale e sociale hanno coinciso con innovazioni tecnologiche e scientifiche che hanno incrementato la mobilità di persone e merci. Ma è solo con le recenti tecnologie mobili che si è annullato quasi del tutto la barriera spazio-temporale e avviato un processo evolutivo che sta cambiando profondamente il modo di condurre il business.

Si tratta di un cambiamento tumultuoso che si prevede accelererà con un gradiente ancora più sostenuto negli anni a venire. Ormai la percentuale di penetrazione dei "cellulari" in Italia è del 100%. Di fatto il numero di questi ultimi è di gran lunga superiore a quello della popolazione attiva, pur contando solo le schede SIM attive. Ma ha ancora margini di crescita la percentuale di smartphone rispetto il totale dei dispositivi mobili "atti" a telefonare.

Si tratta, peraltro, solo di una parte dei mobile device, che comprendono anche tablet, notebook e un numero variabile di apparati "ibridi", spesso indicati come convertibili, che nascono per venire incontro alle diverse esigenze di "user experience".

La User Experience è un concetto che supera quello tradizionalmente rappresentato dalla interfaccia utente, perché, parallelamente al proliferare di nuovi dispositivi si è assistito anche alla nascita di nuovi sistemi operativi che hanno modificato radicalmente lo scenario business prima caratterizzato dall'uso quasi esclusivo di Windows sul computer fisso e su quello mobile.

Smartphone e tablet sono strumenti operativi a tutti gli effetti e la loro diffusione sta cambiando anche la modalità di fruizione del software applicativo. È la logica della "app", cioè di un software dedicato a svolgere una singola funzionalità o a gestire un singolo servizio. App e Web Service stanno rivoluzionando lo sviluppo applicativo, con ripercussioni che non tarderanno a sentirsi sull'infrastruttura software e sul portfolio applicativo di ogni azienda.

Il risultato è che l'utilizzatore è sempre più orientato a privilegiare un nuovo modo di interazione con il dispositivo, che sostituisce a tastiera e mouse uno schermo touch popolato di icone e semplici "bottoni".

La praticità di questi strumenti e il proliferare di app per le attività più varie sta portando a una nuova informatizzazione del consumatore nel privato con conseguenti impatti anche sulle modalità operative sul fronte professionale.

Le aziende si stanno adeguando definendo strategie e implementando soluzioni per l'Enterprise Mobility, al fine di massimizzare i benefici indotti dal lavoro in mobilità.

Vivere il cambiamento rende difficile percepirlo, perché si è parte del sistema ed è difficile notare i piccoli mutamenti che avvengono, o sembrano apparire, un poco alla volta. È come quando si vedono i propri figli o nipoti crescere giorno dopo giorno. Non ci si rende conto del loro cambiamento sino a che non si vanno a riprendere le foto dell'anno precedente.

Se si porta alla mente un'istantanea dell'organizzazione aziendale risalente a vent'anni fa e una di dieci anni fa, confrontandole con la situazione attuale si può comprendere la portata del cambiamento. Ma la differenza è notevole anche solo guardando pochi anni addietro, perché i cambiamenti sono profondi e al tempo stesso rapidi.

Non è facile accorgersene, anche se il mondo del lavoro si sta trasformando modificando il nostro modo di lavorare, produrre, interagire, spostarsi sul territorio, accedere a servizi pubblici o privati, insomma, tutto quanto ha a che fare le modalità operative e le relazioni interpersonali.

Naturalmente un cambiamento non avviene per caso, soprattutto nell'economia o nella catena dei bisogni. Esiste sempre un elemento o un insieme di elementi scatenanti. La trasformazione è resa possibile da due fattori: il bisogno e gli abilitatori, nella fattispecie quelli tecnologici.

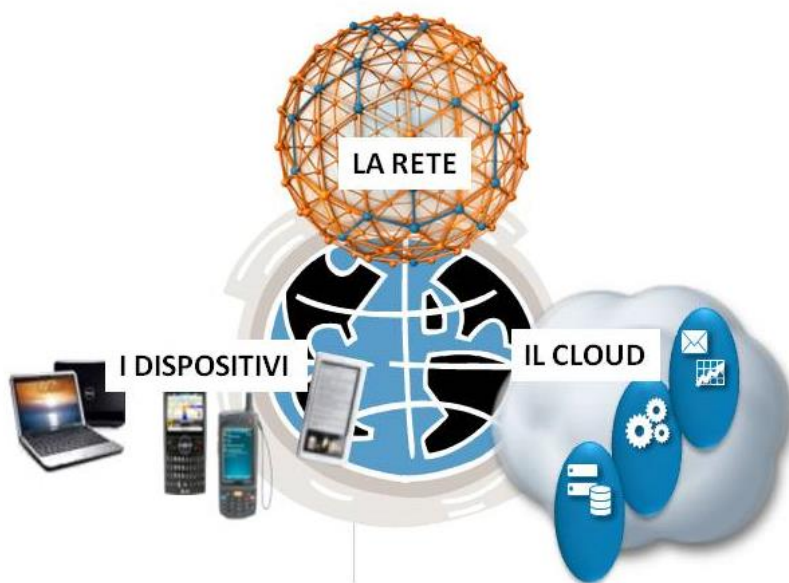
Quando le è stato chiesto quale fosse l'invenzione più importante, la scienziata e premio Nobel Rita Levi Montalcini ha risposto senza indugio: "Internet". È innegabile che la Rete abbia avuto un impatto equiparabile per portata a quelle invenzioni "primitive" che hanno radicalmente cambiato le abitudini di vita degli essere umani.

Oltre alla Rete, gli abilitatori che hanno soddisfatto nuovi bisogni d'interazione e che stanno favorendo lo sviluppo di nuove modalità lavorative sono sintetizzabili dal cloud e dai dispositivi mobili.

Come accennato i cambiamenti non sono, per quanto rapidi, istantanei e

Internet, Cloud e device rappresentano l'attuale punto di arrivo di un processo di trasformazione che ha coinvolto tutti i sottosistemi IT utilizzati in azienda per la conduzione del business e l'interazione interna ed esterna. L'ottimizzazione e razionalizzazione che si sono, anche tumultuosamente, susseguiti, prima di consolidamento, poi di virtualizzazione e infine di cessione in outsourcing o con il ricorso a service provider, hanno coinvolto le reti trasmissive i server, lo storage, le applicazioni in modo progressivo e pervasivo. Un'accelerazione l'ha poi avuta anche lo sviluppo di processori e batterie, sempre più miniaturizzati, causa e contemporaneamente effetto, che ha messo a disposizione delle aziende e del business soluzioni e dispositivi innovativi e flessibili, mutuati dalla consumer electronics, che hanno aperto la strada a nuovi modi di operare.

Se, per semplicità di analisi, si riduce il numero si arriva appunto alla disponibilità della rete, cioè di una connettività ubiqua, alle infrastrutture cloud private e pubbliche e ai terminali mobili.



I tre abilitatori della Mobility

Questi tre abilitatori, anche se in misura diversa, possono essere considerati le leve su cui si è innescato il profondo cambiamento in corso. Le aziende stanno affrontando la trasformazione della propria infrastruttura

accentrando e al tempo stesso "allargando" il data center in chiave cloud, sia esso ibrido o totalmente basato su infrastrutture pubbliche.

La connettività è ormai data per acquisita, anche se rimangono differenze notevoli di servizio in alcune aree disagiate del Paese. Sul fronte dei dispositivi mobili, invece, l'evoluzione continua deve ancora esprimere ulteriori potenzialità di cambiamento. Le imprese, peraltro, sono oggi chiamate a scelte importanti, sotto la spinta anche delle richieste provenienti dal "basso", cioè dalla forza lavoro che con tali dispositivi ha ormai una confidenzialità quotidiana.

Il fenomeno della "consumerizzazione" ha ribaltato il rapporto con la tecnologia che, un tempo, era più avanzata all'interno delle aziende, dove gli alti investimenti necessari venivano ripagati dai benefici dell'automazione. Con lo sviluppo di dispositivi intelligenti a basso costo, il consumatore medio dispone di una potenza di calcolo relativamente paragonabile a quella che può trovare in azienda.

Le imprese stanno prendendo la rincorsa e, ben presto, potranno contare sugli stessi vantaggi amplificati dalla maggiore disponibilità di risorse economiche. Nel frattempo dovranno maturare delle strategie per modificare i processi aziendali e definire policy d'utilizzo dei dispositivi mobili affrontando tre requisiti da conseguire:

- l'appagamento dell'utilizzatore finale;
- la sicurezza dei dati aziendali;
- la gestione dei dispositivi e delle applicazioni che su questi sono disponibili.

Tali obiettivi non sono indipendenti tra loro, anzi sono strettamente correlati e, per certi aspetti, contrapposti, come vedremo in seguito.

La User Experience, il BYOD e il suo superamento

L'appagamento dell'utilizzatore finale passa attraverso la sua esperienza lavorativa. Gli strumenti di lavoro che egli ha a disposizione giocano un ruolo importante nel determinare la sua soddisfazione e, di riflesso, la sua produttività.

Come accennato, la consumerizzazione ha messo nelle mani dei consumatori dispositivi intelligenti con potenza e, soprattutto, con interfacce molto user friendly. Interfacce decisamente più semplici di quelle che dovevano utilizzare in ufficio.

Il risultato è stata la nascita del cosiddetto BYOD (Bring Your Own Device). In passato, erano le imprese a fornire i dispositivi, telefoni e computer, ai lavoratori, che non avevano possibilità di scelta e che hanno così cominciato a utilizzare un proprio apparato per le attività lavorative. All'inizio molte imprese hanno visto l'opportunità di risparmio sull'acquisto dell'equipaggiamento e hanno incoraggiato questo fenomeno.

Finché si trattava del giovane nuovo dipendente che preferiva usare il Mac al pc, poco male, ma quando si è trattato di configurare e gestire il tablet o lo smartphone di grido dell'amministratore delegato, si è verificato che i conti non sempre tornavano: a fronte di un risparmio sull'acquisto si aveva un considerevole aumento dei costi sull'help desk.

Peraltro, l'ondata del BYOD non era né è arrestabile (Gartner prevede che entro il 2017 circa metà dei lavoratori chiederà di poter utilizzare dispositivi propri), perché per l'utente finale conta soprattutto l'esperienza: per il dipendente è "fondamentale" avere la possibilità di scegliere il dispositivo con il sistema operativo preferito, anche solo perché quello che si è abituati a utilizzare.

Secondo diversi studi, questa libertà aumenta la soddisfazione del dipendente con positivi effetti sulla sua produttività. Certamente quello che si è andato diffondendo è un nuovo modo di gestire l'orario di lavoro. In passato quest'ultimo era vincolato alla presenza in ufficio. Grazie alla mobility e alla disponibilità di un unico dispositivo, usato anche per il privato e quindi sempre acceso, si è esteso "always on" della connessione alla continua disponibilità della persona.

Sussiste un rischio "stress", ma c'è il contraltare della maggiore libertà nella gestione del proprio tempo. Una flessibilità che si adatta a un sempre maggior numero di lavoratori, considerando che circa il 70% della forza lavoro in Italia è impegnato come "information worker". Basti considerare che oltre il 63% delle imprese opera nel terziario (dati Istat 2013).

Si deve comunque trattare di una libera scelta, anche perché il dipendente non dovrebbe essere costretto a comprarsi lo strumento di lavoro, come se si trattasse di un libero professionista.

A fronte di tali vantaggi, il BYOD, però, comporta due complicazioni: il suddetto aumento dei costi operativi per la gestione dei dispositivi e un incremento del rischio che possano avvenire violazioni alla sicurezza dei dati aziendali. In pratica, consentire ai dipendenti di utilizzare un proprio dispositivo per il lavoro permette di conseguire il primo requisito per il successo della mobility, quello sull'appagamento dell'utilizzatore finale, ma contemporaneamente ostacola il soddisfacimento degli altri due.

Dal BYOD al COPE

Il BYOD si è contrapposto all'unica situazione fino a quel punto contemplata, cioè l'utilizzo da parte del dipendente di un dispositivo messi a disposizione dall'azienda. Una pratica logica, perché è effettivamente l'azienda a dover fornire al lavoratore gli strumenti per farlo lavorare. È interesse dell'azienda permettere al lavoratore di produrre nel miglior modo possibile.

Fin quando le tecnologie sono state molto costose, questa logica era naturale, ma, come abbiamo visto, la consumerization ha ribaltato la situazione. Per questo le imprese hanno convenienza a permettere il BYOD, perché dovrebbe rendere più produttivo il dipendente. È d'uopo il condizionale, perché una perdita di controllo rende anche più difficile valutare i risultati. Sopra ogni cosa pesa il crescere del rischio aziendale.

Spesso il dispositivo mobile con a bordo i dati più critici per l'azienda è in mano all'amministratore delegato o a qualche altro dirigente. Anche solo la perdita del dispositivo mette a repentaglio la riservatezza delle informazioni. Gli aspetti legati alla sicurezza sono esaminati nel prossimo paragrafo, mentre adesso vogliamo sottolineare come sia impossibile per l'impresa entrare nella sfera del privato. Ma tale è, in effetti, il dispositivo utilizzato, quando si parla di BYOD.

Per questo si è ipotizzato un altro approccio, noto come COPE (Corporate Owned Personal Enabled). In pratica, l'azienda torna a fornire il dispositivo al dipendente, ma gli permette di utilizzarlo anche per scopi personali. Questo cambia radicalmente la strategia attuabile, perché dà il permesso all'azienda di gestire l'apparecchio, di cui è proprietaria.

Per mantenere anche i vantaggi del BYOD, però, occorre un sistema di gestione che consenta di supportare qualsiasi tipo di dispositivo: solo così, infatti, l'azienda potrà comunque lasciare ai dipendenti una scelta ampia e non obbligare l'uso di un sistema operativo non gradito.

Altra caratteristica fondamentale per abilitare il COPE consiste nella capacità di "containerization", cioè la possibilità di tenere quanto più separati possibile i due diversi tipi di utilizzo. In altre parole, separare app e dati del lavoro da app e dati della sfera privata. Solo isolando e potendo intervenire sulla parte aziendale da remoto, salvaguardando la privacy del dipendente da incursioni dell'impresa e, al tempo stesso, evitando che un comportamento insicuro metta a rischio i dati aziendali, si possono prendere gli aspetti migliori del BYOD e quelli del device proprietà dell'azienda.

La sicurezza di device e dati

Quanto più i dispositivi mobili sono diffusi nelle aziende, tanto più si sottovalutano i rischi materiali, economici e legali connessi alla loro sicurezza. Un paradosso, ma la confidenza eccessiva gioca brutti scherzi.

Innanzitutto va considerato che le tecniche con cui vengono attaccati i dispositivi mobili sono complesse tanto quelle utilizzati verso i comuni pc e ne condividono i medesimi deleteri effetti.

Anzi, in alcuni casi possono causare un immediato danno economico, per esempio connettendo il dispositivo a siti con un costo di connessione per minuto molto elevato, o esportando fraudolentemente dati, o, ancora, utilizzando il dispositivo per inviare sms a estese liste di utenti, per esempio quelli presenti nella directory della funzione mail o telefonica.

Gli esperti nel creare applicazioni di malware sono sovente in grado di scovare tutte le debolezze nella sicurezza delle piattaforme mobile, degli application store e dell'ecosistema in generale. Non è raro che proprio dagli app store si scarichino quelle che sembrano innocenti e utili applicazioni che poi nascondono al loro interno virus in grado di infettare il dispositivo.

A questi rischi, già di per sé consistenti si aggiungono quelli connessi alla perdita o al furto dei dispositivi mobili e quindi di dati e informazioni personali e aziendali.

Come se questo non bastasse, va considerato che la trasmissione via etere e onde radio è intrinsecamente, per sua stessa natura, più esposta a intercettazioni di quanto possa avvenire su reti fisse perché non è nemmeno necessario collegarsi a un cavo (cosa poi particolarmente difficile nel caso di dorsali ottiche Wan o Lan, ma è sufficiente disporre di strumenti in grado di intercettare le frequenze Wi-Fi (Sniffing, MITM) e di decodificare i dati sui diversi canali trasmissivi.

Sono attacchi molto difficili da evidenziare perché operano a un livello

trasparente per il proprietario di un dispositivo. Lo sniffing si limita semplicemente a intercettare e decodificare le trasmissioni e se queste sono in chiaro (e cioè non cifrate mediante opportuni algoritmi) il gioco è fatto. Ancora più subdolo è la metodologia di attacco MITM (acronimo di Man in the Middle), che consiste sostanzialmente nel fraporsi tra due interlocutori. Le soluzioni, esistenti, non sempre vengono attivate, considerando sufficiente l'utilizzo di protocolli sicuri quali HTTPS ed SSH, ma questi, normalmente, sono implementati nei livelli alti della pila ISO/OSI (un modello definito negli anni settanta che rappresenta il riferimento generale per la realizzazione di sistemi informatici) e possono essere superati da attacchi portati ai livelli inferiori, quali appunto quelli di trasmissione radio delle informazioni.

Proprio la diffusione esponenziale dei dispositivi mobili ha reso conveniente lo sviluppo di malware e exploit kit (strumenti software chiavi in mano per attuare attacchi): gli sforzi possono così essere ripagati. Il punto è che la maggior parte di questi dispositivi sono stati progettati per un uso consumer, senza considerare la sicurezza un requisito.

Solo le più aggiornate versioni dei sistemi operativi hanno cominciato a preoccuparsi della questione, proprio per il crescente impatto degli attacchi. Resta il problema delle architetture, molte delle quali non si prestano a un'operazione di hardening. Inoltre, pressoché nessun utilizzatore procede all'aggiornamento del sistema operativo (addirittura questa operazione in passato comportava la perdita dei dati).

Sussiste poi un ulteriore elemento di rischio, rappresentato dalla memorizzazione dei dati in cloud: un'operazione utilissima in termini di backup, ma soggetta a rischio quando il servizio utilizzato è di tipo gratuito e consumer, quindi dotato di un livello di protezione minimo.

Si sono già verificati altisonanti casi in cui hacker (di quelli ancora animati da spirito goliardico e non criminali) sono riusciti a fare notizia copiando immagini osé di attrici e Vip, portando così alla ribalta il problema della sicurezza su queste piattaforme cloud. Certamente, i provider potranno alzare il livello di sicurezza, ma occorre comunque attivare una strategia "culturale", per educare gli utilizzatori aziendali a osservare regole comportamentali adeguate e a seguire le politiche sulla sicurezza, per esempio in termini di password da utilizzare.

Sono proprio queste situazioni a rendere critico l'approccio al BYOD, perché il dipendente aziendale è abituato a un utilizzo più "rilassato" del proprio

dispositivo, ma il livello di sicurezza è generalmente unico, con il BYOD, come unico è l'apparecchio usato sia per il lavoro sia per la vita privata.

Data questa situazione ci si può chiedere cosa fare per ridurre al minimo i rischi, considerando che la loro totale eliminazione è in ogni caso impossibile. Si tratta quindi di identificare il break-even tra quanto si è disposti a fare dal punto di vista procedurale (e a investire economicamente in sistemi, software e applicazioni di sicurezza) e il rischio che si può correre aziendalimente (e, per chi ha aderito al BYOD, anche personalmente).

A livello aziendale quello di cui ci si può dotare può prevedere:

- Sistemi anti-malware sul dispositivo per proteggerlo da applicazioni infette, spy/ad-ware, schede SD corrotte e altri attacchi.
- Client SSL VPN per proteggere i dati sulla connessione logica e fisica e assicurare un'adeguata autenticazione dei dati e dei partecipanti a una sessione di comunicazione.
- Funzionalità per l'amministrazione dei dispositivi mobili (attività di blocco del dispositivo on site e da remoto, cancellazione dati, backup, ripristino dei dispositivi persi e/o rubati).
- Rinforzare le policy di sicurezza.
- Utilizzare strumenti che aiutino nel monitorare l'attività del dispositivo in caso di perdita dei dati o di un suo uso inappropriato.

Il Mobile Device Management

Le funzionalità base di sicurezza sono normalmente garantite dai cosiddetti sistemi di Mobile Device Management (MDM), che forniscono le politiche di "enforcement" della sicurezza, le quali vengono attuate di solito o dal provider del servizio o a livello aziendale da parte dell'entità preposta, usualmente il reparto IT.

Nell'ambito aziendale è poi di rilevanza il coprire sia gli aspetti inerenti le modalità di accesso alle applicazioni business da parte di un dispositivo mobile che quanto concerne alla sua protezione da possibili e come si è visto molto probabili attacchi esterni.

Entrando nel dettaglio di una possibile policy aziendale per la sicurezza dei dispositivi mobili ci sono quindi diverse cose che si possono fare, in parte attinenti alla rete e ai sistemi informativi e in parte alla flotta di dispositivi, qualsiasi essi siano, perché oramai con le ultime generazioni di apparati, dal telefonino alla stampante, sono tutti dotati o dotabili di indirizzo IP e possono quindi essere oggetto di attacchi malevoli attuati allo scopo di prelevare informazioni e dati sensibili.

Un forte controllo centrale, per esempio, può servire per impedire non solo l'accesso a certi dispositivi a determinate applicazioni (ottenibile definendo specifici profili di utente) ma anche per impedire che lo stesso sia usato per accedere a siti non sicuri, o per impedirgli di esportare informazioni sensibili tramite per esempio una semplice connessione diretta di tipo Bluetooth.

Un esempio di gruppi funzionali di azioni e interventi preventivi da attuare al fine di incrementare il grado di sicurezza e la resistenza nei confronti di possibili attacchi può essere il seguente:

Antivirus, che deve prevedere, un aggiornamento automatico del software antivirus e delle signature, la scansione periodica dei file residenti sul dispositivo e una scansione costante delle connessioni.

Firewall, con filtraggio delle chiamate in ingresso e in uscita, allarmi e logging delle attività a fini statistici e forensi e, infine, una personalizzazione funzionale e profilazione degli utenti.

Antispam, che attui il blocco di sms e di connessioni in fonìa non autorizzate, impedendo eventualmente le connessioni.

Data protection, per un protezione da perdita e furti dei dati, con blocco locale o remoto del dispositivo in caso di furto o di suo smarrimento, backup e restore dei dati su un dispositivo alternativo, eventuale capacità di localizzazione del dispositivo via GPS per facilitarne il recupero.

Controllo dei dispositivi, con funzioni per l'inventario delle applicazioni e il monitoraggio dei contenuti.

Naturalmente quanto sopra elencato non è tutto quello che può essere fatto, ma rappresenta un insieme significativo di opzioni che possono ridurre di molto i rischi che si corrono quando si usa un dispositivo mobile e può aiutare nel definire policy aziendali che implicino un utilizzo corretto, aderente a principi etici, alle norme di legge e alle funzioni aziendali dei dispositivi in dotazione ai dipendenti.

Stabilire una adeguata politica di protezione, oltre a ridurre i rischi, permette anche di limitare l'uso improprio dei dispositivi, prolungarne la durata, ridurre il rischio che si guastino o risultino fuori servizio a causa di software non autorizzato o certificato e, in definitiva, contribuire a ridurre i costi e ad aumentare la produttività dei dipendenti.

Il servizio della Mobility

Una soluzione che supporti la Mobility aziendale deve comprendere tutti gli aspetti legati all'usufruibilità delle applicazioni e dei servizi. Quindi la

garanzia non solo della disponibilità, ma anche di un livello minimo garantito di prestazioni. Soprattutto, però, questo significa poter utilizzare soluzioni che supportino appieno i processi aziendali.

Le suddette tematiche devono dunque essere affrontate con gli opportuni approcci tecnologici e, come già rimarcato, la strada per il futuro è certamente il cloud o IT as a Service, per la quale ciascuna azienda dovrà trovare la propria ideale combinazione tra private e public.

In questa chiave va dunque presa in considerazione l'organizzazione delle infrastrutture necessarie per fornire il servizio di mobility ai diversi utilizzatori in azienda. Ovviamente, la connettività esterna alle sedi aziendali non potrà che essere acquisita presso gli operatori, mentre internamente si potranno utilizzare le reti Wi-Fi. Per quanto concerne, invece, la soluzione dei requisiti prima enunciati, si potranno effettuare le scelte più opportune a seconda dei casi.

Quanto occorre è dunque una piattaforma MaaS (Mobility-as-a-Service), cioè una piattaforma di tipo "always on" di livello Enterprise, atta a erogare servizi di mobilità a un ampio numero di terminali di utente, dal comune telefono al più complesso terminale mobile. Il suo obiettivo primario è quello di abilitare la connessione di un utente e, tramite il dispositivo di cui è equipaggiato, permettergli di accedere alle proprie applicazioni e dati, il tutto con i processi di business che controllano il processo e cioè se l'utente è autorizzato a farlo, a che dati accede, che applicazioni richiede, quali dati genera, eccetera.

Quello basato su un modello SaaS per la connessione, protezione e il controllo dei dispositivi di un utente mobile non è stato l'unico a essere stato usato, anche se le prime generazioni di tali sistemi hanno evidenziato criticità, perché si è rivelato complesso sviluppare e adeguare le applicazioni per la integrità e sicurezza dei dati, complesso controllare i laptop, affrontare la rapida evoluzione di smartphone e degli altri dispositivi mobili intelligenti, oltre a tutti i dispositivi di rete che costituiscono una infrastruttura atta a erogare un servizio di mobilità.

Quello basato sul cloud si sta evidenziando quindi come un modello cost effective e facilmente fruibile per controllare gli utilizzatori e garantirne la sicurezza, i loro dispositivi e i dati aziendali.

Le soluzioni di Enterprise Mobility Management: BlackBerry Enterprise Service 10 e 12

Un servizio ben più esteso del Mobile Device Management è quello usualmente indicato come sistema di Enterprise Mobility Management, che permette di garantire la disponibilità e la sicurezza sia di dispositivi e dati sia delle applicazioni: in pratica quella del servizio nel suo complesso, soddisfacendo tutti i requisiti fin qui evidenziati.

Una delle prime soluzioni per il Mobile Device Management è quella introdotta dall'allora RIM, che con la piattaforma BlackBerry Enterprise Server si è da subito posta l'obiettivo di fornire alle imprese una soluzione per gestire la mobility, puntando in primo luogo sulla sicurezza.

BlackBerry, infatti, per anni è stata esclusivamente focalizzata sul mondo business, ben consapevole che, in tale contesto, la disponibilità del servizio fosse fondamentale. Per questo è chiaramente importante disporre di una soluzione per la gestione dei dispositivi affidabile e versatile.

Dall'allora modello client/server, si è poi passato a una più moderna impostazione basata sul servizio e la piattaforma, già utilizzata da migliaia di imprese, comprese importanti organizzazioni governative, è stata ulteriormente migliorata con il lancio del BlackBerry Enterprise Service (BES) 10, che permette di gestire anche i precedenti BlackBerry Enterprise Server o l'ambiente BlackBerry Enterprise Server Express.

Inoltre, con il recente BES 10 sono stati aggiunti importanti aggiornamenti. Questo, infatti, fornisce supporto oltre che per dispositivi BlackBerry (compreso il più recente OS 10), anche per smartphone e tablet Apple iOS e Android. Il tutto attraverso un'unica console di management. Con la versione BES 12, prevista entro il 2014, sarà supportato anche Windows Phone 8.

L'azienda ha quindi da tempo avviato una politica di apertura, per consentire alle imprese di gestire complessi parchi di dispositivi mobili, abilitando il BYOD. Ma non solo, perché, grazie a una serie di innovative funzionalità, permette di sfruttare i vantaggi del COPE (Corporate Owned Personal Enabled) per abbinare sicurezza e produttività a supporto del business aziendale.

Punto di forza storico dei dispositivi BlackBerry è la sicurezza rafforzata dall'architettura "hardened" che rende molto complesso sviluppare malware per penetrare sullo smartphone. In particolare, La soluzione BlackBerry soddisfa l'intera gamma di esigenze di sicurezza; dal livello base fino ai requisiti di controllo di ambienti governativi e settori regolamentati, come per esempio quelli imposti dalla NATO per le comunicazioni classificate "Restricted" oppure i Common Criteria EAL 4+ o, ancora, la certificazione "Full Operational Capability" per il Dipartimento della Difesa statunitense. Peraltro, presso l'azienda di origine canadese, sono consapevoli che le esigenze di massima sicurezza non necessariamente devono riguardare tutti i dipendenti. Il mercato, del resto, è ormai caratterizzato da una varietà di dispositivi e l'utilizzatore vuole essere libero di scegliere quello che preferisce. Per questo, gli sforzi della società si sono concentrati sulla componente software, per aggiungere alla sicurezza, le risposte alle odierne esigenze di flessibilità.

Le imprese possono quindi sfruttare BES 10 per una gestione multi-piattaforma della mobilità d'impresa e per rendere sicuro il BYOD o COPE con funzioni come BlackBerry Balance e Secure Work Space.



Nuova politica di apertura per BlackBerry con BES 10 e BES 12

Come accennato, attenzione è posta alla gestione con una singola console per amministrare dispositivi, utenti, gruppi, app e servizi. Disponibile, poi, il

supporto BlackBerry gratuito, che include accesso telefonico 24x5 agli esperti tecnici, supporto rapido online, accesso a formazione e a strumenti di diagnostica e produttività.

Inoltre, un sistema di reportistica migliorato rispetto le precedenti versioni e dotato di una funzione per l'esportazione dei dati, consente di effettuare ulteriori analisi approfondite utilizzando strumenti standard.

Semplificata anche l'architettura, in modo che tutti i precedenti componenti possano ora funzionare sullo stesso server fisico o virtuale.

BlackBerry Balance e Secure Work Space

BlackBerry Balance è stato l'antesignano delle soluzioni di "containerization". Disponibile per dispositivi BlackBerry, questa funzionalità consente di separare i dati e le applicazioni aziendali dai dati e le app utilizzate per le attività personali.

Con BES 10 è stata aggiunta la funzione Secure Work Space per dispositivi iOS e Android, cui fornisce le stesse capacità del Balance, cioè containerizzazione, wrapping delle applicazioni e connettività sicura.

Non solo le applicazioni dei due mondi, business e personale, vengono separate, ma ciascuna app viene "avvolta" (wrap appunto) da un layer di management che la rende gestibile e protegge il dispositivo, impostando le policy di utilizzo.

Secure Work Space, inoltre, fornisce una connessione protetta da firewall, senza che sia necessaria una soluzione separata di VPN.

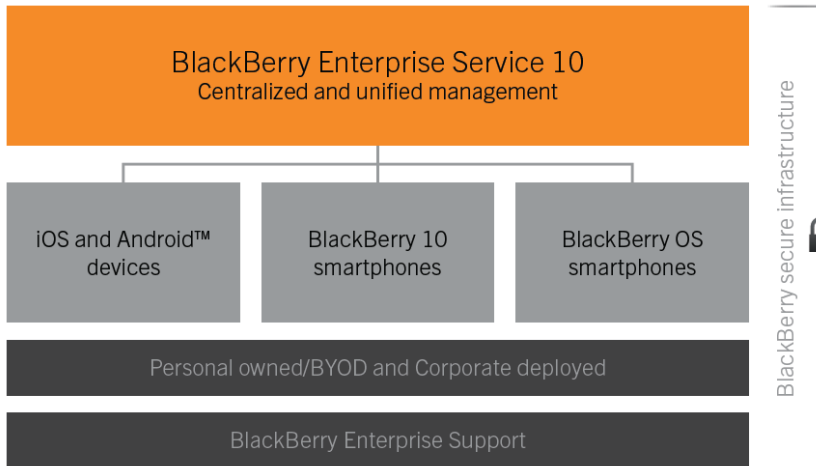
La containerization consente alle imprese di prevedere policy più restrittive per l'utilizzo delle app aziendali, cioè quelle che devono prevedere l'accesso alla rete dell'azienda. Per esempio, banalmente, si può bloccare l'accesso se lo stesso non può avvenire attraverso una connessione sicura. Un'eventualità peraltro rara, grazie alla disponibilità della rete della stessa BlackBerry.

Al riguardo, va sottolineata la disponibilità di un sistema per la gestione sicura degli accessi, fondato su un'architettura a singola porta, basata su NOC (Network Operation Center).

App e funzionalità

Per quanto riguarda la disponibilità di app, va ricordato il forte impegno di BlackBerry nello sviluppo di un ecosistema, basato sulle SDK messe a

disposizione di un cospicuo numero di partner. Questi hanno creato numerose applicazioni, in massima parte orientata a risolvere problematiche di business e a rinnovare i processi aziendali. Lo sviluppo della mobility ha permesso a molte imprese di sviluppare nuove app, anche se progettate essenzialmente per l'ambito consumer.



BES10 fornisce un'unica console di gestione centralizzata

La libertà di scegliere dispositivi iOS o Android non pone limiti agli utilizzatori, che possono scaricare le app con cui preferiscono operare. BlackBerry, peraltro, ha un programma di certificazione, attraverso il quale garantisce che l'applicazione iOS o Android è sicura e garantisce gli stessi standard come le certificazioni native BlackBerry.

In ogni caso, BlackBerry mette a disposizione uno store nutrito, fornendo app per email, agenda, rubrica, note e così via. Non manca, ovviamente, un browser sicuro, una soluzione di editing, l'accesso a sistemi come SharePoint per la condivisione dei documenti e un affidabile sistema di messaggistica: Enterprise BlackBerry Messaging (eBBM).

L'ambito lavorativo è ben definito, come prima evidenziato e può essere organizzato attraverso BlackBerry World for Work: uno storefront di app aziendali completamente integrato.

BlackBerry Enterprise Service 12

BlackBerry Enterprise Service 12 unifica in un'unica piattaforma BES10 e BlackBerry Enterprise Server 5. L'urgenza delle funzionalità previste nella

release 12 ha portato i vertici della società ad anticipare nella versione 10 alcune funzionalità e nell'accelerare il rilascio della 12, cancellando di fatto l'edizione 11.

L'obiettivo è quello di completare la soluzione di Enterprise Mobility, con una soluzione application-enabled. Il "salto generazionale" corrisponde alle intenzioni del nuovo management di spingere sulla componente software e di gestione. Sono infatti queste due le componenti più importanti delle soluzioni per l'Enterprise Mobility.

Con BES 12 e la focalizzazione sui sistemi operativi e non sui dispositivi, BlackBerry, a detta dei suoi stessi responsabili, si sta preparando all'evoluzione della mobility o, meglio, alla rivoluzione dell'Internet of Everything e del M2M (Machine to Machine).

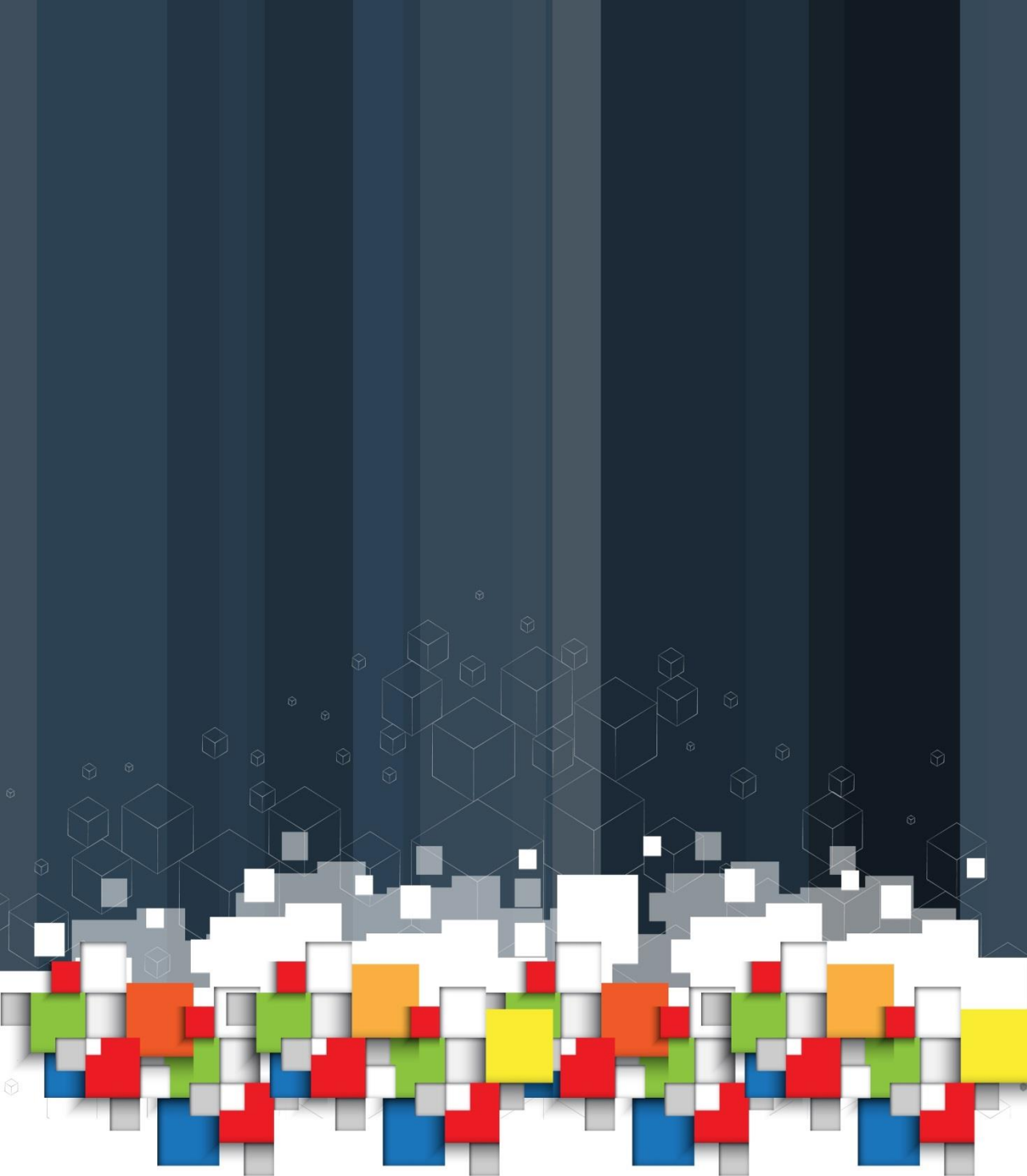
Ovviamente, sottolineano presso BlackBerry, vengono mantenute le caratteristiche di affidabilità e sicurezza già note al mercato.

Tra le caratteristiche che saranno incluse in BES 12, secondo le anticipazioni fornite dal produttore, sono da evidenziare funzionalità di user self service, service management avanzato, possibilità di installazioni scalabili a livello di data center e di implementazioni con cluster ridondanti di tipo active-active, per garantire affidabilità senza eccessivo spreco di risorse.

Più in dettaglio, viene spiegato che la funzionalità di service management fornisce un monitoraggio proattivo e strumenti per calibrare la piattaforma, che consentono di ottenerne una prospettiva end to end e conferiscono capacità automatiche di risoluzione dei problemi.

La console di gestione, inoltre, è disponibile per ambienti, sia on premise sia in cloud, tanto pubblico quanto privato o ibrido.

Importante è poi la disponibilità di tool per lo sviluppo di app mobile, progettati per facilitare l'integrazione delle risorse aziendali sulla piattaforma.



Copyright Reportec Srl - 2014