


 Di Filippo Moriggia



I VOSTRI DISPOSITIVI AL SERVIZIO DELL'AZIENDA



Rischi e vantaggi del Byod,
Bring Your Own Device,
*soluzione sempre più diffusa
che può avvantaggiare
sia la società sia il dipendente.*

Quando finisce la giornata lavorativa e quando inizia la vostra vita privata? Per molti la distinzione tra le attività di lavoro e quelle personali è marcata chiaramente da luoghi e tempi (pensate a una commessa o a un operaio), ma il numero di persone che si occupano di business anche la sera, nei fine settimana o in qualsiasi momento se ne presenti la necessità è in continua crescita. Nel 2014 non sono certamente solo i Ceo o i manager delle aziende multinazionali a rispondere a una e-mail o a un messaggio, a preparare una presentazione o qualche altro documento la sera o nei fine settimana, ma una fetta crescente di dipendenti, professionisti, consulenti o semplici collaboratori.

Per lavorare da casa servono ovviamente degli strumenti che permettano di accedere alle risorse aziendali, garantendo un livello minimo di sicurezza e affidabilità. Smartphone, tablet o notebook in grado di collegarsi in modo sicuro, inviare e ricevere email, produrre documenti. Le aziende si trovano dunque davanti a una scelta fondamentale: o permettono

al dipendente di portare con sé i dispositivi aziendali o consentono l'uso di dispositivi di proprietà del dipendente. In passato la pratica più consolidata, anche per motivi fiscali, era la prima. Il numero di dipendenti che aveva questa esigenza era relativamente ridotto e l'acquisto di un portatile o un cellulare aziendale permetteva di aumentare le spese, pagando meno tasse. La crisi,

l'esigenza di ridurre sempre più spese e sprechi e l'evoluzione sempre più rapida dei dispositivi mobili ha però invertito questo trend. Molti dipendenti infatti – affascinati dalla tecnologia – acquistano tablet o smartphone più avanzati e sofisticati di quelli aziendali e dunque premono per utilizzarli in azienda e a casa anche per svolgere il proprio lavoro.

QUALCHE ANNO FA



Non serve andare molto indietro nel tempo per trovarsi davanti a uno scenario tradizionale ma molto diverso da quello attuale: allora molti dispositivi che oggi la fanno da padrone nelle nostre case e in azienda non erano neppure presenti sul mercato. I computer più diffusi erano i desktop e i dirigenti iniziavano a usare il telefono per rispondere a qualche e-mail. La responsabilità del reparto IT era limitata all'ambito aziendale e l'unico oggetto che poteva essere presente sia a casa sia al lavoro era il portatile.

Questo fenomeno viene chiamato *consumerization* (una parola inglese che descrive l'avvicinamento del mondo professionale a quello consumer) e coinvolge l'intero settore informatico da ormai diversi anni. Basta pensare alla diffusione di dispositivi come l'iPad anche in azienda o al numero crescente di Ultrabook – portatili ultrasottili e curati esteticamente – che oggi fanno parte delle linee business dei principali produttori di Pc. Ormai la tecnologia vince, a casa e in azienda, solo quando riesce ad affascinare e coinvolgere non solo sistemisti e appassionati, ma anche "l'uomo della strada".

Secondo un'indagine del 2013 di Innovation Group su 70 aziende di media e grande dimensione la maggior parte di esse (più dell'80%) già permette o prevede il concetto di Byod (*Bring Your Own Device*, letteralmente "portati il tuo dispositivo"), ma si tratta di una possibilità riservata solo a pochi: manager, professionisti e profili più alti. E cosa succede invece nelle aziende più piccole della realtà italiana? Tracciare un quadro è certamente difficile, ma il trend è sicuramente in evoluzione. Secondo Gartner il Byod e il Cloud sono di fatto il futuro del mercato It, insieme



alla crescente presenza dei dispositivi mobili anche all'interno dell'azienda, dunque tutte le realtà, piccoli e grandi, devono essere preparate a sfruttare questo fenomeno, riducendone al minimo i rischi.

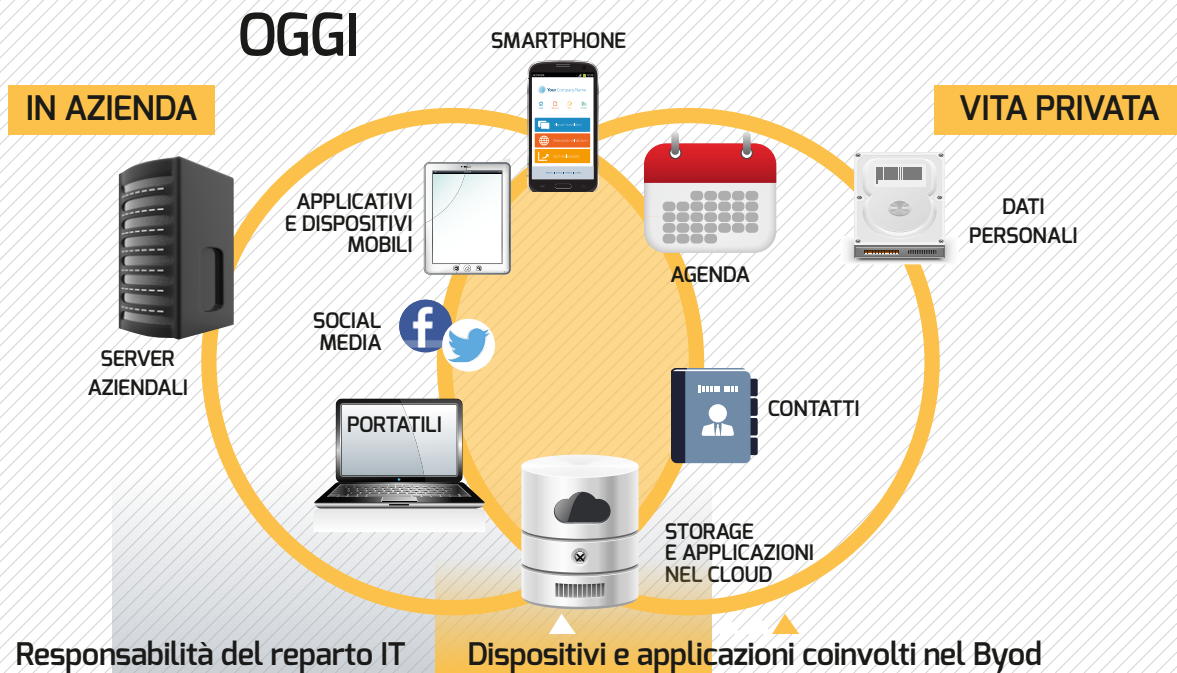
Prima di capire meglio nel dettaglio quali tecnologie permettono di sfruttare al meglio il Byod vediamo dunque quali sono i vantaggi e gli svantaggi di questo fenomeno

VANTAGGI E SVANTAGGI DEL BYOD

I vantaggi del Byod sono facilmente individuabili, a differenza degli svantaggi. Il dipendente viene messo in condizione di utilizzare il terminale che ha scelto e che usa anche nella vita privata. Dunque è portato naturalmente

a lavorare e rispondere a clienti e colleghi anche al di fuori delle ore di lavoro. L'azienda non deve affrontare spese aggiuntive ma solo consentire l'accesso alle risorse aziendali dai terminali che vengono portati in azienda o collegati da remoto. I costi di ownership (possessione) dei dispositivi si riducono così drasticamente, anche considerando l'eventuale necessità di effettuare interventi di manutenzione e configurazione sui dispositivi del dipendente. Anche i costi di upgrade dei dispositivi vengono sostenuti dal dipendente, tutto a vantaggio dell'azienda.

Purtroppo la lista di potenziali svantaggi è ben più ampia. La prima considerazione riguarda la risoluzione di tutte le problematiche di connessione dentro e fuori dalle mura aziendali: dal momento che il "parco macchine"



Oggi sempre più dispositivi utilizzati in ambito personale vengono usati anche in azienda e viceversa. Questo cambiamento ha portato a una crescita enorme delle responsabilità del reparto informatico che oggi si trova a dover proteggere da virus e difendere da attacchi non solo i server on premises, ma anche quelli nel cloud oltre a tutti gli smartphone, i tablet e i portatili di proprietà aziendale o privata che vengono usati per lavorare.



I telefoni BlackBerry hanno dominato il mercato aziendale per anni e ora sono in estinzione, a causa proprio del fenomeno chiamato consumerization. Oggi sono soprattutto un costo a livello di supporto e manutenzione.

potrebbe essere anche ben più vasto del previsto bisogna prevedere l'uso di sistemi di posta, Vpn e applicativi compatibili con il numero più ampio possibile di terminali. Nella maggior parte dei casi questo significa perlomeno supportare sia Android sia iOS, i sistemi operativi di Google e Apple, che sono ormai gli unici veri protagonisti del settore.

Il server di posta aziendale deve prevedere uno o più protocolli per la connessione di terminali mobili, per garantire un collegamento adeguato. In azienda diventa poi praticamente indispensabile fornire un accesso Wi-fi in tutte le aree, per garantire il collegamento di tablet e smartphone. Questo può comportare spese anche significative, dal momento



Il supporto a Windows 8 è limitato in azienda, ma è indispensabile per garantire il Byod: la maggior parte dei portatili acquistati per uso personale ha infatti questo sistema operativo.

che nella maggior parte dei casi la rete esistente è cablata e solo in alcune aree viene messa a disposizione una connessione wireless.

Anche quando i dipendenti sono fuori dalle mura aziendali potrebbe esserci un problema di connettività. Il collegamento a Internet, che in molte aree in Italia è solo di tipo Adsl, spesso offre una banda in upload particolarmente ridotta. Perciò se, ad esempio, i server di posta elettronica sono in azienda, la banda non potrebbe essere sufficiente a garantire un collegamento affidabile e veloce *off premises* (fuori dalle mura). Naturalmente il problema non si pone se il sistema di posta aziendale si trova già nel cloud.

Uno dei problemi più importanti del Byod è la sicurezza. Finché tutti i dati si trovano entro l'azienda può essere relativamente semplice custodirli (anche se purtroppo questo non è sempre vero). Il fatto che documenti, comunicazioni, rubriche e agende siano disponibili sui dispositivi di proprietà dei singoli dipendenti rappresenta invece un rischio ben più alto. In questo caso l'azienda si deve proteggere da diverse

minacce. Dall'eventualità che i dati vengano rubati insieme al dispositivo del dipendente, dalla possibilità che sia il dipendente stesso a rivendere a terzi i dati e dai possibili attacchi alla propria infrastruttura legati all'apertura di uno o più canali verso l'esterno, proprio per consentire l'uso di risorse aziendali. È dunque chiaro che un investimento diventa pressoché indispensabile per garantire un minimo di protezione ai dati aziendali. D'altronde

Sicurezza

Disponibili ma sempre al sicuro: la sicurezza dei dati è forse il problema più importante da affrontare

non si tratta sempre di pericoli causati esclusivamente dalla pratica del Byod: anche quando il cellulare o il portatile era di proprietà aziendale esisteva il rischio di un furto di dati. Nel caso del Byod però la sfida

è riuscire a garantire lo stesso livello di sicurezza su macchine che non hanno necessariamente i sistemi operativi aziendali e che non sono gestite dall'IT aziendale.

Infine i dispositivi di proprietà dei dipendenti possono difficilmente essere controllati limitando ad esempio l'installazione di giochi o di applicazioni anche al limite della legalità che



Nel Byod la sfida è riuscire a garantire lo stesso livello di sicurezza su macchine che non hanno necessariamente i sistemi operativi aziendali e che non sono gestite dall'IT aziendale

utilizzano magari eccessivamente la connessione a Internet aziendale. Per evitare problemi a tutta l'azienda è dunque fondamentale che ci siano sistemi automatizzati di controllo della banda e che esista la possibilità di un blocco in caso di consumi palesemente eccessivi. Nell'ottica di limitare la diffusione di malware o di altre minacce potrebbe anche essere necessario obbligare i dipendenti a installare qualche software antivirus su tutti i terminali che si collegano alla rete aziendale.

POLICY CHIARE PER TUTTI

Basta iniziare a parlare del fenomeno del Byod e dei pericoli e vantaggi che nasconde per capire che è fondamentale definire delle policy che ne regolamentino l'adozione. Si tratta della prima difficoltà davanti alla quale si trova ad esempio un sistemista al quale venisse chiesto di gestire l'accesso a dati e applicativi tramite terminali di proprietà del dipendente.

Se ad esempio l'azienda utilizza esclusivamente terminali Windows, come si può gestire un portatile Apple? Nel caso si adottino soluzioni specifiche per le piattaforme mobili iOS e Android, come comportarsi con un dipendente che ha un cellulare Windows Mobile o BlackBerry? Se non ci sono delle regole un dipendente potrebbe ad esempio sentirsi escluso solo perché il suo dispositivo è diverso da quelli aziendali. Nello stesso tempo l'azienda se per policy accetta il Byod deve necessariamente chiarire le specifiche degli strumenti che possono essere accettati in azienda e i limiti di utilizzo degli stessi. Dunque per ogni categoria di dispositivi (per esempio smartphone, tablet e portatili) bisogna comunicare chiaramente le specifiche in termini di hardware, sistemi operativi e persino applicazioni.

Queste caratteristiche non possono essere scritte nella roccia, ma devono anzi essere aggiornate frequentemente, proprio perché il fenomeno della consumerization rende tutto più veloce rispetto ai canoni aziendali. Ad esempio ad oggi moltissime aziende hanno solo Windows 7 in azienda, mentre chi ha comprato un computer per uso personale dal 2013 ad oggi quasi certamente lo ha preso con Windows 8 (o 8.1). Dunque la scelta di adottare il Byod richiede necessariamente tempi di aggiornamento più veloci per gli applicativi aziendali e

un supporto più rapido ai nuovi sistemi operativi sul mercato. Altrimenti è il concetto stesso di Byod a perdere significato. Lo stesso riguarda per esempio il mondo del *mobile*. I telefonini BlackBerry sono stati per anni la scelta preferita di molte aziende, ma oggi rappresentano una fetta di mercato risibile e in estinzione. Proprio per questo motivo se una azienda passa al Byod l'impatto su chi gestisce i sistemi informativi potrebbe portare a costi eccessivi o a inutili sprechi di risorse se ad esempio si richiede di mantenere il supporto sia a dispositivi di proprietà aziendale ma relativamente obsoleti come i terminali BlackBerry e Symbian, sia ai dispositivi di ultima generazione come i terminali Android fino alla release 4.4 e iOS fino alla 7. Nello stesso tempo i software e i connettori utilizzati lato server per supportare queste piattaforme sono differenti e non necessariamente compatibili e potrebbe essere difficile riuscire a garantire una connessione affidabile almeno alla posta elettronica, alla rubrica e all'agenda.

CYOD: UNA POSSIBILE ALTERNATIVA

Un termine di cui sempre più spesso si parla per risolvere la maggior parte delle problematiche legate al Byod è la sigla Cyod, *Choose Your Own Device*, letteralmente "scegli il tuo dispositivo". In questo approccio – differente per molti aspetti – il dipendente può decidere in autonomia quale dispositivo utilizzare (che si tratti di telefono, tablet o portatile), ma non andando al supermercato o al centro commerciale. Può effettuare la scelta a partire da un elenco di dispositivi approvati e preconfigurati, disponibili su un portale interno aziendale. Tipicamente in questo caso i dispositivi sono comunque di proprietà aziendale e il dipendente ha così il vantaggio di poter utilizzare il dispositivo che preferisce, senza pagarlo. D'altro canto l'azienda ha un numero comunque limitato di device da supportare, dunque le policy aziendali vengono necessariamente supportate. Con il Cyod la scelta dei dispositivi proposta al dipendente può poi variare in base al suo ruolo e possono esserci anche dipartimenti aziendali in cui non è disponibile questa soluzione, ma viene comunque fornito un accesso – pur limitato – alla rete, per l'uso con i propri terminali.



L'ACCORDO IBM/APPLE

Quando il Byod non è più sufficiente

Chi avrebbe mai pensato che due aziende diverse per concezione, approccio e tipologia di clienti come Apple e Ibm sarebbero arrivate a un accordo così importante per tutto il mondo dell'informatica? Apple, che sta certamente subendo una forte concorrenza sul fronte mobile da parte dell'ormai onnipotente Android di Google, vuole entrare nel settore corporate in modo più massiccio, passando non più dalla porta di servizio del Byod, ma da quella principale, presentandosi come un partner concentrato al 100% sulle aziende, con servizi, opzioni e assistenza dedicati agli utenti business. Sfruttando la diffusione oltre che l'appello dei suoi due prodotti iPhone e iPad (utilizzati da più del 90% delle aziende Global 500, secondo la stessa Apple) potrà così sfruttare i servizi e le applicazioni di Ibm, un punto di riferimento in tutto il mercato corporate.

L'accordo nasce certamente anche dalla necessità di migliorare la sicurezza e l'interoperabilità dei dispositivi iOS in azienda: tra i suoi punti principali c'è infatti la realizzazione di "servizi cloud Ibm ottimizzati per iOS, inclusi gestione dei dispositivi, sicurezza, analisi e integrazione mobile". Ibm poi venderà direttamente i dispositivi Apple, integrandoli con la sua piattaforma per il mondo mobile, chiamata MobileFirst Platform.

Così da una parte Apple avrà nella sua manica una nuova carta per promuovere la diffusione dei suoi dispositivi, dall'altra Ibm potrà proporsi con un pacchetto business completo e curato nei minimi dettagli, che comprende sia hardware sia software. Tra qualche anno potremo dire chi sarà il vero vincitore in questo accordo: Apple, Ibm o – se le cose non andranno per il verso giusto – magari Google o Microsoft.

IL PUNTO DI VISTA DEL DIPENDENTE



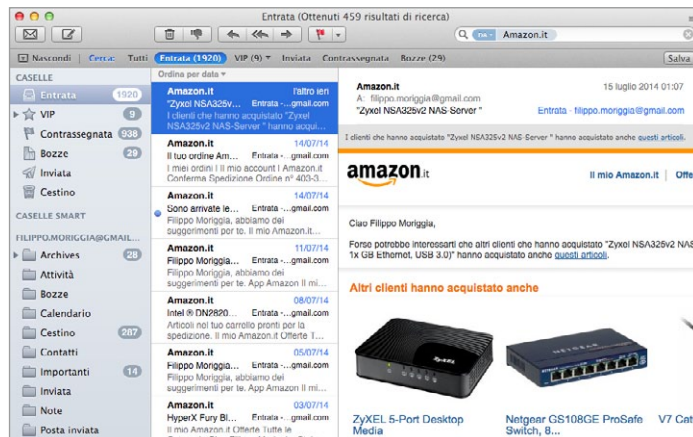
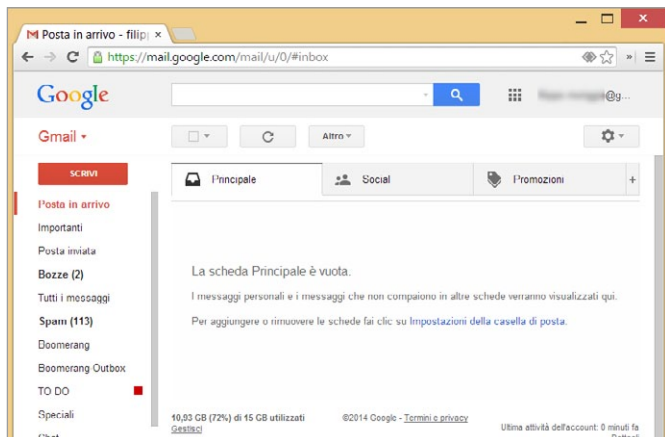
Il Byod coinvolge principalmente due attori: il dipendente e l'azienda. Vediamo di studiare brevemente il punto di vista di ciascuno di essi, offrendo dritte e suggerimenti utili ad entrambi. Iniziamo mettendoci nei panni del dipendente. Utilizzare il telefono o il portatile personale anche per l'uso aziendale ha certamente alcuni vantaggi ma può creare alcune difficoltà, soprattutto per i dipendenti che si trovano con un reparto IT non particolarmente propenso a intervenire su dispositivi che non appartengono al parco macchine aziendale. Diventa dunque importante sapersi "arrangiare" o comunque cercare di mettersi nella condizione più favorevole per sfruttare la situazione e lavorare comodamente. Il primo problema da affrontare è certamente quello della connessione all'email aziendale ed eventualmente all'agenda e ai contatti. In questo caso è certamente meglio cercare di separare nettamente l'email aziendale da quella personale non soltanto utilizzando ovviamente due account diversi (ad esempio *mario.rossi@dominioazienda.it* e *mario.rossi@gmail.com*) ma anche accedendo tramite due applicazioni o interfacce completamente separate. In caso contrario l'uso di un unico terminale può essere molto pericoloso: basterebbe infatti un attimo di distrazione per trovarsi a mandare un'offerta a un cliente con l'email personale o organizzare un addio al celibato

con quella aziendale. Se, ad esempio, si utilizza Outlook per collegarsi al server aziendale (il software Microsoft è certamente quello che offre maggiori garanzie di compatibilità con le piattaforme corporate), è meglio utilizzare un client differente o addirittura l'interfaccia Web per l'email personale. Naturalmente dal momento che il portatile nel caso del Byod è di proprietà del dipendente, l'installazione di un client email anche per uso personale è un diritto innegabile. Si può però optare per un client alternativo: chi è abituato a Outlook si troverà sicuramente a suo agio con l'ultima versione di Windows Live Mail. Per chi preferisce un client più sobrio ma comunque potente Mozilla Thunderbird è invece una valida alternativa, che può essere presa in considerazione anche da chi avesse acquistato un portatile Linux o OS X. Questi due sistemi operativi sono certamente meno diffusi e visti con maggiore diffidenza in ambito aziendale, ma non significa per questo che debbano essere emarginati. Su OS X per esempio si può sfruttare anche l'applicazione Mail fornita in dotazione con il sistema operativo: si interfaccia tranquillamente con i principali server email sul mercato e a differenza di Thunderbird è sviluppata

e supportata attivamente. Se cercate una applicazione che includa tutte le funzionalità di groupware per vedere anche il calendario e l'agenda condivisa aziendale sicuramente Outlook (disponibile comunque anche su Mac) è il punto di riferimento, ma si tratta di un prodotto a pagamento, incluso solo nelle versioni per l'azienda di Office (Home & Business e Professional). Chi non riuscisse a collegarsi con client alternativi e non avesse Outlook installato può ovviamente chiedere una licenza al reparto IT aziendale. Nella peggiore delle ipotesi la risposta sarà un no. Il programma Mail di Apple anche su iOS ha un buon livello di compatibilità e si comporta bene in quasi tutte le situazioni. Per chi dispone di un iPad o un iPhone la scelta è quasi obbligata. Su Android invece la scelta è più ampia, anche se non ci sono prodotti che si distinguono in particolar modo. L'app Gmail permette un livello di integrazione totale con l'omonima casella di posta, ma non supporta caselle di fornitori differenti. Dunque a meno che la vostra organizzazione non utilizzi la piattaforma Google Apps (nel qual caso Android è sicuramente la scelta migliore) dovrete cercare una app alternativa. Il client denominato *E-mail* non è purtroppo sempre all'altezza, anche se

Posta

Outlook, il client email Microsoft, offre maggiori garanzie di compatibilità in azienda



Per evitare di far confusione è meglio visualizzare i messaggi dall'interfaccia Web della propria casella personale o usare un client completamente diverso da quello aziendale.

Il client email Apple pur non essendo eccelso offre un buon livello di compatibilità con la maggior parte dei server aziendali, anche nella versione disponibile su iOS.

è migliorato nel tempo. Tra le soluzioni alternative più interessanti ci sentiamo di consigliare *Aquamail*: ha un'interfaccia curata e un approccio più professionale, ma nella versione gratuita ha qualche limitazione, tra cui l'obbligo di inserire nella firma il disclaimer "Inviato con Aquamail". Chi pensa di farne un uso continuativo non avrà comunque difficoltà a pagare i 3,77 euro della versione Pro.

Android dalla versione 4.2 ha introdotto, anche se solo per i tablet, la possibilità di gestire due o più utenti su un unico dispositivo. Purtroppo questa funzione non è attivabile sui terminali che hanno anche la funzione di telefono (come gli Asus Phonepad che sono a tutti gli effetti dei tablet), ma per tutti gli altri è una possibilità utilissima per chi pensa di sfruttarlo in azienda. Basta infatti creare un utente dedicato da usare al lavoro e tenerne uno solo per l'uso personale. Si potrà così utilizzare la stessa applicazione anche per la gestione della posta o dell'agenda: i dati rimarranno separati. Ovviamente la gestione sarà però più complessa per chi spesso passa dalle

applicazioni personali a quelle lavorative. Lo stesso problema si pone in effetti sui sistemi operativi che sono concepiti già a livello nativo come piattaforme multiutente, come Windows, OS X o Linux. In questo caso l'adozione di due profili deve essere valutata con attenzione: il passaggio da uno all'altro richiede un po' di tempo e può appesantire i portatili che già non sono particolarmente brillanti a livello di prestazioni. Certamente è l'ideale per chi vuole una separazione totale tra lavoro e vita personale. Chi dispone di un numero di telefono cellulare ad uso aziendale almeno qualche volta avrà pensato di acquistare un cellulare dual sim. Questi dispositivi sono principalmente basati su Android e sono sempre più diffusi anche nell'offerta delle marche più blasonate. Possono certamente essere una soluzione interessante per quanto riguarda l'uso Byod. Prima di acquistarli è bene valutare con attenzione anche i piani dati disponibili



Diversi produttori hanno oggi in catalogo smartphone dual sim: una soluzione brillante per gestire un numero privato e uno aziendale con un solo telefono.

sulla Sim privata e aziendale. Molti di questi telefoni infatti sono in grado di collegarsi in 3G (o 4G) con una sola Sim, quella principale: la seconda funziona esclusivamente in modalità Gsm per la gestione delle chiamate. Questo è un problema abbastanza significativo per chi ha ad esempio un operatore che usa (anche per telefonare) solo le tecnologie Umts/3G/4G, come Tre. Fortunatamente Android permette comunque di impostare la scelta dell'utenza telefonica ad ogni chiamata o in base a una opzione generale, facilmente modificabile. Il numero che si sta utilizzando per chiamare viene poi indicato chiaramente. Il venerdì sera dunque si può facilmente cambiare l'operatore predefinito, per evitare di addebitare erroneamente le chiamate sul numero aziendale.

IL PUNTO DI VISTA DELL' AZIENDA

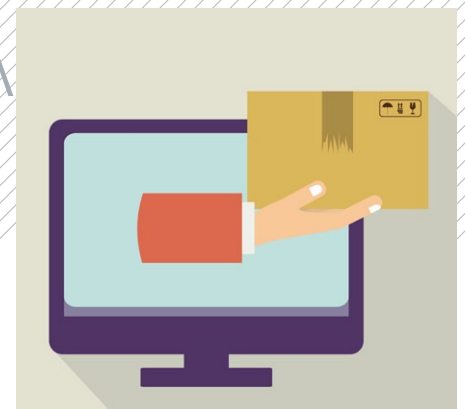
Nell'analizzare il punto di vista dell'azienda sono certamente molti di più i fattori da tenere in considerazione. In primo luogo il Byod non coinvolge esclusivamente l'ambito sistemistico, ma riguarda sia quello strategico e finanziario, sia i dipartimenti in cui viene applicato. La scelta di adottare il Byod deve dunque essere valutata con attenzione, considerandone tutti i possibili svantaggi, tra cui i rischi di furto dei dati e di sicurezza che porta con sé.

Ci saranno sicuramente dipartimenti e aziende in cui i benefici sono nettamente superiori ai rischi, mentre in alcuni ambienti specifici potrebbe non essere neppure preso in considerazione. In ogni caso è fondamentale, come già spiegato, che ci siano delle policy chiare e che venga predisposto un piano preciso per il

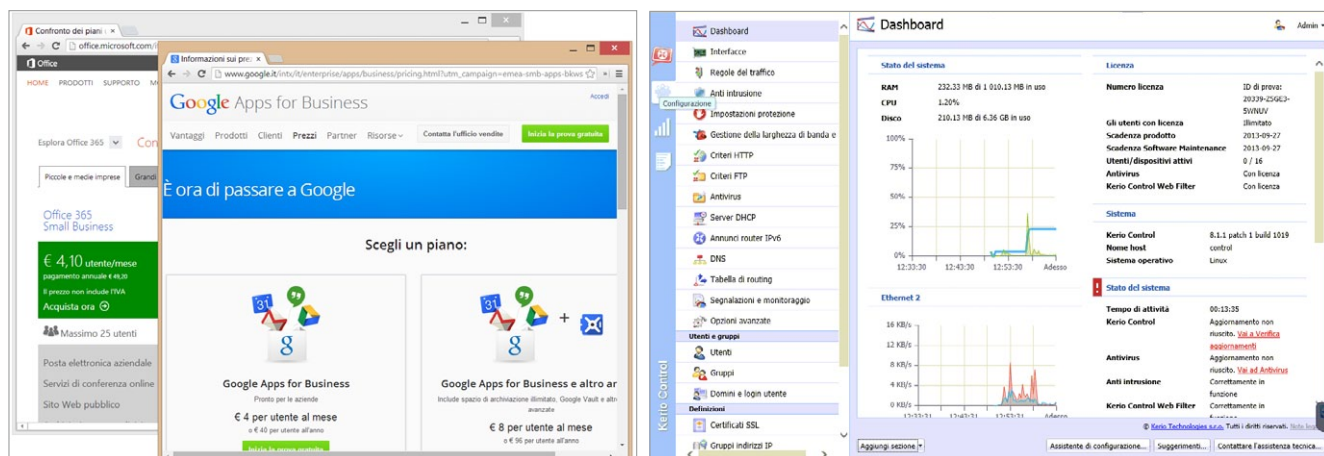
controllo e la messa in sicurezza dei dispositivi collegati alla rete aziendale *on premises* (dentro le mura) e *off premises* (fuori dalle mura).

La prima problematica da affrontare è quella della connessione, fuori e dentro le mura. Per la connessione dall'esterno bisogna affrontare due problemi, quello della connettività e quello della sicurezza della connessione.

Per quanto riguarda la connettività come già accennato il principale problema è la banda in upload, fondamentale quando la maggior parte del flusso dati è dall'interno (ad esempio dal server di posta aziendale) verso l'esterno. Purtroppo non in tutte le parti d'Italia questo problema può essere affrontato allo stesso modo. Nelle aree meglio coperte dai vari operatori si possono prendere in considerazione le connessioni simmetriche



in fibra (ad esempio 10 o 100 Mbit) o quelle via etere sempre simmetriche o con un buon livello di upload. Le esigenze in termine di banda in upload variano ovviamente in base al numero di dipendenti o agenti che si trovano all'esterno e in base all'uso che ne fanno. Per tutti una soluzione semplice ma non sempre facile da mettere in pratica è ovviamente lo spostamento della posta e di tutte le funzioni di groupware come agenda, contatti e così via nel cloud. Attivando ad esempio i servizi SaaS (*Software as a Service*) di Microsoft (Office 365) o Google (Apps) si può spostare



Le soluzioni di posta elettronica nel cloud (nella figura Google Apps) sono certamente più comode da utilizzare in un'ottica Byod.

Kerio Control è un firewall commerciale che integra anche funzionalità di filtro dei contenuti e di antivirus.

fuori dall'azienda questo servizio con un costo fisso abbastanza limitato e facilmente controllabile (rispettivamente 60,02 e 48,80 euro a utente all'anno Iva inclusa per i piani base *Small Business* e *For Business*).

Per quanto riguarda invece la sicurezza della connessione la problematica può essere affrontata in modi diversi. Nel caso più semplice potrebbe essere sufficiente aprire le porte del firewall aziendale per consentire la connessione diretta al server e-mail o ad altri server locali. In questo caso ovviamente le connessioni dovranno essere protette tramite la tecnologia Ssl/Tls, per evitare che password e altri dati sensibili possano essere intercettati durante la trasmissione.

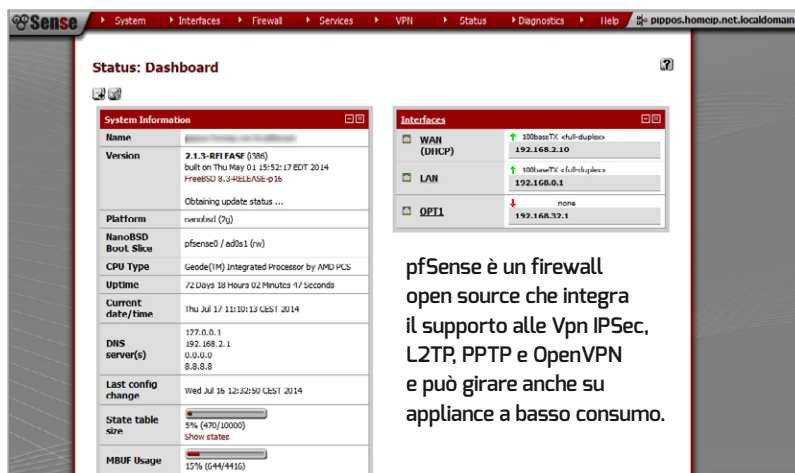
In alternativa si può adottare una soluzione Vpn che garantisca un collegamento sicuro alla rete aziendale, in modo che tutti gli applicativi agiscano come se il computer o il cellulare fosse all'interno della Lan. La soluzione Vpn scelta deve utilizzare algoritmi sicuri, dunque è certamente meglio dare priorità alle soluzioni basate su IpSec o sulla piattaforma OpenVPN. In ogni caso è bene verificare che i protocolli di cifratura siano attivati e vengano configurati come requisito per il successo della connessione. Alcune tecnologie abbastanza diffuse come la rete Vpn Microsoft Pptp (*Point to Point Tunneling Protocol*) per esempio vengono spesso utilizzate senza cifratura, con tutti i problemi che questo comporta.

Nel caso di una connessione Vpn ovviamente il firewall aziendale dovrà limitare l'accesso, per quanto possibile, ai server e alle macchine che devono effettivamente essere raggiunte dall'esterno, per limitare i danni in caso ad esempio di un portatile infetto che si collega da remoto. Le soluzioni gestite

– *managed* – più efficaci sono certamente quelle che utilizzano un agent dedicato da installare sul computer del dipendente e verificano ad esempio che il sistema operativo abbia le necessarie patch di sicurezza e che l'antivirus sia aggiornato: i dispositivi che non sono *compliant*, cioè che non soddisfano i requisiti vengono automaticamente relegati a uno stato di quarantena, per evitare che possano infettare altre macchine o creare problemi. Chi non utilizza già soluzioni di firewall commerciali può valutare ad esempio il progetto open source pfSense (www.pfsense.org), basato su FreeBSD che può girare tranquillamente sia su un Pc, anche datato, sia in macchina virtuale sia su appliance dedicate (come quelle basate sulla piattaforma Alix di PC Engines). Nonostante si tratti di un progetto open source chi lo sviluppa offre – qualora fosse necessario – supporto commerciale a pagamento (prezzi a partire da 400 dollari Usa, assistenza solo in lingua inglese). pfSense supporta IPsec, Pptp e OpenVPN. È interessante notare che per la creazione di una Vpn con OpenVPN,

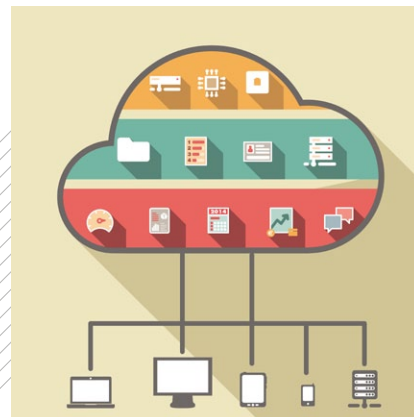
una delle tecnologie più complesse, è disponibile ad esempio un comodo wizard guidato e un plugin (*Client Export*) che permette l'esportazione diretta dei file necessari per la connessione da tutti i principali sistemi operativi (Windows, Linux, Mac, Android, iOS).

Un altro prodotto interessante, anche se commerciale, per chi cerca una soluzione facile da gestire e configurare è Kerio Control (www.kerio.com), che integra anche funzionalità di controllo dei contenuti, una feature non disponibile sui prodotti gratuiti. Control fa della semplicità la sua forza e include procedure guidate per la configurazione che permettono anche a un utente alle prime armi con conoscenze di base di networking di configurare una soluzione Vpn complessa come IPsec. Il prodotto è completamente tradotto in italiano ed è facile avere supporto grazie ai due distributori italiani (Coretech, www.coretech.it e Multiwire, www.multiwire.net) e una ampia rete di rivenditori. I prezzi partono dai 258,64 euro (Iva inclusa) per i primi 5 utenti.



pfSense è un firewall open source che integra il supporto alle Vpn IPsec, L2TP, PPTP e OpenVPN e può girare anche su appliance a basso consumo.

DISPOSITIVI SOTTO CONTROLLO



Il Byod nasconde molti pregi, ma può diventare un vero incubo per il reparto IT se non si utilizzano soluzioni dedicate per il controllo dei dispositivi. Una volta risolti i problemi di connettività bisogna prima verificarne la *compliance*, controllando che rispettino le policy aziendali, poi bisogna connetterli e configurarli di conseguenza, installando applicazioni o utility necessarie al buon funzionamento del sistema. Fortunatamente esistono soluzioni che permettono di gestire queste problematiche in automatico, con un sistema di controllo e gestione centralizzato.

In questo settore si fa ovviamente differenza tra i computer che usano sistemi operativi tradizionali (Windows, OS X, Linux) e i device mobili, come smartphone e tablet. Iniziamo col parlare dei primi. In generale il collegamento del computer dei dipendenti alla rete aziendale è ancora più critico rispetto al collegamento di un telefono, anche se di ultima generazione. Un notebook infatti include un disco di grosse dimensioni con cui si possono rubare anche molti dati. Il numero di virus e di cavalli di troia disponibili per la piattaforma Windows è certamente molto elevato e ci sono malware specifici che sfruttano la rete locale per la loro diffusione. Diventa pressoché fondamentale avere la certezza che le macchine che si collegano

on premises oltre ad avere un sistema operativo e dell'hardware adeguato per riuscire a utilizzare le applicazioni e gli strumenti aziendali siano protette con un antivirus aggiornato e perfettamente funzionante. Inoltre è importante verificare che non avvengano furti di dati o che il dispositivo esterno non abbia accesso a share di rete o archivi particolarmente critici dal punto di vista della sicurezza. A titolo di esempio citiamo due soluzioni abbastanza differenti ma ugualmente interessanti da utilizzare per proteggere l'azienda e definire meglio i limiti di accesso dei dipendenti.

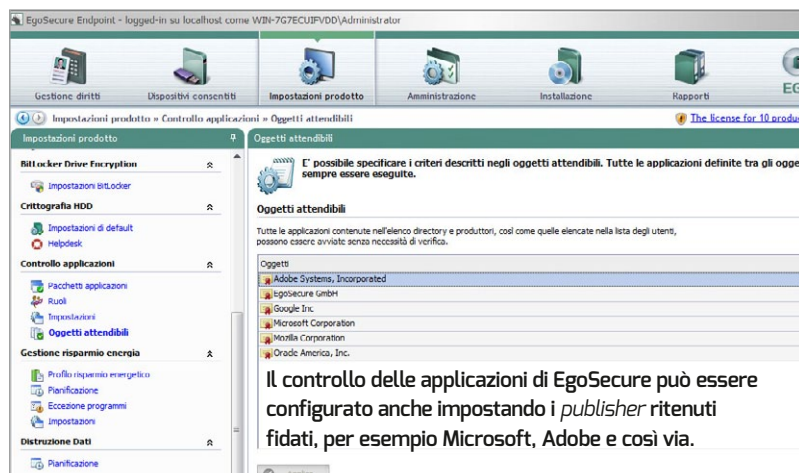
Policy

È fondamentale definire quali sono i sistemi operativi supportati all'interno dell'azienda

La prima soluzione che abbiamo valutato è EgoSecure Endpoint (www.egosecure.com), una suite sviluppata dalla omonima casa tedesca che fa della protezione dei dati (Dlp, *data loss prevention*) il suo punto di eccellenza. La suite è completamente modulare sia a livello funzionale sia per quanto riguarda i costi. Utilizza un sistema di licenza flessibile che permette di acquistare separatamente le licenze per ogni singola funzionalità e assegnarle ai vari computer della rete. Uno dei moduli disponibili è il *Controllo degli accessi* che permette di controllare gli accessi e i trasferimenti di dati verso chiavette Usb, Cd, Dvd, rete e piattaforme cloud. In questo caso il supporto è ampio e prevede la possibilità di bloccare o regolamentare il collegamento al computer di periferiche

di qualsiasi tipo come Floppy, Cd, Pda, schede esterne, dispositivi Android o iOS. Questo modulo, come tutti quelli della suite, è amministrato centralmente dalla console del prodotto che deve essere installato su un server Windows (con o senza *Active Directory*, su database MySQL o Microsoft SQL Server o Sql Server Express). I pacchetti per l'installazione vengono generati direttamente dal server e possono essere distribuiti tramite AD o una semplice share di rete. Il costo di listino del pacchetto di controllo degli accessi per singola postazione all'anno è ad esempio di 14,15 euro (Iva inclusa). EgoSecure comprende anche un modulo antivirus (18,67 euro all'anno a postazione) basato sul premiato engine di BitDefender, ma può essere utilizzato anche in combinazione con un altro antivirus, sia aziendale, sia installato dal dipendente. Se l'azienda sospetta o teme fortemente la violazione di segreti aziendali o il furto di dati ad opera di un dipendente o collaboratore può attivare anche il modulo *Audit* che permette di raccogliere informazioni dettagliate su ciò che i dipendenti fanno con il computer personale o aziendale quando sono in azienda senza violare in alcun modo la legge che è sempre a garanzia dei diritti e della privacy del cittadino. I log catturati da questo modulo infatti non sono accessibili neppure all'amministratore di sistema ma possono essere esportati e analizzati esclusivamente con un principio di autorizzazione a due o tre persone. Vengono infatti utilizzati solo in caso di un procedimento legale e richiedono l'autorizzazione appunto di più attori, come il responsabile del personale e un rappresentante sindacale. Questo modulo, che verrà probabilmente attivato solo sulle macchine dei dipendenti su cui si ha qualche dubbio o sospetto, costa 14,15 euro annue, a postazione.

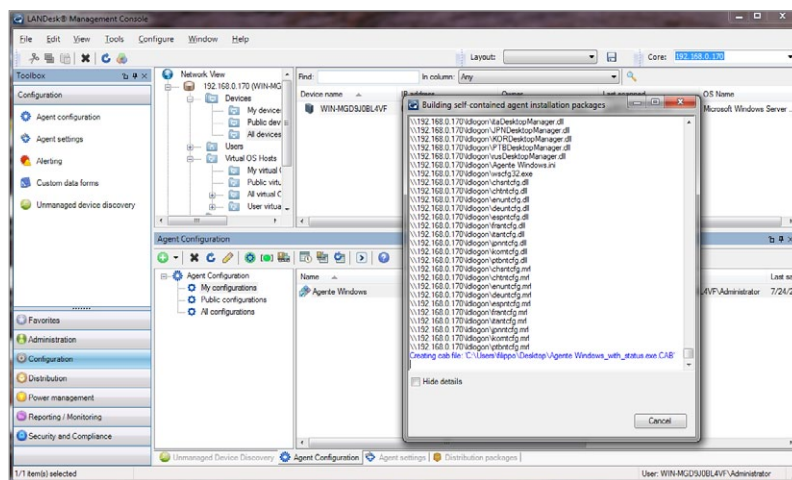
Un altro modulo interessante soprattutto nell'ottica Byod è il *Controllo delle applicazioni* che permette di prevenire l'installazione di software non autorizzati, con una naturale riduzione della perdita di produttività e un livello altissimo di protezione da malware e software pericolosi ancora non riconosciuti in termini di imminente virali. In questo modo – quando il



Il controllo delle applicazioni di EgoSecure può essere configurato anche impostando i publisher ritenuti fidati, per esempio Microsoft, Adobe e così via.

computer è in azienda – possono essere utilizzate solo le applicazioni autorizzate. Il software include una serie di pacchetti standard preconfigurati e una procedura di analisi dei software installati che semplificano la definizione di una *white list*. Il pannello di gestione di Egosecure mette il dipendente in condizione di chiedere facilmente l'apertura di un ticket per una richiesta di autorizzazione non solo all'accesso di un'applicazione, ma anche all'uso di una chiavetta Usb o di un'altra periferica. In questo modo il dipendente non si sente limitato, ma può facilmente chiedere l'aggiunta di permessi qualora la configurazione iniziale sia troppo restrittiva. Il modulo di controllo applicazioni costa 7,08 euro a postazione, all'anno. Lo stesso Egosecure include svariati moduli per la cifratura di cartelle locali o di rete, risorse condivise nel cloud o addirittura per criptare l'intero disco di sistema, sia usando una soluzione proprietaria, sia usando un sistema dedicato per la gestione della tecnologia Bitlocker di Microsoft. Anche in questo caso i costi variano: si parla di 46,85 euro per la cifratura completa del disco con la soluzione proprietaria, 3,54 euro per il sistema di gestione di Bitlocker, 11,60 per la cifratura dei dispositivi rimovibili e 28,18 per il cloud e le cartelle di rete. Tutti i prezzi sono sempre a postazione all'anno, Iva inclusa.

È interessante notare che nell'ottica della massima semplicità d'uso il sistema di cifratura di Egosecure è trasparente – per quanto possibile – all'utilizzatore.



La console di gestione di Landesk permette di tenere sotto controllo tutti i Pc dell'azienda e di generare l'agent da installare su ogni client.

Dunque nello spostamento di dati su una chiavetta il dipendente non deve preoccuparsi di attivarlo manualmente, ma il software può adottare automaticamente la protezione. Egosecure funziona esclusivamente con client e desktop Windows ed è distribuito in Italia da Coretech.

Il secondo prodotto per la gestione di computer che abbiamo studiato a titolo di esempio è LANDesk Security Suite. Questo sistema ha un approccio ancora più enterprise e fa parte di una offerta integrata e modulare che comprende tutti i prodotti LANDesk. Nella sua versione base ha un costo abbastanza basso (18,30 euro Iva inclusa a dispositivo, con 12 mesi di aggiornamenti, sconti quantità e legati alla tipologia di cliente esclusi) e offre un buon numero di funzionalità che vanno dal controllo della compliance dei dispositivi al controllo delle applicazioni. Oltre a verificare la presenza di un antivirus supportato e a includere un personal firewall più sofisticato di quello integrato

in Windows, la Security Suite di LANDesk permette di applicare policy remote, di cifrare i dispositivi Usb, di segnalare le vulnerabilità e la disponibilità di patch per il sistema operativo. Sono esclusi dal prezzo citato le funzioni di antivirus, di antispyware e di manutenzione. Un punto di forza di LANDesk è certamente il supporto a un numero di piattaforme particolarmente ampio: non si limita infatti solo a Windows, ma può gestire anche terminali OS X e Linux. Come nel caso di Egosecure poi le policy e le restrizioni applicate possono essere differenti quando il portatile viene collegato in azienda o a casa, per evitare di limitare l'utilizzatore quando lavora entro le mura domestiche con un dispositivo di sua proprietà.

Le soluzioni di sicurezza vengono normalmente vendute da LANDesk con un costo a dispositivo, ma esistono anche formule di pagamento a utente, in particolare per le due soluzioni più complete,

UNA RETE WI-FI SICURA

Le reti Wi-fi sono indispensabili per permettere il collegamento on premises di dispositivi come tablet o smartphone, ma costituiscono di fatto un rischio non da poco per la sicurezza aziendale. Innanzitutto spesso possono essere raggiunte anche nei dintorni dell'azienda, al di fuori delle mura, poi rappresentano uno strumento fin troppo semplice per l'accesso ai dati anche da parte di ex dipendenti o ex collaboratori. Come fare dunque a garantire un accesso sicuro? Una prima pratica molto semplice è quella di attivare una rete Wi-fi solo per gli ospiti, così da tenerli separati dalla rete aziendale e bloccare l'accesso ai server locali. In questo modo se la password di questa rete è poco sicura si limitano anche notevolmente i rischi. Tutti i dipendenti o i collaboratori che hanno solo la necessità di un accesso a Internet possono utilizzare questa rete che avrà ovviamente un SSID (l'identificativo della rete) diverso.

Ci sono router, access point e soluzioni di fascia corporate che integrano direttamente la funzionalità di rete ospite nella loro configurazione. È

importante valutarla già nella fase di acquisto. Se ad esempio si sta cercando una soluzione in grado di coprire un'area ben più ampia di quella di un normale appartamento o un piccolo ufficio, sfruttando più access point gestiti in modo centralizzato, l'americana Ubiquiti (www.ubnt.com) offre una piattaforma chiamata Unifi che è particolarmente semplice da configurare e gestire e non ha costi particolarmente elevati. Con questa soluzione la rete guest è automaticamente bloccata dall'accesso alla rete locale e si possono definire policy per limitare anche l'uso di banda da parte degli ospiti. Unifi è distribuita in Italia da Sice Telecom (www.sicetelecom.it). Naturalmente non mancano le soluzioni anche di tutti i principali produttori di dispositivi di networking, come Cisco, Netgear o D-Link. A livello di sicurezza le organizzazioni di dimensioni anche solo medio-piccole devono valutare necessariamente la versione Enterprise del protocollo di sicurezza Wpa. Questa sfrutta un sistema di autenticazione centralizzato chiamato Radius (Remote Authentication Dial-In User Service) che permette

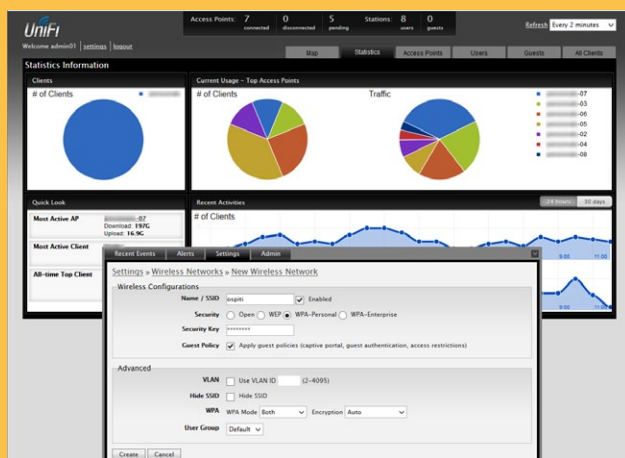


Prey permette di tracciare gratuitamente fino a due dispositivi tra cellulari e notebook. Supporta Windows, Mac, Linux, iOS e Android.

denominate *Secure User Manager* (Sum) e *Total User Manager* (Tum). Questi pacchetti comprendono tutte le funzionalità disponibili della piattaforma con la sola esclusione delle funzionalità di Service Management che sono disponibili solo per la Tum e hanno un costo pari rispettivamente a 140,30 e 170,80 euro a utente. Adottando queste soluzioni ogni dipendente può avere anche due o più dispositivi a lui intestati, senza alcun costo aggiuntivo. Dopo aver parlato di computer nel senso più classico del termine, vediamo come proteggere invece i sempre più diffusi ed evoluti dispositivi mobili. In questo settore il termine più in voga del momento è certamente Mdm, sigla che sta per *Mobile Device Management*, gestione dei dispositivi mobili. Appartengono infatti alla categoria Mdm i software di cui vi parliamo, poiché permettono di gestire i dispositivi utilizzati dai dipendenti dell'azienda in modo centralizzato. Nell'ultimo periodo i vendor

di prodotti del settore si sono sbizzarriti anche con molte altre sigle: Mam (*Mobile Application Management*, gestione delle applicazioni aziendali su dispositivi mobili), Mcm (*Mobile Content Management*, gestione dei contenuti), Mem (*Mobile Email Management*, gestione della posta elettronica), Msm (*Mobile Security Management*, protezione dei dispositivi). Le stesse piattaforme EgoSecure e LANDesk già citate integrano anche funzionalità specifiche per la protezione dei dispositivi mobili. EgoSecure ad esempio ha un modulo dedicato compatibile sia con iOS sia con Android. Per quanto riguarda iOS il dispositivo può inviare direttamente via email ai dispositivi un file completo per la configurazione di tutte le policy del telefono (o del tablet) Apple, senza installare alcuna applicazione. Per Android invece si può distribuire sempre via e-mail una applicazione dedicata che ha qualche limite rispetto alla soluzione Apple ma permette di definire alcune

impostazioni importanti, come l'obbligo di un Pin/password, procedure di cancellazione remota in caso di furto, blocco dello schermo in caso di non uso e volendo anche cifratura del dispositivo. Questo sistema permette anche di definire white list e black list per le applicazioni e fornisce informazioni sullo stato del dispositivo all'amministratore di sistema. LANDesk ha recentemente acquisito invece l'azienda israeliana LetMobile che sviluppa un software per la protezione delle applicazioni aziendali e delle comunicazioni via posta, può così fornire un sistema di protezione adeguato anche per i dispositivi mobili che devono collegarsi alla rete aziendale. Chi non avesse implementato alcun sistema di gestione centralizzato può comunque fare qualcosa per migliorare la sicurezza dei dispositivi mobili, ad esempio attivando le funzioni di Apple e Google per il ritrovamento e il wipe remoto del telefono. Sulla piattaforma Android esistono strumenti eccellenti per il controllo del sistema in caso di furto, citiamo ad esempio Prey (che può funzionare anche su un portatile Windows, con un unico account personale) e Cerberus (www.cerberusapp.com). Prey (www.preyproject.com) è gratuito entro alcuni limiti, mentre Cerberus è disponibile solo a pagamento. Merita sicuramente una menzione anche Plan B, una applicazione per gestire un telefono rubato pensata per essere installata persino dopo il furto, sfruttando l'interfaccia Web del Play Store accessibile da qualsiasi browser. •



I sistemi unificati per la gestione di reti Wi-fi aziendali come quello in figura permettono di creare reti ospiti e di limitare la banda utilizzata.

di utilizzare ad esempio la stessa password di Active Directory o della rete aziendale per autenticarsi sulla rete. La configurazione è certamente più complessa e richiede un server in grado di gestire questo protocollo, ma i vantaggi sono notevoli. I dipendenti che cambiano azienda o si licenziano ad esempio vengono immediatamente esclusi dall'accesso, senza che sia necessario procedere ogni volta al cambiamento della password di tutta la rete. Una soluzione più semplice per la gestione dell'autenticazione può essere invece l'adozione di un Captive Portal. Questa tecnologia prevede che al primo accesso a qualsiasi sito o pagina Web il gateway richieda all'utente di autenticarsi, attivando di fatto la connessione su quel dispositivo. Si tratta di fatto dello stesso sistema utilizzato in aeroporti o altri hotspot: è certamente più scomodo ma non per questo meno funzionale. Questa funzionalità può essere gestita direttamente da molti firewall, come pfSense e Kerio Control che vengono citati nell'articolo, ma anche da alcune soluzioni di Wi-fi centralizzate, come la stessa UniFi di Ubiquiti.