



McAfee **Security Connected**:
sicurezza completa
e conveniente

Sommario

COTS vale più di GOTS.....	4
Semplicità contro complessità: l'approccio della piattaforma.....	5
I clienti ne hanno compreso il valore.....	6
Un'unione vincente.....	6
Ulteriori informazioni.....	7

Anche prima degli effetti dei tagli, il Professional Services Council prevedeva una riduzione del bilancio federale statunitense per l'informatica dai 121,7 miliardi di dollari del 2012 ai 115,5 miliardi del 2013¹. Questa riduzione fa parte di ciò che il CIO del governo degli Stati Uniti Steven VanRoekel definisce "fare di più con meno risorse": un'iniziativa tesa a rendere efficiente ed efficace il reparto informatico nelle varie sfere governative, a stimolare l'innovazione, eliminare gli sprechi, semplificare e razionalizzare le operazioni delle agenzie². Allo stesso tempo, VanRoekel e altri esperti ammettono che le attività per la sicurezza informatica federale non devono risentirne. Se non altro perché le esigenze di sicurezza informatica delle agenzie governative sono aumentate, come illustrato dalla prossima pubblicazione *Security and Privacy Controls for Federal Information Systems and Organizations* (Controlli di sicurezza e privacy per i sistemi informatici e le organizzazioni federali) del National Institute of Standards and Technology (NIST), un catalogo delle tecnologie di sicurezza che aiutano le agenzie a soddisfare le normative FISMA e altre ancora³.

Poiché i bilanci federali sono in diminuzione, mentre sia le minacce informatiche sia gli obblighi sono in aumento, la domanda è: "Si può avere una sicurezza informatica completa che fornisca una visibilità della minaccia in tempo reale e a un costo ragionevole?". La risposta è "sì". Non solo si può ottenere una sicurezza esaustiva e conveniente, ma tramite la struttura Security Connected di McAfee – ora parte di Intel® Security – si adotta un metodo migliore che applica integrazione, informazioni sulle minacce in tempo reale, correlazione e velocità per ottenere una protezione robusta a un prezzo inferiore rispetto alle soluzioni alternative e singole. La stessa struttura che offre una protezione più solida, permette anche quelle efficienze operative che perseguono l'obiettivo di VanRoekel di una semplificazione e una razionalizzazione del reparto informatico.

La struttura Security Connected è studiata per aiutare la clientela a integrare i più svariati prodotti, servizi e partnership per mitigare in modo centralizzato, efficiente ed efficace i rischi per la sicurezza. Mike DeCesare, presidente di McAfee, ha descritto la necessità di una tale struttura – e delle sfide che l'industria della sicurezza si trova ad affrontare – in un intervento alla Casa Bianca: "Dobbiamo unificare, semplificare e potenziare il modo in cui forniamo sicurezza, tramite l'utilizzo di una struttura che integri le tecnologie più disparate, gettando dei ponti fra le "isole" della sicurezza per colmare le lacune nella copertura e nella tecnologia. In McAfee chiamiamo questo approccio Security Connected".

Basato su oltre vent'anni di pratiche di sicurezza collaudate, l'approccio Security Connected aiuta le agenzie e i programmi di qualsiasi dimensione – in ogni parte del mondo – ad aumentare la sicurezza, a ottimarla per una maggiore efficienza nei costi e ad allinearla strategicamente alle iniziative dei governi.

Le risorse e gli strumenti di Security Connected offrono un percorso chiaro, dal concetto della sicurezza alla sua messa in pratica, e sono in grado di adattarsi ai rischi, all'infrastruttura e agli obiettivi specifici di un'azienda. I sistemi sono infatti scalabili, il che li rende ideali per la distribuzione nei programmi più piccoli come negli ambienti delle agenzie più grandi.

Architettura di riferimento Security Connected

La struttura Security Connected costituisce una piattaforma e un'architettura delle migliori procedure che offrono resilienza all'infrastruttura governativa:

- sistemi di controllo e comando per il "campo di battaglia";
- monitoraggio costante;
- servizi digitali essenziali per il governo;
- preparazione agli attacchi;
- reazione guidata dalle informazioni;
- condivisione sicura delle informazioni per le operazioni congiunte;
- mobilità sicura;
- centri operazioni di sicurezza;
- centri dati per i servizi condivisi;
- infrastruttura virtualizzata sicura;
- ambienti di rete tattici.

Cosa ancora più importante, Security Connected offre resilienza: la possibilità di continuare le attività durante un attacco informatico. La resilienza richiede:

- azione immediata per la difesa o la reazione;
- agilità per adottare le nuove tecnologie con le possibilità che aprono oppure per aggiungere rapidamente funzioni in risposta a una nuova minaccia;
- con l'aumento delle dipendenze, lo stimolo della collaborazione con una comunità che condivide lo stesso interesse.

La piattaforma Security Connected presenta resistenza e resilienza nei confronti delle minacce avanzate, la capacità di rispondere alla velocità della rete e una struttura che consente l'aggiunta di nuove funzioni. Insieme al nostro programma per i partner McAfee® Security Innovation Alliance, la struttura offre un allineamento senza pari alle esigenze di difesa informatica dei governi e livelli di scalabilità, sopravvivenza e integrazione senza precedenti, per proteggere i difficili ambienti governativi.

In che modo la struttura è conveniente? La risposta si trova nel risparmio costituito dal software già pronto per le aziende (commercial off-the-shelf, COTS).

COTS vale più di GOTS

Noi sviluppiamo software COTS: i costi di ricerca, sviluppo, manutenzione e aggiornamento perpetuo sono assorbiti da McAfee e distribuiti su un gran numero di utenti commerciali. La ragione per cui il COTS è diventato obbligatorio in molti programmi governativi e aziendali è che i prodotti COTS offrono un risparmio significativo in fase di approvvigionamento, sviluppo e manutenzione. I costi della soluzione sono inferiori a quello del software personalizzato e i vantaggi sono spesso maggiori.

L'opposto sono le soluzioni già pronte e personalizzate per i governi (government off-the-shelf, GOTS). Nel mercato della sicurezza informatica i governi hanno espresso l'esigenza di strumenti di sicurezza specializzati che richiedono uno sviluppo personalizzato, non sono collaudati sul campo e sono costosi da usare e mantenere. A volte tali strumenti specializzati non vengono neanche distribuiti ma, dato che ci sono i fondi, i soldi vengono spesi lo stesso. Il Programma di Gestione e Valutazione dei Rischi (Risk Assessment and Management Program, RAMP) del Dipartimento Statunitense per la Sicurezza Nazionale offre un esempio notevole, con 57 milioni di dollari sprecati nonostante le buone intenzioni⁴.

Le proposte sembrano dare risposta a problemi concreti ma, in realtà, i sistemi possono non essere compatibili con gli altri nell'ambiente di rete oppure potrebbero non funzionare sulla vasta scala richiesta dal governo. Una soluzione potrebbe funzionare perfettamente bene nel laboratorio in cui è stata sviluppata ma, quando messa in un ambiente reale a confronto con minacce reali, può dar luogo a problemi imprevedibili. Se una soluzione non può essere resa operativa in modo efficiente, i risultati ottenuti in laboratorio non contano. Un ottimo strumento potrebbe essere efficace in una rete di 50.000 endpoint, ma come si comporterebbe con 500.000 o anche un milione di endpoint?

Nel 2012, una fonte rivelò che l'Ufficio Informazioni e Tecnologia (OIT) del Dipartimento per i Veterani (VA) degli Stati Uniti aveva distribuito solo il 16% delle 400.000 licenze di crittografia degli endpoint acquistate, nonostante il ripetersi delle violazioni dei dati. La successiva indagine appurò che: "L'OIT non aveva installato e attivato tutte le licenze a causa dell'inadeguatezza di pianificazione e gestione del progetto. Nello specifico, l'OIT non aveva previsto i tempi necessari per: testare il software e assicurarne la compatibilità con i computer del VA, garantire la disponibilità di personale sufficiente a installare il software di crittografia nei computer del VA e monitorare adeguatamente il progetto per verificare la cifratura di tutti i computer desktop e portatili del VA⁵."

A favore degli strumenti GOTS non gioca neppure il rapporto costi-benefici. Prendiamo in considerazione i punti seguenti:

- le singole soluzioni autonome richiedono singoli controlli di gestione e singole persone che li utilizzino;
- finiscono con l'essere isolate l'una dall'altra e la condivisione delle informazioni consiste in uno scambio di fogli di calcolo, ognuno dei quali contiene masse di informazioni che non producono una vera sicurezza, ma ne moltiplicano le attività da seguire;
- questo metodo di integrazione tramite i fogli di calcolo è molto laborioso e inefficiente soprattutto se si considera che, in molte organizzazioni, il 70%-80% del budget informatico se ne va in costi operativi.

Per ridurre i costi IT in un ambiente con ristrettezze di bilancio, bisogna cercare una soluzione che riduca quel 70%-80% di costi operativi. La struttura Security Connected di McAfee è proprio quella soluzione.

Un'altra ragione per cui i COTS sono superiori ai GOTS è che il settore privato è generalmente meglio equipaggiato per sviluppare le soluzioni IT più aggiornate in un ambiente in rapida evoluzione. Ciò è vero soprattutto nella sicurezza informatica, in cui la velocità e il volume delle minacce sono così elevati che le aziende di sicurezza innovano costantemente per poterle contenere. Nel momento in cui le esigenze dei governi vengono tradotte in soluzioni personalizzate, le minacce sono già mutate e le esigenze potrebbero essere più adatte alle minacce di ieri piuttosto che a quelle di domani. Il ruolo del governo dovrebbe essere quello di abilitare la ricerca di base nella sicurezza informatica, non la ricerca applicata che sfocia nello sviluppo dei prodotti.

Semplicità contro complessità: l'approccio della piattaforma

Anche se potrebbe sembrare controproducente, l'approccio semplice alla sicurezza è più efficiente di quello complesso. Anzi, come ha affermato Howard Schmidt durante la nuova transizione del servizio di sicurezza dal governo al settore privato, la complessità è nemica della sicurezza e di certo è più costosa. L'aver una sola struttura o suite di prodotti, in grado di soddisfare tutte le proprie esigenze, è estremamente sensato. Questo approccio semplice è di gran lunga superiore a una serie di strumenti che potrebbero non collegarsi l'uno con l'altro e che complicano la reportistica. Inoltre non c'è più bisogno di coprire tutte le minacce con numerosi fornitori di sicurezza, dato che con l'approccio esaustivo ci si affida a quello giusto. La piattaforma Security Connected offre le capacità fondamentali, oltre a un ambiente aperto che copre l'intera gamma di esigenze in materia di sicurezza, sia attuali sia emergenti, con la massima efficienza.

Con il portafoglio di prodotti McAfee, a disposizione tramite Security Connected, le difese della rete apprendono e proteggono allo stesso tempo, diventando sia produttori sia consumatori delle informazioni sulle minacce che provengono dalla rete stessa. Creano un ecosistema che tende alla resilienza, rimuovono gran parte del rumore di fondo e si concentrano sulle minacce più complesse per usare al meglio le risorse limitate. Dato che le soluzioni automatizzano le attività di protezione gestendo simultaneamente le policy, si generano meno avvisi, eventi e dettagli che distraggono gli amministratori. Ciò che rimane sono le cose che contano di più e che hanno più bisogno dell'attenzione umana.

Questo ecosistema viene informato dal servizio McAfee Global Threat Intelligence (McAfee GTI) che, essendo integrato nelle nostre soluzioni, le alimenta con la ricerca sulle minacce nel mondo reale e in tempo reale, per consentire una percezione continua della situazione. McAfee GTI funge da sistema immunitario, proteggendo dagli attacchi tramite il rilevamento e la correlazione elettronici, alla velocità del computer, dei dati comportamentali che le fonti di tutto il mondo hanno identificato come nocivi. In pochi millisecondi McAfee GTI valuta le modifiche, assegna i livelli di rischio e distribuisce ai prodotti le raccomandazioni di protezione a copertura di ogni vettore di minaccia su ogni livello.

La piattaforma Security Connected, combinata con McAfee GTI, facilita la gestione della sicurezza per le aziende di tutte le dimensioni, in modo che l'integrazione delle relative protezioni e controlli e la creazione di un processo di base e di escalation per i rischi principali diventano delle attività più semplici. Con l'approccio Security Connected si ha una piattaforma integrata di soluzioni intelligenti che sfruttano le informazioni sulle minacce. Tali soluzioni sono più affidabili e generano fiducia nei sistemi informatici come PC e portatili, oltre che tablet, smartphone e sistemi integrati, che sono trasversali alle reti e usano il cloud, vi risiedono oppure ne creano uno proprio. Con McAfee si ha una copertura di ampio respiro, con molti meno contratti e minore complessità, così è davvero possibile fare di più con meno risorse. In un'unica piattaforma si possono avere da 35 a 40 controlli distinti e certificati NIST, senza dover avere da 35 a 40 diversi contratti.

E con Security Connected si hanno delle opzioni in più. Tramite McAfee Security Innovation Alliance, si può trarre vantaggio dalle più innovative tecnologie di sicurezza, non solo di McAfee ma di migliaia di sviluppatori, che si integrano nella nostra piattaforma di gestione estendibile. A tutt'oggi oltre 150 partner tecnologici sono entrati a far parte dell'alleanza: imprese grandi e piccole, tutte impegnate nell'innovazione continua per la sicurezza. I loro strumenti possono inserirsi facilmente anche nella struttura Security Connected. La Security Innovation Alliance permette di sfruttare gli investimenti già compiuti, raggruppare gli strumenti strategici e potenziarli dove necessario.

I clienti ne hanno compreso il valore

Dal nostro punto di vista, il valore non sta solo nell'aumento della sicurezza e nella riduzione dei rischi. Il valore che apportiamo è doppio, perché la maggior sicurezza *si combina* con la riduzione dei costi operativi. Possiamo affermarlo per aver studiato i clienti che hanno implementato le nostre piattaforme integrate. Il risultato è che i clienti vedono e comprendono l'effetto a valle di Security Connected in modo più grande e più ampio. Ecco qualche esempio dei risultati:

- una grande città del nord-est degli Stati Uniti ha risparmiato 18 milioni di dollari in cinque anni in seguito alla standardizzazione con McAfee;
- un importante produttore di beni di consumo ha ridotto il numero di fornitori di sicurezza da tre a uno. L'azienda ha inoltre ridotto del 75% il numero di console di gestione della sicurezza e di server e ha risparmiato oltre 1 milione di dollari in tre anni relativamente a helpdesk, gestione degli eventi di sicurezza e costi delle patch;
- una grande organizzazione sanitaria ha dimezzato la spesa in sicurezza passando a McAfee. Ha ridotto la complessità dei processi di gestione dei fornitori, con un risparmio di 3 milioni di dollari relativo ai costi per hardware, licenze software, verifiche e conformità;
- un governo statale degli Stati Uniti ha standardizzato la propria struttura di sicurezza con McAfee, prevedendo un risparmio compreso fra i 5 e gli 8 milioni di dollari in tre anni.

Un'unione vincente

In un articolo del *Federal Times* sui tagli al bilancio, VanRoekel ha sottolineato: "Ritengo che la pressione fiscale abbia come effetto un'ondata di innovazione e di efficienza che non avrebbe luogo con l'espansione del bilancio". Security Connected fa proprio questo: offre un approccio innovativo alla sicurezza che produce importanti aumenti dell'efficienza.

Con la piattaforma Security Connected si ottiene:

- protezione ottimizzata a un costo ragionevole;
- un approccio integrato alla mitigazione delle minacce che interconnette prodotti, servizi e partnership;
- convenienti soluzioni COTS che nel tuo ambiente – grande o piccolo che sia – funzionano molto meglio delle GOTS;
- un fornitore leader del settore, con una serie completa di strumenti di sicurezza straordinari;
- la semplicità di una singola piattaforma di soluzioni che lavorano insieme e si integrano l'una con l'altra;
- McAfee GTI, che aggiunge all'intera struttura le preziose informazioni sulle minacce;
- una serie di prodotti aggiuntivi e integrati nella piattaforma Security Connected tramite la Security Innovation Alliance, che producono interoperabilità, apertura ed efficienza operativa;
- risparmi economici comprovati.

Approfittando di una struttura integrata come Security Connected e usando le tecnologie COTS anziché GOTS si raggiungono degli importanti risultati in termini di efficienza. È possibile avere una sicurezza informatica completa che fornisce visibilità in tempo reale e protezione a un costo ragionevole. Il metodo di protezione COTS, ben integrato, è in grado di soddisfare tutte le esigenze di un'agenzia governativa, ottimizzandone la condizione di sicurezza, riducendone le spese, semplificandone le operazioni e andando incontro ai requisiti governativi di sicurezza informatica. Questo è ciò che chiamiamo una buona proposta di valore.

Ulteriori informazioni

Per maggiori informazioni su Security Connected visitare il sito www.mcafee.com/it/enterprise/security-connected/index.aspx. Per maggiori informazioni sul settore pubblico visitare il sito www.mcafee.com/it/industry/public-sector/index.aspx.

Informazioni su McAfee

McAfee è ora parte di Intel Security. Con la propria strategia Security Connected, l'approccio innovativo alla sicurezza potenziata dall'hardware e l'ineguagliato servizio Global Threat Intelligence, Intel Security è impegnata senza sosta nello sviluppo di soluzioni e servizi di sicurezza proattiva comprovati che proteggono sistemi, reti e dispositivi portatili per l'utilizzo aziendale e personale a livello mondiale. Intel Security combina l'esperienza e la competenza di McAfee con l'innovazione e le prestazioni comprovate di Intel per rendere la sicurezza un ingrediente essenziale di ogni architettura e di ogni piattaforma di elaborazione. La missione di Intel Security è di assicurare a chiunque la tranquillità di vivere e lavorare in modo sicuro e protetto nel mondo digitale. www.intelsecurity.com.



McAfee. Part of Intel Security.

Via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.intelsecurity.com

1. <http://fedconnects.com/index.php/2013/01/part-one-federal-it-budgets-and-infrastructures-face-challenges-and-a-new-era/>
2. <http://cio.gov/wp-content/uploads/2012/09/FY2013-IT1.pdf>
3. http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800_53_r4_draft_fpd.pdf
4. <http://dailycaller.com/2012/07/24/beleaguered-homeland-security-agency-wastes-57-million-on-failed-computer-contract/>
5. <http://www.va.gov/oig/pubs/VAOIG-12-01903-04.pdf>

Intel e il logo Intel sono marchi registrati di Intel Corporation negli Stati Uniti e/o in altri Paesi. McAfee e il logo McAfee sono marchi registrati o marchi di McAfee, Inc. o sue filiali negli Stati Uniti e in altri Paesi. Altri marchi e denominazioni potrebbero essere rivendicati come proprietà di terzi. I piani, le specifiche e le descrizioni dei prodotti contenuti nel presente documento hanno unicamente scopo informativo, sono soggetti a variazioni senza preavviso e sono forniti senza alcun tipo di garanzia, esplicita o implicita. Copyright © 2013 McAfee, Inc. 60183wp_sec-conn-value_0413B_fnl