Cloud Antispam Forcepoint

Sommario

1. Introduzione

Forcepoint (Ex Websense), è leader globale nelle tecnologie integrate per la protezione di Web, posta elettronica e dati, offre soluzioni di sicurezza integrate a oltre 42 milioni di dipendenti di più di 50.000 aziende in tutto il mondo, di cui più di 2.300 sono italiane.

Il software e le soluzioni di sicurezza 'hosted' di Forcepoint, distribuiti attraverso una rete globale di partner di canale, aiutano le aziende a bloccare i codici maligni, prevenire la perdita di informazioni confidenziali e attuare policy di sicurezza sull'utilizzo di Internet.

Le soluzioni Forcepoint migliorano la produttività dei dipendenti e proteggono le aziende dalle minacce alla sicurezza veicolate tramite Web e posta elettronica, fornendo un componente importante e complementare alle soluzioni di protezione tradizionali. Forcepoint è l'unico fornitore in grado di offrire applicazione flessibile e integrata delle policy a livello di gateway Internet, all'interno della rete e a livello di endpoint.

Le soluzioni di Forcepoint sono utilizzate in comparti quali sanitario, finanziario, bancario, assicurativo, nella pubblica amministrazione, nel manifatturiero, nel settore legale, tecnologico, nella distribuzione, nei servizi e nell'istruzione.

Alla luce della crescente convergenza delle minacce nei confronti del Web e della posta elettronica, oggi è più importante che mai poter contare su una strategia omogenea e unificata per prevenire ogni pericolo. Grazie alla suite di prodotti Forcepoint e alle tecnologie sofisticate su cui si basano, è possibile usufruire di una protezione più efficace nei confronti delle minacce Internet ed e-mail.

2. Descrizione della problematica

Il proliferare delle infezioni da virus ransomware necessita di una soluzione rapida, poco invasiva ed affidabile che non consenta al malware di raggiungere gli utenti aziendali. L'unione delle funzionalità dell'architettura cloud antispam di Forcepoint di seguito descritte risultano essere estremamente affidabili contro le numerose varianti di Cryptolocker.

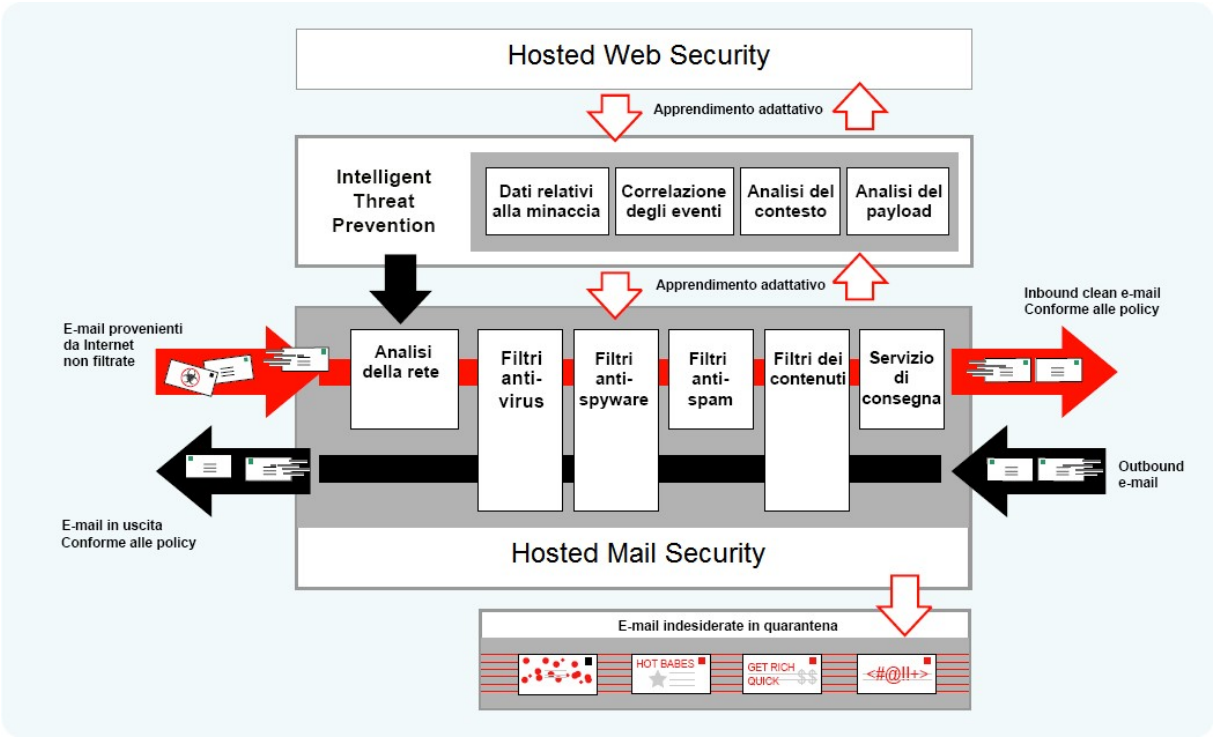
3. Infrastruttura del servizio

La protezione della rete con Forcepoint Hosted eMail security è di semplice implementazione, in quando necessita solamente re-indirizzare gli MX record DNS del dominio di posta verso i Datacenter Forcepoint e **tutte le email saranno ispezionate prima essere inoltrate ai mail server del cliente. Le mail inviate verso l'esterno subiranno lo stesso processo di analisi prima di essere indirizzate ai destinatari**. L'impatto sull'infrastruttura esistente è estremamente contenuto, in quanto non necessita alcuna installazione di apparati hardware o di software: i mail server attualmente operativi resteranno tali, necessiterà solo comunicare a Forcepoint i loro indirizzi IP, in modo che possa essere poi inoltrato il traffico analizzato. La gestione remota delle mailbox e delle politiche applicate verranno gestite tramite interfaccia web con privilegi multi utenza differenziati. I Datacenter di Forcepoint impiegano cluster di macchine ridondanti e load-balanced ad alta disponibilità collocate presso undici sedi nel mondo. Tutti i centri dati Forcepoint sono stati certificati ISO27001 per garantire il massimo grado di sicurezza globale e localizzata, privacy e

riservatezza delle informazioni. Un elevato SLA ed un tempo di latenza dei messaggi i posta certificato come inferiore al minuto, è componente standard del servizio.

In caso di disservizio temporaneo dei mailserver del cliente Forcepoint garantisce il mantenimento dei messaggi in arrivo per un periodo di 7 giorni.

Il portale per la gestione online in tempo reale rende ancor più lineare la definizione e l'applicazione delle policy di sicurezza. Potenti tool per la gestione della quarantena e l'assistenza self-service destinati agli utenti finali, contribuiscono ad alleviare il carico di lavoro degli amministratori IT, mentre le statistiche e il reporting dei messaggi on-demand, consentono di esercitare il pieno controllo sul sistema facilitando la comprensione sulla situazione in atto nella rete.



La soluzione on-demand per la sicurezza della posta elettronica di Forcepoint è parte di una suite integrata di servizi web e mail che, fornendo alla posta elettronica una protezione completa da virus, spam e altri contenuti indesiderati, garantisce la sicurezza delle comunicazioni e-mail all'interno dell'azienda. Grazie alle sofisticate tecnologie euristiche utilizzate, integrate da team di esperti nell'analisi delle minacce con oltre 100 anni complessivi di esperienza nel settore della sicurezza, le minacce e-mail vengono analizzate tempestivamente e le difese vengono aggiornate immediatamente.

Il Forcepoint ThreatSeeker: HoneyGrid Computing

Prima di entrare nel merito della soluzione è bene fare chiarezza su tutti quei processi proprietari che fanno di Forcepoint una tecnologia unica e al passo con i nuovi sviluppi del web; ThreatSeeker è l'insieme di processi e risorse alla base di tutte le soluzioni Forcepoint, un approccio capace di dare una visibilità praticamente real time delle continue evoluzioni del web. La HoneyGrid è invece una rete distribuita capace di collezionare una mole impressionante di informazioni a riguardo non solo di URL, ma anche di protocolli, email, dati e contenuti di applicazioni.

L'elaborazione delle informazioni raccolte è distribuito sui diversi nodi della "grid" così che sia possibile analizzare e processare una mole tanto impressionante di dati. Il grande valore aggiunto è nella visibilità mondiale su qualsiasi nuova minaccia, questa viene interpretata e categorizzata in modo da essere riconosciuta e debellata con un approccio proattivo di filtro.

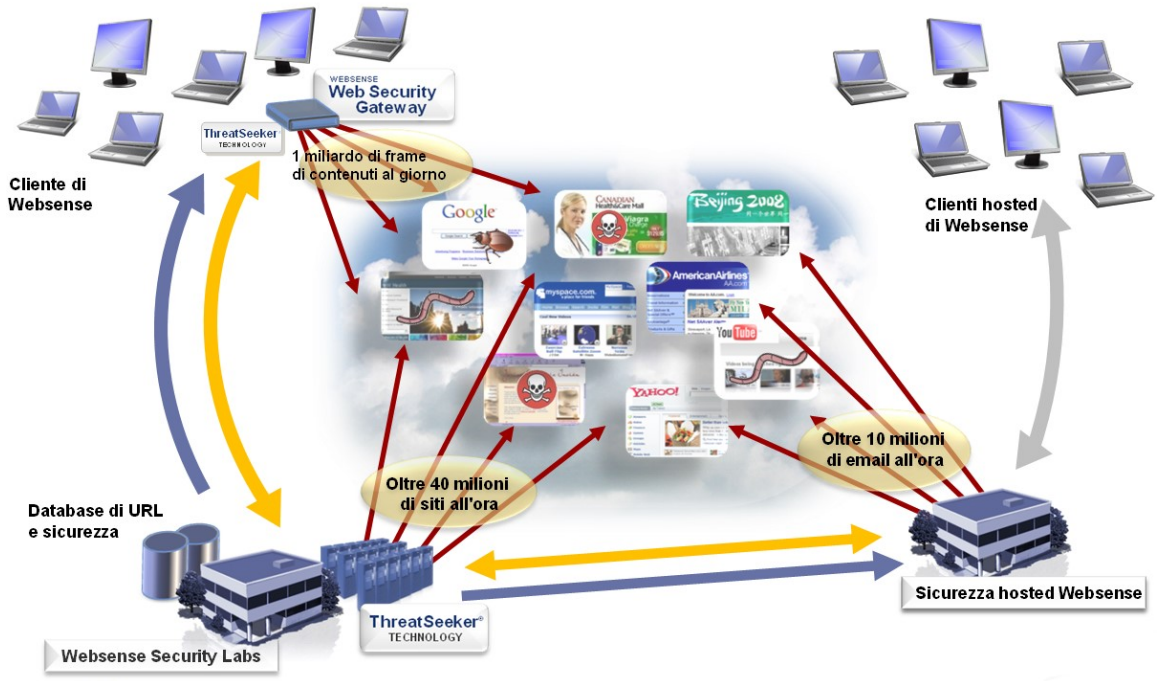


Figura: Forcepoint ThreatSeker Network

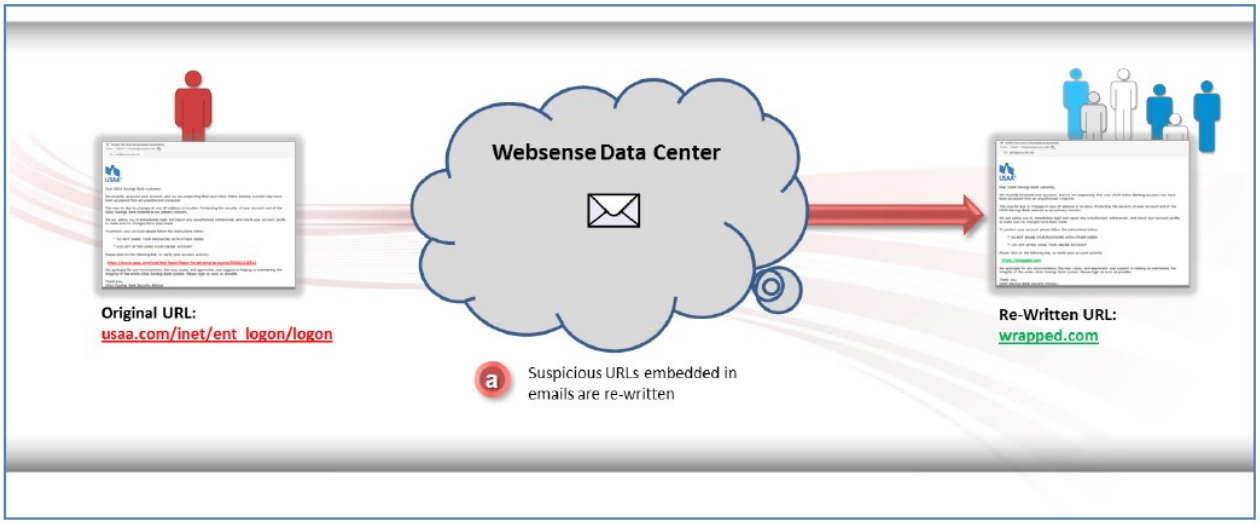
4. URL-Sandbox

Molti attacchi di nuova generazione utilizzano Email forgiate con link che puntano a botnet dinamiche, siti a good reputation o semplicemente sospetti che richiedono un'analisi puntuale degli accessi. Ad esempio una email inviata a Mezzanotte potrebbe contenere un link lecito che riporta ad una pagina che non contiene elementi compromessi, nulla però vieta di sostituire questo contenuto con uno compromesso dopo qualche ora dall'invio del messaggio.

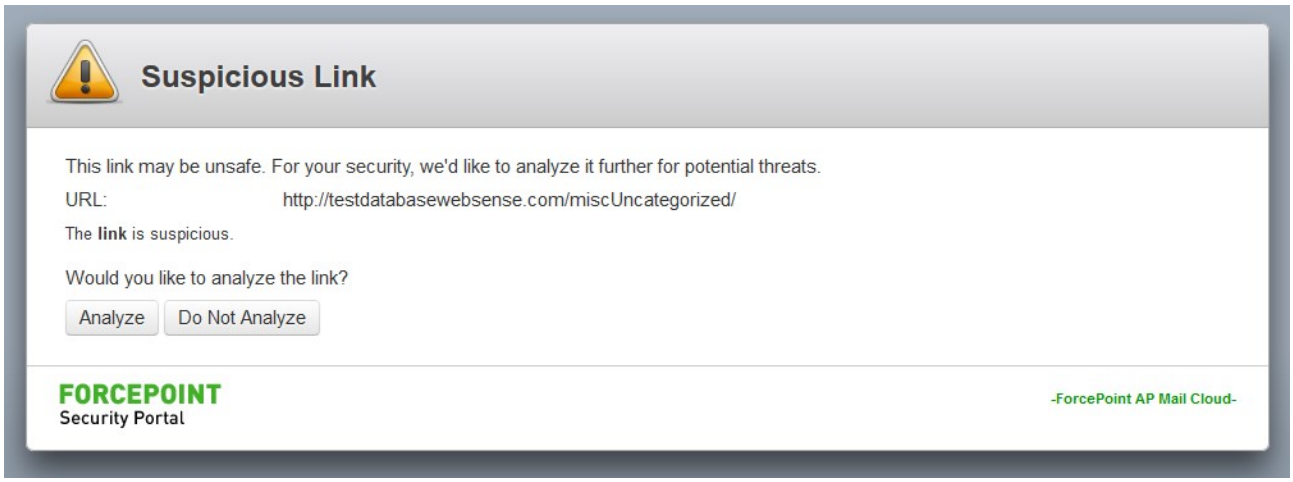
Per venire incontro a questa esigenza di sicurezza il modulo AP-SANDBOX per AP-MAIL implementa una funzionalità di URL Sandboxing in grado di difendere l'utente da questo tipo di attacchi in Real- Time, anche per chi non ha una soluzione di protezione Web o per quegli accessi che avvengono all'esterno della rete aziendale quali Webmail, Dispositivi mobili o portatili in mobilità che non dispongono di alcuna protezione.

Di seguito un breve esempio di tale funzionalità:

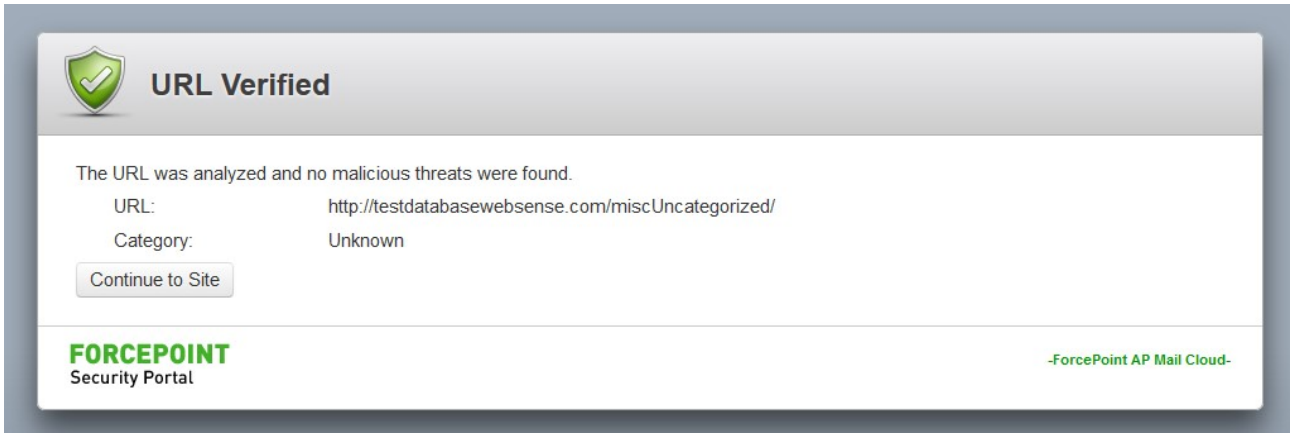
L'URL all'interno della mail viene riscritto. Tutte le email che attraversano il Data Center Forcepoint vengono analizzate alla ricerca di rischi di sicurezza. Se non vi sono elementi compromessi il messaggio viene consegnato all'utente. Tuttavia, nel caso si riscontri un URL sospetto, lo stesso viene sostituito con uno generato dal sistema e che ridireziona la navigazione sul Cloud Forcepoint, in modo trasparente, per consentirne l'analisi ad ogni click.



Real-Time Analysis. Quando l'utente clicca sull'URL viene rediretto verso il sandbox Forcepoint che consente di fruire del contenuto attraverso un filtro, come se si guardasse attraverso un vetro di protezione. Forcepoint analizza il sito e lo consente solo nel caso in cui sia sicuro. Questo controllo viene effettuato ad ogni click dell'utente, da qualsiasi dispositivo si connetta.



Security Enforcement. Se le scansioni rilevano un accesso ad un sito compromesso l'utente viene protetto ed avvisato tramite una pagina di cortesia.

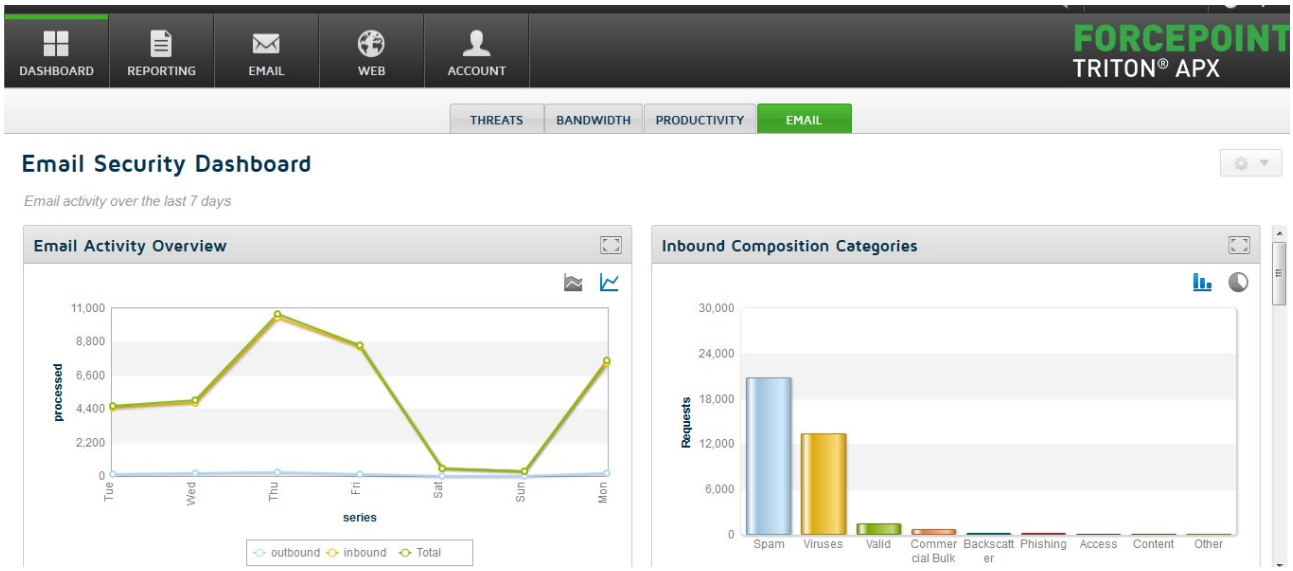


5. Analisi e Ricerca

Forcepoint vanta un centro di ricerca specializzato sul Web, i **SecurityLabs**, con sedi e ricercatori in tutto il mondo. Al di là degli automatismi, indispensabili per la gestione di un volume di dati impressionante, esiste sempre un uomo capace di discernere il falso positivo dal reale attacco, un professionista capace di supervisionare i processi di categorizzazione e di analisi per affinare sempre al meglio la categorizzazione e l'analisi dei dati forniti dalla HoneyGrid.

6. L'interfaccia

Una reportistica avanzata ed una GUI di amministrazione intuitiva costituiscono un interfaccia semplice ed efficace per ottimizzare il filtraggio e la sicurezza sulla rete.



In figura la GUI di Hosted Email Security: il portale di configurazione ed accesso alla reportistica è unico, presentato in https all'amministratore del servizio. Il portale è di semplice utilizzo e studiato per essere facilmente gestibile, pochi click sono infatti sufficienti per effettuare tutte le operazioni.
Il portale è accedibile da qualsiasi computer ed è attivo 24 ore su 24, con un uptime garantito del 99,999%.

7. Caratteristiche e SLA di servizio

Parametro	
Numero centri di servizio	10, di cui 6 in Europa
Certificazione centri di servizio ISO 27001	SI per tutti i datacenter
Numero di tecnologie antivirus	1 Motore proprietario

	+ 2 Motori commerciali + Motore dinamico proprietario ThreatSeeker
Numero di tecnologie ANTISPAM	1 Motore Euristico Proprietario 1 Motore basato su Dizionari tematici + Motore dinamico proprietario ThreatSeeker
SLA – Tempo di latenza messaggio	Mail di 2 MB / 60 secondi
SLA – Protezione minacce virali note	= 100,00% su virus noti
SLA – Eliminazione SPAM	> 99%
SLA - Uptime	= 99,999%
Numero caselle gestite mondiale	> 10.000.000
Controllo e gestione prodotto	Portale accessibile dal cliente H24, le regole vengono aggiornate in real-time in tutti i datacenter
Tempo di attesa rilascio email	Immediato, sia da parte da parte dell'utente che dell'amministration
Statistiche	Si, disponibili H24
Reporting	Si, disponibile H24
Servizi aggiuntivi – mantenimento messaggi non consegnabili all'utente	144 ore

8. Integrazione antispam Forcepoint con Google e Office 365

Forcepoint è partner tecnologico di Google e Microsoft e consente di effettuare con una semplice configurazione l'integrazione del servizio cloud antispam con i servizi cloud email dei due conosciuti fornitori di servizi.
Qui http://www.websense.com/content/support/library/email/hosted/admin_guide/configure_route.aspx è riportata la modalità di attivazione dell'integrazione.

9. I vantaggi di una tecnologia anti-spam in-the-cloud

I vantaggi di una soluzione hosted sono molteplici, primo su tutti l'enorme risparmio di risorse in termini di banda, numero di macchine, corrente e risorse umane che ricevere e gestire oltre il 90% di email-spazzatura comporta. A questo aggiungiamo una quarantena esternalizzata che lascia codici virali e spam fuori dal perimetro aziendale.
La soluzione Forcepoint è inoltre ridondata a livello Geografico, il che, unito alla capacità di conservare le email non consegnate al server del cliente fino a sette giorni, consente di garantire la massima disponibilità del servizio senza costi imprevisti per una funzionalità che diventa ogni giorno di più un problema da gestire.

L'attivazione del servizio cloud antispam consentirà:

- una netta riduzione dei costi di gestione della piattaforma antispam, in quanto non necessita gestire le singole mailbox
- un comprovato aumento dell'affidabilità dei filtri che porta all'eliminazione dello spam e dei falsi positivi altrettanto dannosi
- un netto risparmio della banda internet grazie al filtraggio effettuato a monte dell'infrastruttura aziendale
- la possibilità di gestire, con politiche definibili ad utente, l'invio di un avviso via mail in caso di messaggi presenti in quarantena, lasciando al singolo la gestione dell'azione da intraprendere
- l'attivazione del filtraggio antispam anche sui messaggi in uscita, utile nel caso di presenza di worm sulla rete aziendale che si diffondono via mail
- il vantaggio di non avere più pubblicati a livello DNS gli IP del mail server, con la conseguente eliminazione del rischio di inserimento in mail relay gray o black list
- in caso di disservizio temporaneo del mail server o della connettività, il servizio cloud garantisce il mantenimento dei messaggi in arrivo per un periodo di 7 giorni
- l'attivazione del servizio di cloud antispam non comporta nessun tipo di impatto sulle attuali funzionalità della posta elettronica e non necessitano riconfigurazioni se non del server Domino