

Tutti i vantaggi di un modello di sicurezza Hosted

Un White Paper di Osterman Research

Data pubblicazione: Luglio 2009

COMMISSIONATO DA

websense[®]



Osterman Research, Inc. • P.O. Box 1058 • Black Diamond, Washington 98010-1058
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com • www.ostermanresearch.com

In breve

La sicurezza è senza dubbio un aspetto critico per le infrastrutture di e-mail o Web in ogni azienda. I crescenti volumi di spam, virus, worm, Trojan, minacce composite e pericoli vari, in aggiunta agli attacchi più sofisticati ad opera di spammer e altri, hanno reso indispensabile per le aziende l'utilizzo di sistemi di difesa efficaci e flessibili, in grado di proteggere reti, utenti e dati da una ampia gamma di vulnerabilità. Per esempio, lo spam costituisce il 90% di tutto il traffico e-mail, e circa una e-mail su 100 contiene un virus. Tuttavia, poiché l'utilizzo di e-mail aumenta del 20% circa ogni anno, anche i volumi di spam, virus e altro malware stanno crescendo in modo spropositato, il che costringe le aziende a mettere a punto una infrastruttura di sicurezza per i sistemi di messaggistica in risposta a questa tendenza.

Inoltre, abbiamo assistito ad un forte aumento di contenuti dannosi provenienti dal web, come e-mail che nascondono link a siti web pericolosi, allegati che attivano il primo livello di download di altro codice dannoso dal web, malware che si installa e apre un canale di comunicazione con la fonte dell'attacco, e altri pericoli. Normalmente, questi siti di malware raggiungono il loro scopo, creando ulteriori bot zombie che mantengono attivo il circolo vizioso di spam e virus.

Tuttavia, la gestione interna delle funzionalità di sicurezza e-mail e web è costosa e richiede tempo. Le aziende devono predisporre investimenti consistenti in hardware, software, training, manutenzione dei contratti, ecc. per costruire e gestire i loro sistemi di difesa. Inoltre, l'industria del malware è molto redditizia, questo fornisce agli autori di spam, phishing e altro le risorse di cui hanno bisogno per sviluppare attacchi ancora più sofisticati e su scala più ampia. Le organizzazioni che non affrontano in modo adeguato i problemi di sicurezza dei sistemi di messaggistica vanno incontro a conseguenze di natura legale, rischi economici, possibili inadempienze a normative e leggi e altro ancora.

Le organizzazioni che non affrontano in modo adeguato i problemi di sicurezza dei sistemi di messaggistica vanno incontro a conseguenze di natura legale, rischi economici, possibilità di inadempienze a normative e leggi, e altro ancora.

Questo white paper, commissionato da Websense, vuole fornire un quadro delle risposte che le organizzazioni, oggi, danno al nuovo incremento di minacce e alle nuove tipologie, diffuse via e-mail. L'intento della ricerca è di calcolare i reali costi di implementazione di una infrastruttura di sicurezza dei sistemi di messaggistica gestita internamente piuttosto che utilizzare un modello di implementazione esternalizzata, di tipo hosted. L'obiettivo è definire le attuali differenze di costo tra i modelli di implementazione in aziende di varie dimensioni e tipologie di rete, oltre a fornire dati reali ed esempi attendibili.

Background e metodologia

Websense ha commissionato a Osterman Research la realizzazione di una indagine su scala mondiale che riguarda i responsabili delle scelte dei sistemi di messaggistica, con l'obiettivo di definire i costi di gestione dei sistemi di sicurezza e-mail, la loro percezione

dell'efficacia dell'infrastruttura interna di cui sono dotati, e altre questioni. Complessivamente sono stati compilati 818 questionari da piccole, medie e grandi imprese ubicate in Nord America e nelle regioni EMEA (Europe/Middle East/Africa) e APAC (Asia/Pacific). Ecco alcuni dettagli sul sondaggio:

- Il sondaggio on-line è stato realizzato tra i mesi di Febbraio e Marzo 2008
- Sono stati compilati 364 questionari in America settentrionale, 239 in EMEA e 215 in APAC.
- Il numero medio di dipendenti delle aziende oggetto del questionario è 1.500.
- Il numero medio di utenti e-mail delle aziende oggetto del questionario è 1.275.
- Tutte le persone intervistate sono ben informate sull'infrastruttura a protezione dei sistemi di messaggistica della loro azienda.

Risultati principali del sondaggio

Il seguente sondaggio, realizzato in esclusiva per questo white paper, fornisce alcuni interessanti approfondimenti sul modo in cui la sicurezza dei sistemi di messaggistica è gestita presso aziende di tutto il mondo. Questi risultati indicano i costi derivanti dalla gestione di una soluzione di sicurezza interna; si parlerà più avanti di sicurezza dei sistemi di messaggistica esternalizzata, di tipo hosted.

- **I costi di una infrastruttura interna sono notevoli.**

I numeri medi di utenti supportati da server anti-virus e anti-spam sono, rispettivamente, 250 e 260. Se supponiamo, senza esagerare, un costo complessivo di hardware e di software di sicurezza di 3.500 €, il solo costo del server sarà di circa 14 € a utente, o sotto i 5 € a utente per il normale periodo di vita di 3 anni di un qualsiasi sistema di messaggistica. Le appliance anti-virus e anti-spam supportano pochi utenti in più: i valori medi sono rispettivamente 273 e 338. Ipotizzando un'appliance da 2.900 € a supporto di questo numero medio di utenti, il costo a utente sarà all'incirca di 10 €, o intorno a 3,5 € all'anno per utente.

Il costo approssimativo per gestire internamente la sicurezza dei sistemi di messaggistica va approssimativamente da 97 € a 98 € per utente all'anno, o più di 8 € per utente al mese.

Tuttavia, è importante notare che il crescente volume di spam, minacce web e malware renderà indispensabile l'implementazione da parte delle aziende di hardware aggiuntivo, nei successivi tre anni di vita della maggior parte degli elementi dell'infrastruttura di messaggistica, quasi raddoppiando i valori di cui sopra.

- **I costi di manodopera IT per la gestione della sicurezza sono considerevoli.**

Il numero medio di utenti e-mail a cui ogni dipendente di uno staff IT dedicato alla sicurezza può fornire supporto è 875. Se ipotizziamo che la retribuzione annuale

complessiva (stipendio, ferie, benefit, ecc.) per ogni dipendente di uno staff IT è di circa 64.000 €, questo corrisponde ad un costo annuo per gli interventi IT di 73 € per utente e-mail.

La manodopera per la gestione di una infrastruttura di sicurezza implica varie mansioni, tra cui l'implementazione di hardware/appliance, software o soluzioni; l'assicurarsi che tutto funzioni correttamente virtualmente per il 100% del tempo; la pianificazione della capacità, per assicurare che l'infrastruttura non venga sommersa da picchi di spam; e altre attività aggiuntive.

Fatto molto interessante, la nostra ricerca ha trovato rapporti con valori di poco superiori di utenti per dipendenti IT in America settentrionale piuttosto che in EMEA o APAC, giustificabile attraverso la maggiore maturità del mercato nord-americano, come risultato di maggior esperienza nell'uso di sistemi di sicurezza per la messaggistica e manodopera IT più efficiente.

- **Anche le spese collaterali sono elevate**

Le organizzazioni investono cifre significative in spese collaterali alla manodopera dedicata alle infrastrutture di sicurezza per i sistemi di messaggistica. Per esempio, le aziende nordamericane spendono una media di circa 20 € ogni anno per utente in contratti di manutenzione, aggiornamenti software, nuovo hardware, ecc. Le aziende dell'area EMEA spendono poco più di 20 € per utente e quelle APAC intorno a 13,5 € per utente.

Basandoci sui costi riportati sopra, e supponendo un ciclo di vita di 3 anni per l'infrastruttura di sicurezza dedicata ai sistemi di messaggistica, il costo approssimativo della gestione interna va da 97 a 98 € annui per utente, o più di 7,8 € mensili per utente.

- **I dipendenti IT richiedono una quantità rilevante di training.**

I requisiti di training IT sono considerevoli, richiedono inizialmente una media di 30 ore per persona, seguita da una media di 20 ore annue. Su un periodo di tre anni, considerando una retribuzione complessiva di 64.000 €, questo si traduce in un costo di 2.200 € a dipendente IT e circa due settimane di training per imparare ed essere aggiornati sulle funzionalità di sicurezza per i sistemi di messaggistica.

- **L'ampiezza di banda ha un impatto significativo sul traffico dei sistemi di messaggistica.**

Il valore medio di ampiezza di banda disponibile nelle imprese considerate è di 592 Mbit al secondo, sebbene l'ampiezza di banda sia maggiore nelle aziende dell'America settentrionale (734 Mbit al secondo), seguita dalle regioni EMEA (534 Mbit al secondo) e APAC (427 Mbit al secondo). Fatto che non sorprende, il traffico SMTP occupa una parte consistente della banda disponibile, circa il 29% del totale.

Questo genera forti conseguenze sul Total Cost of Ownership (TCO) della sicurezza dei sistemi di messaggistica gestita internamente: dato che i volumi di spam e di malware sono in crescita, una percentuale maggiore di banda sarà occupata da contenuto indesiderato, il che costringerà le aziende a mettere a disposizione banda supplementare. Inoltre, i picchi di spam possono intasare la banda, causando addirittura la caduta della rete, in alcuni casi.

- **La fiducia nella sicurezza dei sistemi di messaggistica gestita internamente non è elevata**

Molte organizzazioni non hanno una fiducia elevata nelle potenzialità dei loro sistemi anti-spam e anti-virus. Per esempio, il 73% delle organizzazioni ha dichiarato di essere fiducioso o molto fiducioso nella capacità della loro infrastruttura anti-virus di fermare in modo efficace tutti i virus, i worm, i Trojan e le altre minacce; solo il 61% di queste ha fiducia nella capacità della propria infrastruttura anti-spam di bloccare tutti contenuti indesiderati. Ciò significa che una parte considerevole di aziende non ha fiducia nelle difese dei sistemi di messaggistica in loro dotazione.

Questi dati sottolineano una rilevante vulnerabilità percepita e reale ad un'ampia varietà di minacce, e indicano che le organizzazioni non sono protette così efficacemente come ne avrebbero bisogno.

- **A proposito di soluzioni hosted**

La maggior parte delle organizzazioni non ha ancora considerato di migrare verso una soluzione di sicurezza e-mail gestita esternamente. Molte organizzazioni spesso sottovalutano il costo di gestione dell'infrastruttura di cui sono dotati, e così ritengono che sia anche meno costosa la gestione interna della sicurezza dei sistemi di messaggistica; oppure non colgono l'elevato livello di sicurezza ottenibile dai provider di servizi hosted rispetto ad una gestione interna.

Detto ciò, Osterman Research ha trovato che i decision maker sono sempre più orientati all'idea di esternalizzare le applicazioni critiche, come la sicurezza dei sistemi di messaggistica.

Molte organizzazioni non hanno un livello di fiducia elevato nell'affidabilità dei loro sistemi anti-virus e anti-spam.

E, detto ciò, la maggior parte dei decision maker crede che le offerte di sicurezza dei sistemi di messaggistica affidata a terzi in hosting siano in grado di fornire numerosi vantaggi, tra cui i costi ridotti di attività in ambito IT e di intervento per gli upgrade, i miglioramenti nelle quantità di spam, virus e altre minacce intercettate, e una maggiore flessibilità per l'azienda.

- **Consolidare un unico vendor è percepito come vantaggioso.**

Circa un decision maker di azienda su due ritiene di poter considerare, se non di aver quasi deciso, di consolidare la sicurezza di rete, la sicurezza dei dati, la sicurezza e-mail e le funzionalità connesse su un unico vendor. È interessante notare che solo una organizzazione su sei ritiene che un consolidamento di questo tipo non sia in grado di recare alcun valore.

I vantaggi di un modello di sicurezza di tipo hosted

La sicurezza e-mail e web di tipo hosted può offrire molteplici vantaggi per organizzazioni di tutte le dimensioni, come costi di proprietà inferiori rispetto alle soluzioni interne, gestione più semplice delle funzionalità di sicurezza, e il più alto livello possibile di protezione dalle minacce.

TCO ridotto

Molti decision maker ritengono che la gestione interna della sicurezza e-mail e Web sia meno costosa dei servizi di tipo hosted in grado di fornire analoghe funzionalità. Anche se per le grandi aziende (con più di 1.500 dipendenti) questa percezione può essere attendibile, molto spesso non è così. Per esempio, molti decision maker spesso non considerano il costo complessivo di dare in dotazione e-mail, sicurezza e altre funzionalità ai loro dipendenti. Spesso sottovalutano il volume totale di attività richiesta per gestire il sistema, la natura dirompente delle interruzioni di energia elettrica e altri imprevisti in altre attività IT, le spese per investimenti necessari, i costi non previsti della gestione interna del sistema, il fabbisogno di energia e di raffreddamento necessario a gestire l'hardware interno, e così via.

Inoltre, la maggior parte dei decision maker semplicemente non conosce quanto costi davvero fornire e-mail e altri servizi. Per esempio, in una indagine di Osterman Research del 2007, è stato chiesto ai decision maker di competenza in che modo tengano traccia dei costi dei servizi di messaggistica forniti ai loro utenti. Il sondaggio ha rilevato che l'8% degli intervistati sapeva esattamente quali fossero questi costi, mentre un altro 25% era in grado di stimarli a più o meno il 10% del costo effettivo. Questo significa che i due terzi di questi decision maker non conoscono il vero costo connesso all'erogazione di servizi di messaggistica nella loro organizzazione.

Poiché molti decision maker sottovalutano il completo impatto del costo di gestione di una infrastruttura interna, e dal momento che la maggior parte non è in grado di calcolare con accuratezza il costo di implementazione e di gestione, molti non si rendono conto che spesso è meno costoso esternalizzare le attività di sicurezza di e-mail ad un provider di terze parti. Questo è giusto per i costi fissi – quelli per i quali l'azienda incorrerà in una spesa diretta – così come per i costi di opportunità. Riguardo quest'ultimo, poiché un provider di servizi di tipo hosted può liberare lo staff IT per svolgere altri lavori, il ricorso a un servizio esternalizzato può permettere allo staff IT di generare molto più valore per la propria organizzazione contribuendo al business, rispetto ai casi in cui l'infrastruttura di sicurezza e-mail è gestita internamente.

RIDURRE LA COMPLESSITÀ E L'INCERTEZZA

La protezione dei sistemi di e-mail è complessa e lo diventa sempre più. Nuove minacce, unite al crescente volume di queste minacce e ai picchi di traffico malware possono creare numerosi problemi. Per le organizzazioni che utilizzano la loro infrastruttura di sicurezza, il risultato può essere una saturazione delle funzionalità interne o il malfunzionamento dei sistemi stessi che può tradursi in prestazioni ridotte o in un totale crollo della rete. Per esempio, l'enorme crescita di volume di spam tra maggio e novembre 2006 causata dalle reti bot e dall'uso di spam con immagini causò in molte soluzioni interne il raggiungimento del massimo della loro capacità. In molte organizzazioni, lo staff IT dovette trovare un rimedio aggiungendo nuovi server o appliance e arginare i problemi causati dall'imprevista esplosione di spam.

Una soluzione di tipo hosted, d'altro canto, può ridurre fortemente la complessità e l'insicurezza associata alle nuove minacce o alla crescita dei volumi di spam, spyware, ecc. Poiché i provider di servizi di tipo hosted sono in grado di fare fronte a questi problemi e sono provvisti di funzionalità più adatte rispetto a quelle che la maggior parte delle aziende può implementare internamente, i loro clienti sono al riparo dalla crescente catena di pericoli a cui i loro sistemi sono a rischio.

FORNIRE IL MASSIMO LIVELLO DI PROTEZIONE

I provider di sicurezza di tipo hosted aggiornano i loro servizi praticamente in tempo reale. Per esempio, un provider di servizi di filtraggio anti-virus e anti-spam normalmente aggiorna i suoi servizi continuamente; spesso, infatti, hanno accesso alle più aggiornate banche dati di minacce ancora prima che si propaghino al pubblico, e hanno accesso alle informazioni sui nuovi pericoli appena si diffondono. Inoltre, i provider di servizi di tipo hosted normalmente implementano una gamma più ampia di tecnologie di protezione dalle minacce e offrono una competenza ai loro clienti non altrimenti disponibile o fuori dalla loro portata, soprattutto nel caso delle realtà più piccole.

Inoltre, i principali provider di servizi di tipo hosted utilizzano sistemi di scansione anti-virus, filtraggio URL per intercettare gli attacchi di phishing, sistemi di rilevamento della reputazione per determinare se un indirizzo IP possa essere considerato una fonte di contenuto sospetto o attendibile, e sono in grado di analizzare porzioni di traffico complessivo in tempo reale. Si tratta di caratteristiche che la maggior parte delle organizzazioni – specialmente le più piccole – non può permettersi di implementare e gestire internamente.

La maggior parte dei decision maker non è a conoscenza del costo effettivo di servizi come l'e-mail o simili. Osterman Research ha rilevato che i due terzi dei decision maker non conoscono il vero costo dei servizi di messaggistica forniti all'interno della loro organizzazione.

Così, i provider di servizi di tipo hosted sono normalmente in grado di investire nella propria infrastruttura maggiori risorse rispetto a quanto una singola organizzazione possa permettersi, e fornire in questo modo affidabilità di livello ampiamente superiore. Considerando che la maggior parte di questi provider è dotata di data center molto solidi, normalmente è in grado di offrire alti livelli di affidabilità e di SLA (Service Level Agreement) difficilmente paragonabili a quelli dei sistemi gestiti internamente. Questo permette ai clienti di focalizzarsi sui servizi che offrono maggior valore alla loro organizzazione, con la certezza che i sistemi di messaggistica saranno disponibili nella quasi totalità delle occasioni. È anche importante notare che i data center dei provider di servizi di tipo hosted sono presidiati 24x7 e che le funzionalità sono monitorate continuamente, con SLA inerenti la disponibilità così come per i livelli di sicurezza. Ciò significa che i problemi possono essere affrontati con una maggiore rapidità di quanto sarebbe possibile alla maggior parte delle organizzazioni, le quali provvedono internamente alla loro sicurezza.

Per il 2009, Osterman Research prevede che le aziende pianificheranno di implementare una percentuale maggiore dei loro sistemi di messaggistica utilizzando servizi di tipo hosted, come mostra la seguente tabella. Mentre la tendenza a esternalizzare alcuni servizi subirà variazioni minime o nulle, la sicurezza dei sistemi di messaggistica sarà protagonista di una crescita sostanziale nei prossimi anni.

Percentuale delle organizzazioni che Utilizzeranno una Soluzione di tipo Hosted o di tipo Managed.

Sistema di Messaggistica	2007	2008	2009
Anti-virus e anti-spam	22%	29%	32%
Servizi e-mail di tipo Hosted e Managed	13%	14%	19%
Ricezione e archiviazione di e-mail	14%	24%	31%
Servizi wireless/mobility	21%	21%	27%

ALTRI VANTAGGI DI UN MODELLO HOSTED

La sicurezza di tipo hosted per Web e e-mail offre altri vantaggi, come:

- L'ampiezza di banda della rete interna richiesta utilizzando un provider di servizi hosted può essere notevolmente inferiore rispetto all'uso di una infrastruttura interna, in quanto è distribuito molto meno contenuto lungo la rete interna dopo il filtraggio operato su spam e altro malware. Ciò significa che il potenziamento della banda può essere rimandato, con un risparmio non indifferente.

L'ampiezza di banda della rete interna richiesta utilizzando un provider di servizi di tipo hosted può essere considerevolmente inferiore rispetto all'uso di una infrastruttura interna.

- La maggior parte dei principali provider di servizi di sicurezza di tipo hosted ricorre a strutture di sicurezza fisica come la videosorveglianza, punti di accesso multipli con l'utilizzo di autenticazione a due livelli, strumenti di tracking e di monitoraggio e altri sistemi che proteggono i dati dei loro clienti dai pericoli. È importante rivolgersi a provider in possesso di una certificazione standard di terze parti, come la ISO 272001.
- Il ricorso a un provider di servizi hosted o managed può rendere un cliente meno dipendente da un particolare vendor di tecnologia, riducendo così l'impatto di sistemi legacy su tecnologie o scelte di vendor future.
- I provider di servizi di tipo hosted normalmente hanno molta più resistenza per i sovraccarichi di e-mail di una organizzazione che gestisce la propria infrastruttura e-mail internamente. Questo perché, semplicemente, non è conveniente per le aziende dotarsi di funzionalità adeguate per i casi eccezionali, in modo da rimanere in attività in caso di attacchi spam devastanti e su larga scala, per esempio.

LA SICUREZZA E-MAIL DI TIPO HOSTED È ADATTA SOLO ALLE PMI?

L'opinione comune è che i provider di sicurezza di tipo hosted possano offrire vantaggi economici e tecnici per le piccole imprese che non hanno adeguate risorse interne da dedicare a questo genere di attività; ma, nel caso di grandi aziende, si ritiene che sia più economico ed efficace provvedere in autonomia ai propri sistemi di sicurezza. Tuttavia, Osterman Research ha dimostrato che anche le organizzazioni molto grandi possono ottenere vantaggi economici e tecnici delegando la sicurezza a provider esterni.

I vantaggi di un Modello di Sicurezza Single Source.

Alcuni anni fa, proteggere la rete aziendale da un numero allora modesto di minacce provenienti da autori di virus e worm in cerca di notorietà piuttosto che da una bassa quantità di spam inviato attraverso Internet, era piuttosto semplice. Tuttavia, la crescente tipologia di minacce, il rapido aumento del loro volume e la varietà stessa dei problemi che possono avere conseguenze per le aziende, hanno reso indispensabile l'implementazione di una ampia gamma di precauzioni anche presso le piccole realtà. Si tratta delle stesse funzionalità che proteggono già le organizzazioni da virus, Trojan, spyware, spam di contenuto testuale, spam di foto, pdf, siti web dannosi e numerosi altri problemi.

Esiste un numero crescente di vendor specializzati in servizi progettati per filtrare e porre rimedio ad alcuni di questi problemi. Alcuni vendor invece propongono soluzioni olistiche progettate per un approccio complessivo.

Osterman Research crede che costituisca sempre di più una best practice l'implementazione di soluzioni in grado di far fronte all'intera gamma di minacce e-mail, web o di altro tipo in grado di impattare sulle reti aziendali. Ecco perché:

- L'utilizzo di singole soluzioni da diversi vendor richiede maggiori investimenti di tempo dello staff IT rispetto a una soluzione olistica di un unico vendor che può essere gestita attraverso una interfaccia centralizzata. La gestione di un insieme di singole soluzioni fa lievitare il costo della gestione IT, in alcuni casi considerevolmente.
- Ogni vendor avrà una peculiare gestione degli upgrade e dell'installazione delle patch, con un ulteriore aumento del tempo dello staff IT impiegato per gli aggiornamenti di ogni singola soluzione, senza contare le possibili incompatibilità tra di esse.
- Implementare diverse soluzioni singole da vari vendor può essere, nella maggior parte dei casi, più costoso che implementare una soluzione di un unico vendor con lo stesso numero di funzionalità.
- Gestire relazioni con più vendor è più complicato e dispendioso in termini di tempo per i decision maker del settore IT, per i responsabili acquisti o per l'amministrazione, piuttosto che gestire una relazione con un unico vendor.

Il tempo dedicato dallo staff IT può essere inferiore e i costi generali ridotti, nella maggior parte dei casi, scegliendo un unico vendor per tutte le funzionalità di sicurezza necessarie a proteggere un'organizzazione dalle minacce provenienti dalle e-mail e dal web.

In poche parole, il tempo dei dipendenti può essere diminuito, nella maggior parte dei casi, scegliendo un unico vendor in grado di fornire tutte le funzionalità di sicurezza necessarie a proteggere una organizzazione dalle minacce via e-mail e web.

In breve

La sicurezza di tipo Hosted è ora una soluzione sostenibile per le organizzazioni di tutte le dimensioni ed è sempre più implementata, a garanzia di una sicurezza più efficace e con costi inferiori. Una soluzione di tipo hosted offre numerosi e importanti benefici, non ultimo la possibilità per i clienti di avere a disposizione una infrastruttura progettata per fornire alti livelli di throughput e di protezione dal maggior numero possibile di minacce. D'altro canto, dotarsi di una infrastruttura analoga a quella di un provider di servizi hosted, semplicemente può non essere alla portata della maggior parte delle organizzazioni. Questo è evidenziato dai costi inferiori per molte organizzazioni, come si evince dalla seguente tabella.

**Costi di gestione interna di una infrastruttura di sicurezza dei sistemi di messaggistica su tre anni
(secondo i dati ottenuti nel sondaggio)**

Voci di costo	INTERNA		HOSTED	
	Costo per utente	Costo per utente per tre anni	Costo per utente	Costo per utente per tre anni
Manodopera 875 utenti per ogni amministratore FTE Costo annuale complessivo per amministratore: 64.000 € 5% di crescita annuale dichiarata	73,50 € (annuale)	231,6 €	3,38 € (annuale)	3,38 €
Server/appliance anti-virus 250 utenti per server/appliance Costo della soluzione: 3.500 €	3,38 € (iniziale)	4,76 €	0 €	0 €
Server/appliance anti-spam 250 utenti per server/appliance Costo della soluzione: 3.500 €	13,73 € (iniziale)	4,57 €	0 €	0 €
Ampiezza di banda dedicata ai sistemi di messaggistica 2.100 € mensili per 1.000 utenti 20% dedicata al traffico dei sistemi di messaggistica il 90% del traffico di messaggistica è spam/malware	0,38 € (mensile)	13,88 €	0,04 € (mensile)	1,44 €
TOTALE PER TRE ANNI	254,81 €		11,58 €	
COSTO ANNUALE MEDIO	84,93 €		3,86 €	
COSTO MENSILE MEDIO	7,07 €		0,32 €	

Nota: i costi di licenza e di sottoscrizione non sono inclusi.

Inoltre, le soluzioni integrate che forniscono sicurezza sia web che e-mail di tipo hosted possono garantire alle organizzazioni la migliore protezione dalle minacce in rapida evoluzione, che si diffondono lungo questi due canali di comunicazione più largamente usati.

Websense

Websense, Inc. (NASDAQ: WBSN), azienda leader mondiale nelle tecnologie di protezione Web, sistemi di messaggistica e dati, fornisce Essential Information Protection (TM) a più di 42 milioni di dipendenti in più di 50.000 organizzazioni in tutto il mondo. Distribuiti grazie alla sua rete internazionale di partner di canale, i software e le soluzioni di sicurezza di tipo hosted di Websense aiutano le organizzazioni a fermare il codice dannoso, a prevenire la perdita di informazioni sensibili e ad attuare le policy di sicurezza nell'uso di Internet e dei sistemi di messaggistica. Maggiori informazioni sono disponibili al sito www.websense.com.

© 2008-2009 Osterman Research, Inc., tutti i diritti riservati.

Nessuna parte di questo documento può essere riprodotta in qualsiasi forma e con qualsiasi intento, non può essere distribuita senza l'autorizzazione di Osterman Research Inc., non può essere commercializzata o distribuita da alcuna realtà escluso Osterman Research Inc., senza una previa autorizzazione scritta di Osterman Research Inc.

Osterman Research Inc. non fornisce consulenza in ambito legale. Nulla in questo documento è da considerarsi di valore legale; questo documento o alcun prodotto software o altra offerta nominata al suo interno non potranno essere osservati dal lettore al posto di qualsiasi legge (un elenco esaustivo ma non completo comprende ogni atto, statuto, regolamento, norma, direttiva, ordine di esecuzione ecc., nell'insieme definito "legge") nominata in questo documento. Qualora lo ritenga necessario, il lettore può contattare l'organismo legale di competenza per ogni legge a cui si fa riferimento all'interno. Osterman Research Inc. non si assume alcuna responsabilità e non conferisce alcuna garanzia sulla completezza o sull'accuratezza delle informazioni contenute in questo documento.

QUESTO DOCUMENTO È FORNITO "AS IS", PRIVO DI OGNI GARANZIA DI QUALUNQUE TIPO. TUTTE LE RESPONSABILITÀ, CONDIZIONI E GARANZIE DICHIARATE O IMPLICITE, COMPRESA OGNI GARANZIA IMPLICITA DI COMMERCIALIZZABILITÀ O DI IDONEITÀ PER UN PARTICOLARE PROPOSITO, SONO DICHIARATE, SALVO NELLA CASO IN CUI QUESTO DISCLAIMER SIA DEFINITO NON LEGALE.