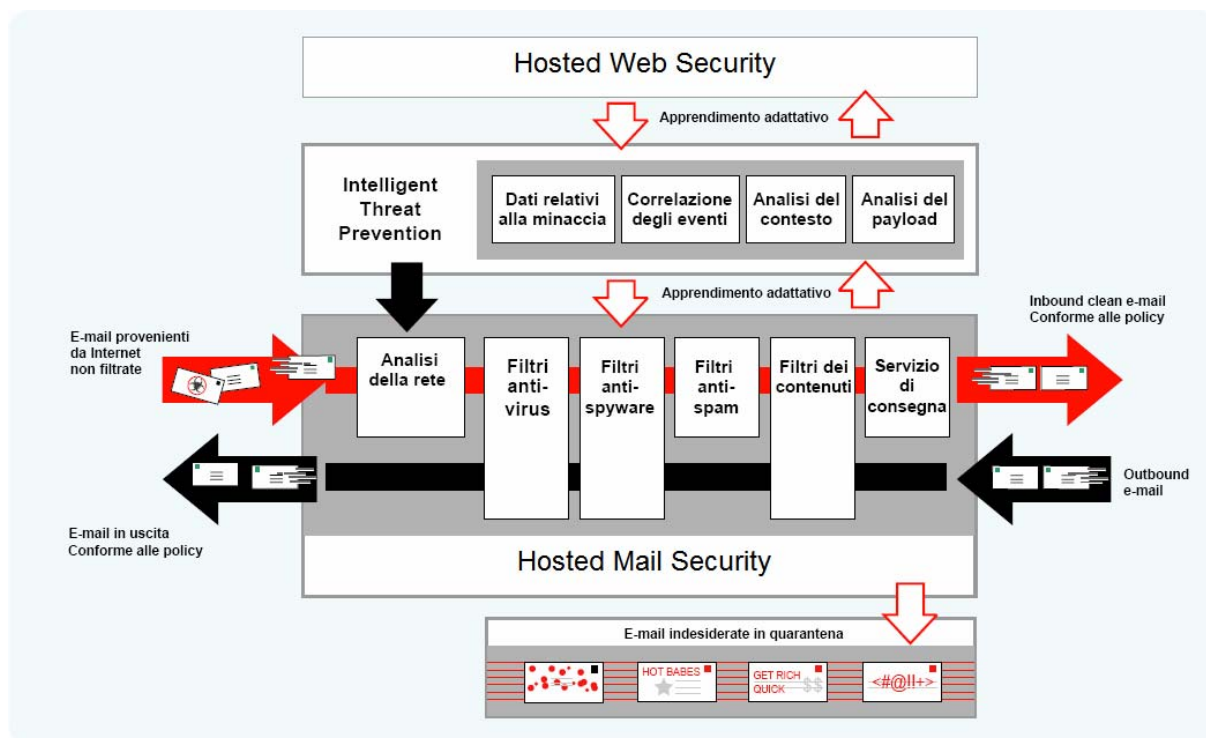
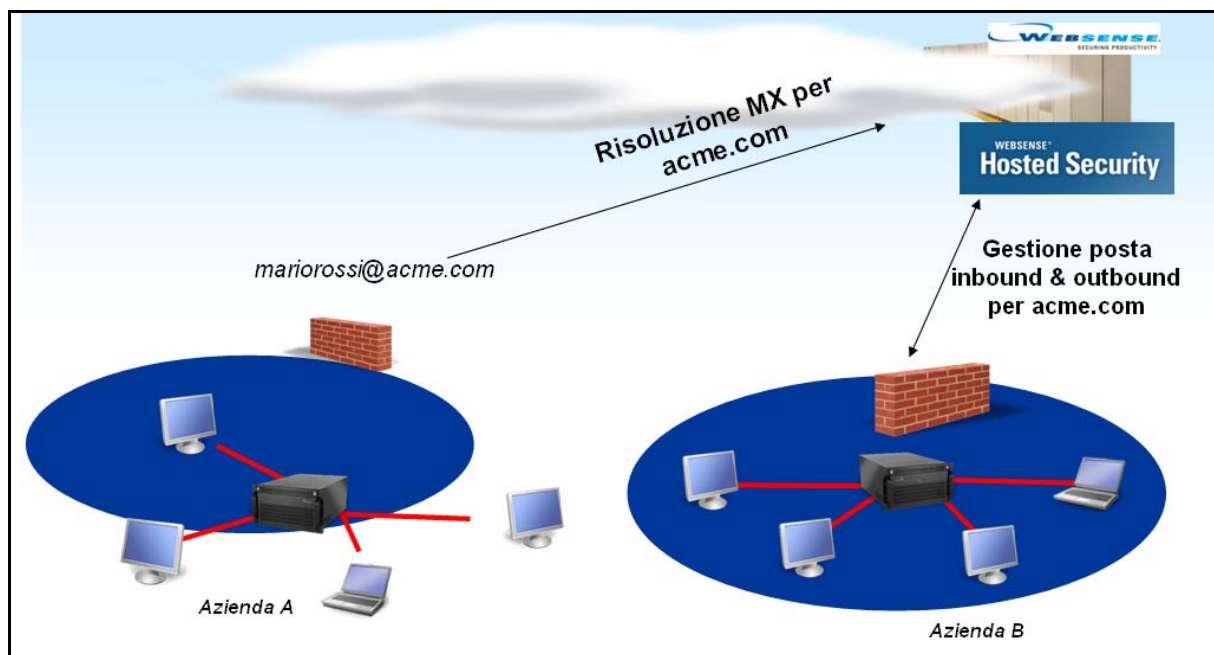


## Descrizione servizio Websense Hosted Mail Security

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 Websense e alle tecnologie sofisticate su cui si basano, è possibile usufruire di una protezione più efficace nei confronti delle minacce Internet ed e-mail.



La soluzione on-demand per la sicurezza della posta elettronica di Websense 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.



## Infrastruttura del servizio

La protezione della rete con Websense Hosted eMail security è di semplice implementazione, in quanto necessita solamente re-indirizzare gli MX record DNS del dominio di posta verso i Datacenter Websense 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 Websense 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 Websense impiegano cluster di macchine ridondanti e load-balanced ad alta disponibilità collocate presso undici sedi nel mondo. Tutti i centri dati Websense 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 Websense 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.

### **Protezione Anti-Virus combinata**

Hosted Mail Security utilizza tre tecnologie anti-virus di tipo commerciale per analizzare i messaggi alla ricerca di e-mail infette. A queste si aggiunge , la tecnologia Treathseeker per la prevenzione intelligente delle minacce, la quale fornisce una protezione completa e costantemente aggiornata dalle nuove minacce e-mail non appena queste si presentano.

### **Prevenzione intelligente delle minacce: ThreatSeeker network**

Attraverso l'uso di sofisticate tecniche di scansione euristiche ed intervento umano, la tecnologia Threatseeker è in grado di identificare e bloccare i nuovi tipi di malware riducendo al minimo la "finestra di vulnerabilità" che intercorre da quando il nuovo malware viene identificato a quando i vendor anti-virus rendono disponibile la relativa segnatura.

La forte integrazione tra le tecnologie di gestione delle minacce Web e Mail consente inoltre una maggiore reattività nell'individuare quelli che oggi vengono indettificate come minacce combinate, ovvero che sfruttano tecnologie Web e Mail per la diffusione di codice malizioso o attacchi phishing.

#### **Principali vantaggi**

- Capacità di bloccare automaticamente virus e altri malware prima che raggiungano la rete aziendale
- Possibilità per i clienti di ottenere controllo e visibilità attraverso un portale online real-time dedicato
- Operazioni 24 x 7 gestite da esperti nella sicurezza
- Facilità di implementazione e gestione
- Protezione combinata fornita da tre tecnologie avanzate di tipo commerciale
- Tecnologia per la protezione intelligente dalle minacce per contrastare i pericoli e-mail ignoti

### **Gestione delle Mail Indesiderate**

Hosted Antispam è un sofisticato servizio gestito in grado di identificare in modo intelligente lo spam e di bloccarne la diffusione. Attraverso l'impiego di un insieme di tecniche differenti, Hosted Antispam è capace di bloccare regolarmente oltre il 98% dei messaggi indesiderati.

Il filtraggio dello spam pone diverse sfide complesse, a causa della natura dinamica dei messaggi spazzatura. Un filtro realmente efficace deve essere in grado di bloccare la quasi totalità dei messaggi indesiderati con il numero minimo di "falsi positivi" (e-mail valide identificate erroneamente come spam).

Hosted Antispam risolve brillantemente tutti questi problemi grazie a un engine adattativo per il filtraggio dello spam capace di apprendere realmente ciò che l'azienda considera spam e di filtrarlo di conseguenza. Questo approccio, abbinato



alla capacità di definire soglie per lo spam specifiche per ogni dominio e utente, fa di Hosted Antispam una delle tecnologie di filtraggio dello spam più efficaci attualmente disponibili in commercio.

### **Funzionalità self-service per gli utenti**

Hosted Antispam riconosce che la decisione definitiva riguardo ciò che è o non è spam spetta agli utenti, i quali possono scegliere di ricevere report regolari riguardanti i messaggi, accedere alla propria area di quarantena per esaminare le e-mail bloccate, e gestire proprie black- e white-list. Abbinato a un engine adattativo per il filtraggio dello spam, questo approccio elimina le preoccupazioni di utenti e amministratori e-mail riguardo i rischi di falsi positivi.

### **Principali vantaggi**

- Protezione accresciuta, costi operativi ridotti
- Tassi di identificazione elevati, falsi positivi ridotti al minimo
- Tecnologia per il filtraggio dello spam adattativa e auto-ottimizzante
- Pieno controllo e visibilità da parte dei clienti attraverso un portale online real-time protetto

### **Regole di cifratura basate su policy**

Hosted Encryption è un servizio on-demand basato su policy che permette lo scambio di comunicazioni e-mail protette tra business partner e singoli utenti.

Molte aziende sono fortemente interessate ai vantaggi ottenibili attraverso la cifratura delle comunicazioni e-mail; tuttavia per la maggior parte di esse i costi e le complessità dell'implementazione e della successiva gestione di una simile capacità risultano semplicemente troppo elevate. La conseguenza è che numerose aziende finiscono per accettare i rischi associati all'invio di e-mail sensibili non cifrate e quindi, per loro stessa natura, vulnerabili.

Hosted Encryption fornisce una conveniente alternativa all'implementazione di una soluzione desktop-to-desktop completa. Questo servizio non richiede l'implementazione di hardware o software addizionale; di conseguenza risulta particolarmente facile da implementare e gestire sia per gli amministratori che per gli utenti finali.

Con Hosted Encryption gli amministratori di rete sono in grado di definire policy per proteggere le comunicazioni e-mail delle aziende. Ciò permette di dare vita a comunità nelle quali viene praticato lo scambio di e-mail cifrate. Il protocollo standard TLS viene utilizzato per cifrare il tunnel di comunicazione tra gli utenti Websense e i destinatari specificati all'interno della policy.

### **Principali vantaggi**

- Privacy accresciuta delle comunicazioni
- Superiore integrità dei messaggi
- Funzione di autenticazione
- Applicazione delle policy di sicurezza alle e-mail protette



- Facilità di implementazione e gestione
- Funzionamento trasparente. Non è richiesta alcuna formazione per il personale
- Niente hardware o software aggiuntivo
- Conformità accresciuta con le principali normative

### **Service Level Agreement**

- Il servizio offre un Up-Time garantito del 99.999%, attraverso una serie di datacenter dislocati geograficamente in Europa e nel mondo
- Percentuale di blocco SPAM garantita del 97%
- Percentuale di blocco Virus Conosciuti del 100%
- Tempo massimo di processamento per e-mail fino a 2Mbyte pari a 60 secondi
- In caso di indisponibilità del server interno, le e-mail rimangono in attesa di inoltrare fino a 7 giorni solari. Tale tempo può essere esteso su richiesta del cliente.

### **Certificazione ISO 27001**

Lo standard ISO/IEC 27001 è uno standard pubblicato nell'ottobre 2005 dall'International Organization for Standardization and the International Electro-technical Commission che fornisce i requisiti di un Sistema di Gestione della Sicurezza nelle tecnologie dell'informazione (Information Security Management System - ISMS). Obiettivo dello standard è la protezione dei dati e delle informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità, e garantire quindi un elevato standard per la fornitura di un servizio che implica il trattamento e la gestione dei dati sensibili del cliente.

### **Principali Caratteristiche del servizio**

Un servizio on-demand fornisce una protezione efficace contro ogni minaccia con un costo di possesso complessivo inferiore. Tra i principali vantaggi si segnalano:

- Il blocco delle minacce e-mail accade a livello Internet, prima dell'arrivo all'interno della rete aziendale
- La tecnologia per la prevenzione intelligente delle minacce (Threatseeker network) analizza tutte le e-mail per identificare in tempo reale i nuovi pericoli e aggiornare le difese al fine di restringere la finestra di vulnerabilità
- Impatto minimo sull'infrastruttura esistente: l'implementazione del servizio non richiede l'acquisto di ulteriori risorse Hardware o Software
- Soluzione unica per più domini priva di singoli punti deboli, l'architettura è in grado di scalare automaticamente all'aumentare del carico di lavoro.
- Architettura ad alta disponibilità per garantire la continuità dei servizi e-mail e web: la presenza allo stato attuale di 8 datacenter nella sola Europa

garantisce che in caso di caduta di un intero datacenter il servizio venga preso immediatamente in carico da uno dei rimanenti centri.

- E-mail disaster recovery - accodamento dei messaggi in caso di indisponibilità del mail server del cliente
- Componente di una suite di soluzioni per la sicurezza del Web e della posta elettronica sviluppate da Websense per accrescere la protezione e incrementare il grado di controllo; il tutto proposto da un leader riconosciuto del settore della sicurezza Internet
- La soluzione e quindi tutti i datacenter che erogano il servizio sono certificati ISO27001

Prodotto	Descrizione	Funzionalità	Vantaggi per i clienti
<b>Hosted Mail Security</b>	Hosted Anti-Virus	Garantisce che nessuna mail infetta possa arrivare all'interno della propria azienda, attraverso il controllo con tre diversi motori antivirus: Authentium, kaspersky e Panda.	- Minimizza il rischio di ricevere mail infette grazie all'utilizzo di più tecnologie anti-virus in cascata.
	Hosted Anti-Spam	Consente di gestire lo spam e la quarantena delle email indesiderate, garantendo comunque accesso all'utente finale ad un portale personalizzato.	- La gestione a monte delle email consente di ridurre il carico di amministrazione del server di posta, della banda inutilmente consumata da mail subito eliminate grazie ad un sistema ridondato e altamente scalabile.
	Reporting	Un portale avanzato di reportistica consente di avere la massima visibilità sullo stato del sistema e statiche avanzate sull'andamento della rete.	- La visibilità immediata dei report attraverso una console personalizzata consente di avere in qualsiasi momento il controllo del sistema