



L'implementazione a strati della sicurezza dei messaggi consente di ottenere un'efficienza e una protezione maggiori massimizzando nel contempo gli investimenti nelle risorse di rete.

Una migliore protezione della messaggistica deriva da una visione d'insieme completa. Websense Hybrid Messaging Security fornisce la migliore protezione dalle minacce incrociate provenienti dal Web e dalle email.

Websense®

Protezione per la messaggistica ibrida

Le odierne minacce per la posta elettronica sono più invasive e abbondanti che mai e la natura di questi attacchi è in continua trasformazione. Le aziende moderne devono implementare soluzioni di sicurezza che vanno oltre il blocco dello spam. Una buona soluzione di sicurezza dei messaggi offre standard precisi per l'attenuazione del rischio e per l'allineamento con la conformità aziendale e policy di governance.

Websense Hybrid Messaging Security combina la soluzione Websense Hosted Email Security implementata a livello di Internet e la soluzione Websense Email Security implementata a livello di gateway. Sovrapponendo queste soluzioni in un'implementazione ibrida, le organizzazioni ricevono una maggiore protezione e possono soddisfare una più ampia gamma di requisiti sicurezza in un singolo modello di implementazione. Le aziende e gli analisti riconoscono sempre di più il valore di garantire protezione dove ha maggiormente senso. L'implementazione della sicurezza dei messaggi a strati consente di ottenere un'efficienza e una protezione maggiori massimizzando nel contempo gli investimenti nelle risorse di rete.

come funziona

Websense Hosted Email Security filtra lo spam e i virus a livello di Internet, con risparmio in termini di larghezza di banda, tempi di amministrazione e risorse di sistema.

On-premise Websense Email Security opera a livello di gateway e offre una protezione granulare per la posta elettronica in uscita, consentendo alle organizzazioni di configurare policy adeguate per

il filtraggio in uscita, nonché un secondo strato opzionale per il filtraggio in entrata. Utenti delegati possono accedere a potenti strumenti di reporting. È previsto inoltre un accurato controllo degli allegati per garantire la conformità normativa.

Solo un'implementazione ibrida offre la riduzione dei costi di un servizio hosted combinato a controlli in loco per un filtraggio granulare dei contenuti e-mail.

principali vantaggi

- **Rete migliore e riduzione dei costi**

Vantaggi combinati offerti da entrambi i modelli di implementazione, Websense Hosted Email Security e on-premise Websense Email Security. Spam e virus vengono bloccati prima che raggiungano la rete, questo offre una maggiore larghezza di banda, più risorse e prestazioni migliori, garantendo nel contempo che messaggi riservati e sensibili rimangano all'interno della rete.

- **Attenuazione del rischio e dell'esposizione con ritorno sull'investimento dimostrato**

Websense Hosted Email Security offre livelli certi di protezione della posta elettronica da virus, garantendo operatività e visibilità supportate da SLA a fronte di possibili tendenze e attività di minaccia. On-premise Websense Email Security offre report drill-down con una visibilità senza precedenti di minacce per la posta in uscita.

- **Costo totale della proprietà ridotto**

Websense Hosted Email Security riduce il costo della larghezza di banda occupata da spam, liberando tempo e risorse di sistema. Le aziende riacquistano risorse preziose in termini di hardware e tempo di amministrazione per concentrarsi su altri elementi della sicurezza per la posta elettronica, inclusi il rafforzamento e la conformità delle policy in uscita.

- **Meno complessità grazie a una soluzione unificata**

Consolidare la protezione contro minacce per la posta elettronica, la conformità e la prevenzione contro la perdita di dati tramite una soluzione unificata di sicurezza delle e-mail, che blocca più tipi di minacce per la posta elettronica nel punto di origine.

riassumendo

Websense Hybrid Messaging Security combina la soluzione Websense Hosted Email Security (implementata a livello di Internet) e la soluzione Websense Email Security (implementata a livello di gateway). Sovrapponendo queste soluzioni in un'implementazione combinata, le organizzazioni ricevono una maggiore protezione rispetto a un singolo modello di implementazione.

La combinazione di competenze nell'ambito della sicurezza e Websense ThreatSeeker™ Network garantisce una protezione dinamica contro minacce per il Web e la posta elettronica, fermando gli attacchi prima che colpiscano la rete. La tecnologia Websense ThreatSeeker™ offre i massimi livelli di accuratezza con i minimi livelli di falsi positivi e garantisce una valida protezione contro molte delle odierne minacce.

contatti sede

Websense, Inc.
San Diego, CA USA
tel +1 800 723 1166
fax +1 858 458 2950
www.websense.com

Websense UK Ltd.
Reading, Berkshire UK
tel +44 118 938 8600
fax +44 118 938 8698
www.websense.co.uk

Websense Ireland
Dublin Ireland
tel +353 1 6319360
fax +353 1 6319001
www.websense.com

Websense Singapore
Singapore
tel +65 6248 4857
fax +65 6248 4531
www.websense.com/apac

altri indirizzi
www.websense.com/international

sede uffici

Australia websense.com.au
Israele websense.com

Cina prc.websense.com
Italia websense.it

Francia websense.fr
Giappone websense.jp

Germania websense.de
Paesi Bassi websense.com

Hong Kong websense.cn
Singapore websense.com

India websense.com
Spagna websense.com.es

Irlanda websense.co.uk
EAU websense.com

• Consolidamento grazie ad un solo fornitore di fiducia

Websense è leader di mercato nella fornitura di sicurezza per il Web, per la posta elettronica e per i dati alle aziende di tutto il mondo. Grazie al consolidamento della sicurezza dei messaggi in entrata e in uscita tramite Websense, le organizzazioni si avvalgono del supporto da un singolo punto di contatto. Con Websense Essential Information Protection™ le aziende possono anche ampliare la protezione e includere la sicurezza per il Web e per i dati garantita da Websense.

esempi

I seguenti esempi illustrano come le organizzazioni possono trarre vantaggio da un'implementazione ibrida.

Esempio n. 1: La sicurezza ibrida della posta elettronica tiene lontane le minacce dalla posta in entrata e in uscita.

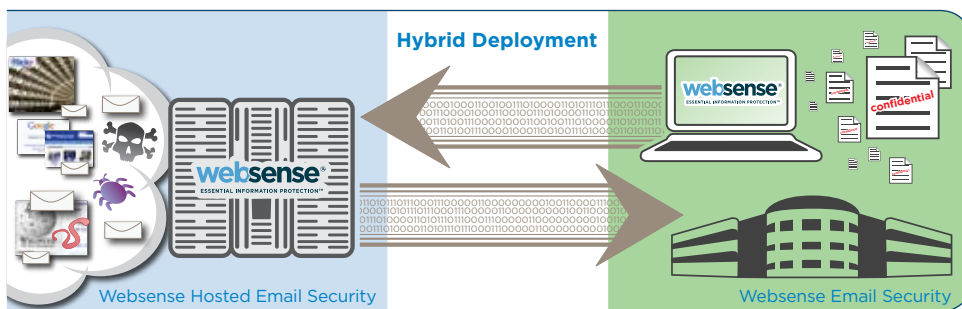
Mantenere certi tipi di messaggi al loro posto garantisce un vantaggio logico; i messaggi dannosi devono stare fuori dalla rete; i messaggi sensibili e riservati devono stare all'interno della rete. La sicurezza ibrida della posta elettronica tiene le e-mail potenzialmente dannose al loro posto.

In questo scenario, Websense Hosted Email Security elimina virus, malware, worm, spam e altre minacce prima che esse raggiungano la rete. On-premise Websense Email Security impedisce che i dati sensibili lascino la rete via e-mail. Per molti clienti, soprattutto piccole e medie imprese, questo rappresenta il primo passo giusto verso l'implementazione di una soluzione completa di prevenzione della perdita di dati.

Esempio n. 2: La sicurezza ibrida dei messaggi migliora la rete e riduce i costi.

Websense Hosted Email Security può eliminare circa il 90% del traffico di posta elettronica in entrata. Questo perché circa il 90% di tutta la posta elettronica è spam. Bloccando lo spam e i virus prima che raggiungano la rete, il carico di ciò che viene elaborato con Websense Email Security è notevolmente ridotto. Il secondo vantaggio è che una volta eliminato il grosso dello spam, Websense Email Security può eseguire un'ulteriore selezione della posta elettronica attraverso un secondo set di tecnologia, per assicurare che la posta elettronica sia pulita.

In questo modo, le organizzazioni migliorano l'efficienza dell'elaborazione della posta elettronica e garantiscono una maggiore protezione tramite più strati di protezione dei messaggi.



Websense Hybrid Email Security combines both a hosted and on-premise solution for layered protection.

Per ulteriori informazioni, per iniziare una prova gratuita delle soluzioni Websense per posta elettronica o per visualizzare una demo online, visitare www.websense.com/evaluations.