



“90 dei 100 siti Web più conosciuti sono classificati come siti di social networking o di ricerca, e più del 47% di questi siti supporta i contenuti generati dagli utenti.”

Websense Security Labs™, 2009

Websense®

Soluzioni Web Security Gateway

Le tecnologie dinamiche e interattive, tipiche del Web 2.0, hanno trasformato Internet in una piattaforma per applicazioni core business. Sistemi tradizionali di Customer Relationship o di contabilità oggi sono resi disponibili, in modo interattivo, attraverso il Web, mentre applicazioni di social networking sono utilizzate quotidianamente per operazioni di recruitment, lead generation e altri processi di business. Con il Web 2.0, tuttavia, sono subentrati rischi sempre nuovi, e allo stesso tempo i contenuti dinamici generati dagli utenti rendono le tradizionali tecnologie di sicurezza, dagli antivirus al filtraggio degli URL, inefficaci. Tali tecnologie, inoltre, non permettono il controllo sui dati sensibili in uscita, pubblicati sui siti 2.0.

Le soluzioni Web Security Gateway di Websense® guidano il settore dei Secure Web Gateway fornendo la migliore protezione contro le attuali minacce del Web 2.0, consentendo il più basso Total Cost of Ownership (TCO). Si tratta delle uniche soluzioni in grado di fornire prevenzione dalla perdita dei dati di livello enterprise e gestione unificata delle implementazioni ibride cloud/on-premise. Le soluzioni Web Security Gateway consentono alle organizzazioni di sfruttare le potenzialità del Web 2.0, senza doversi preoccupare di malware proveniente dal Web, contenuti inappropriati o fuga di dati sensibili.

Come funziona

Le soluzioni Web Security Gateway svolgono il controllo dei contenuti in ingresso e in uscita quando questi attraversano i confini della rete, per proteggere l'azienda dal malware dinamico proveniente dal web, prevenire la fuga di dati sensibili e aumentare la produttività dei dipendenti. La tipologia di implementazione TruHybrid™ di Websense supporta sia gli appliance on-premise che le piattaforme Security-as-a-Service (SaaS), con la gestione dell'intero ambiente di rete tramite una unica infrastruttura di policy e di reportistica. A differenza degli approcci di altre soluzioni, ai clienti di Websense viene offerta la flessibilità di scegliere la piattaforma, o un mix di piattaforme, che al meglio possa rispondere alle loro specifiche necessità operative senza dover sostenere il costo di sistemi di gestione multipli.

Le soluzioni Web Security Gateway di Websense mettono a disposizione:

- **Prevenzione della fuga di dati e controllo della compliance** - Le caratteristiche di prevenzione della perdita di dati di livello enterprise integrate stabiliscono i controlli richiesti per abilitare le comunicazioni in uscita a destinazioni come i siti di Web mail e di social network, soddisfacendo allo stesso tempo i criteri di conformità per controllare la fuga di dati sensibili.
- **Protezione dal malware** - Il sistema di Advanced Classification Engine (ACE) TRITON™ di Websense fornisce protezione sia contro gli attacchi legacy basati su file, sia dagli attacchi dinamici basati su codice che eludono le tradizionali soluzioni antivirus.
- **Web 2.0 e produttività dei dipendenti** - Il sistema di Advanced Classification Engine TRITON elimina i contenuti inappropriati dai siti Web 2.0 complessi, dinamici e protetti da password che non possono essere classificati dalle soluzioni di filtraggio URL tradizionali.
- **Total Cost of Ownership (TCO) più basso** - La TRITON Console di Websense e l'implementazione TruHybrid riducono il numero di appliance e i sistemi di gestione che devono essere supportati lungo la rete, oltre alla varietà di dispositivi di differenti fornitori.
- **Copertura di sicurezza lineare su tutta l'azienda** - La tipologia di implementazione TruHybrid unifica le policy in uso sulle implementazioni on-premise e SaaS. Se gli utenti si spostano tra uffici o lavorano da casa, una unica policy specifica sarà attiva in modo uniforme.

“Nel corso della prima metà del 2009, più di 80 tra i 100 siti più visitati hanno ospitato contenuti pericolosi o un reindirizzamento mascherato verso un sito web illegale.”

Websense Security Labs, 2009

Sistema di classificazione di tipo avanzato

Le soluzioni Web Security Gateway di Websense comprendono il sistema di Advanced Classification Engine (ACE) TRITON, il più rigoroso* sistema di analisi della sicurezza bidirezionale che unisce tecniche di analisi all'interno della rete ad una attività preventiva eseguita in profondità contro la fuga di dati verso l'esterno. Il sistema ACE unisce i sistemi di protezione tradizionali con le più aggiornate tecniche di classificazione dei contenuti, come gli anti-virus, i sistemi di filtraggio Web, i servizi di rilevamento della reputazione e il fingerprinting, per classificare in modo accurato i rischi interni ed esterni. L'Advanced Classification Engine, supportato dalla rete ThreatSeeker® Network di Websense, analizza i contenuti quando attraversano il gateway con attività di security scanning, classificazione dei contenuti in tempo reale e prevenzione della perdita dei dati di livello enterprise.

Security Scanning in tempo reale

Le tecnologie anti-virus, singolarmente, non sono in grado di tenere il passo degli attacchi dinamici e basati su codice che dominano lo scenario delle minacce Web. Le attività di analisi in tempo reale eseguite tramite il sistema di security scanning proprietario di Websense, sono in grado di fare fronte a queste minacce zero-day individuando i contenuti dannosi al volo, senza il bisogno di un controllo preliminare con i database degli attacchi conosciuti.

Classificazione dei contenuti in tempo reale

Molti dei siti più comunemente utilizzati non possono essere classificati in modo preciso dai sistemi tradizionali di filtraggio URL. Per esempio, una singola pagina di Google o di Facebook può contenere contenuti misti, appartenenti a diverse categorie, rendendo impossibile la definizione di una unica categoria. Ne deriva che molte organizzazioni sono forzate a bloccare risorse utili come queste in modo indiscriminato, o a ignorare le policy di utilizzo consentito fornendo l'accesso completo alla navigazione sui siti dinamici Web 2.0.

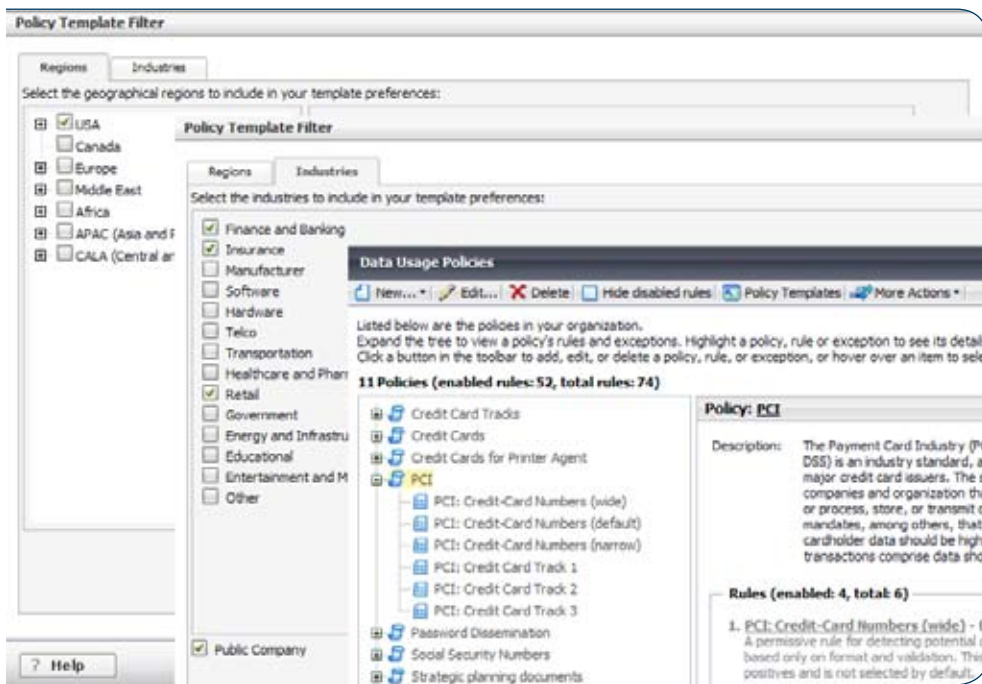
Le soluzioni Web Security Gateway offrono classificazione dei contenuti in tempo reale per estendere le policy di uso consentito ai siti dinamici Web 2.0, classificando i singoli elementi all'interno di ogni pagina Web in tempo reale. Se un particolare contenuto viola una policy, può essere eliminato da una pagina, mentre allo stesso tempo si possono consentire informazioni conformi. Questa funzionalità unica permette un ampio accesso ai siti Web 2.0 ammessi per l'attività aziendale, tutelando così la produttività e la conformità alle policy di uso consentito.

Prevenzione della perdita dei dati di classe enterprise

Il sistema di prevenzione della perdita dei dati (DLP - Data Loss Prevention) integrato, di livello enterprise, determina i controlli necessari a permettere alle comunicazioni aziendali in uscita di raggiungere siti di Web mail e di social networking, in conformità con le regole che controllano la fuga di dati sensibili. A differenza degli approcci di altre soluzioni, le cui funzionalità di DLP si limitano al controllo delle keyword o richiedono l'integrazione di terze parti complesse, le soluzioni Web Security Gateway mettono a disposizione tutte le funzionalità della soluzione di DLP Websense, leader nel settore, relative al traffico di rete http, https e FTP. Queste comprendono più di 800 policy pronte all'uso, fingerprinting per il controllo dei contenuti in profondità e reportistica completa circa il rispetto delle normative.

L'integrazione di Web DLP con le soluzioni Web Security Gateway riduce in modo significativo il TCO, eliminando la necessità di hardware dedicato per attività di DLP in ogni sede dell'azienda. Per le organizzazioni con progetti a lungo termine in ambito Data Loss Prevention, Web DLP fornisce anche una solida protezione dell'investimento: un semplice upgrade software è tutto ciò che si richiede per estendere il controllo oltre il Web per includere altri tipi di traffico (email, messaggistica istantanea e P2P), gli endpoint e i dati archiviati (per esempio database, file share, Exchange, Share Point). Per questo motivo, l'estensione della copertura da Web DLP ad altri canali non richiede un rifacimento dell'architettura. Le policy esistenti e gli investimenti in infrastruttura sono così protetti.

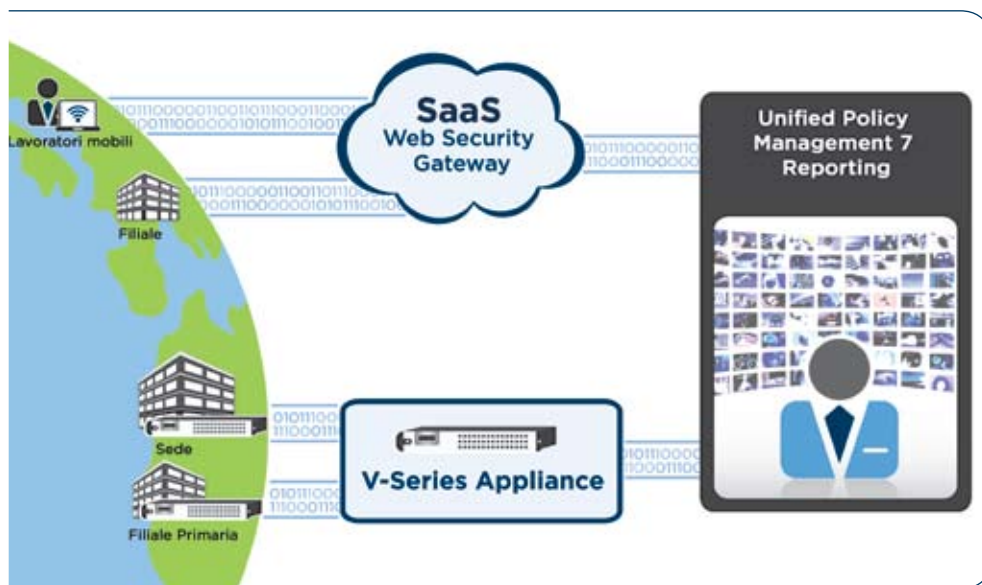
* <http://www.websense.com/content/tolly-report-reg.aspx>



Semplici guide all'uso delle policy DLP aiutano gli amministratori IT a definire rapidamente policy best practice, conformi alle leggi o alle normative specifiche del settore.

Implementazione TruHybrid

L'implementazione TruHybrid consente di scegliere in modo flessibile piattaforme di implementazione mista on-premise e SaaS, permettendo allo stesso tempo di gestire l'intero ambiente con un singolo sistema di gestione unificata. È possibile estendere la sicurezza alle filiali o agli utenti mobili sfruttando la piattaforma SaaS. E allo stesso tempo, è possibile implementare appliance ad elevate prestazioni nelle sedi di grandi aziende o presso data center. Indipendentemente dalla scelta mista di SaaS o di appliance effettuata, è possibile definire una unica policy valida su tutta l'azienda. Si tratta di un approccio unificato che non solo taglia il costo di gestione di una implementazione ibrida on-premise/SaaS, ma anche garantisce la copertura completa di sicurezza su tutti gli ambienti.



L'implementazione TruHybrid consente la gestione unificata delle implementazioni ibride on-premise/SaaS.

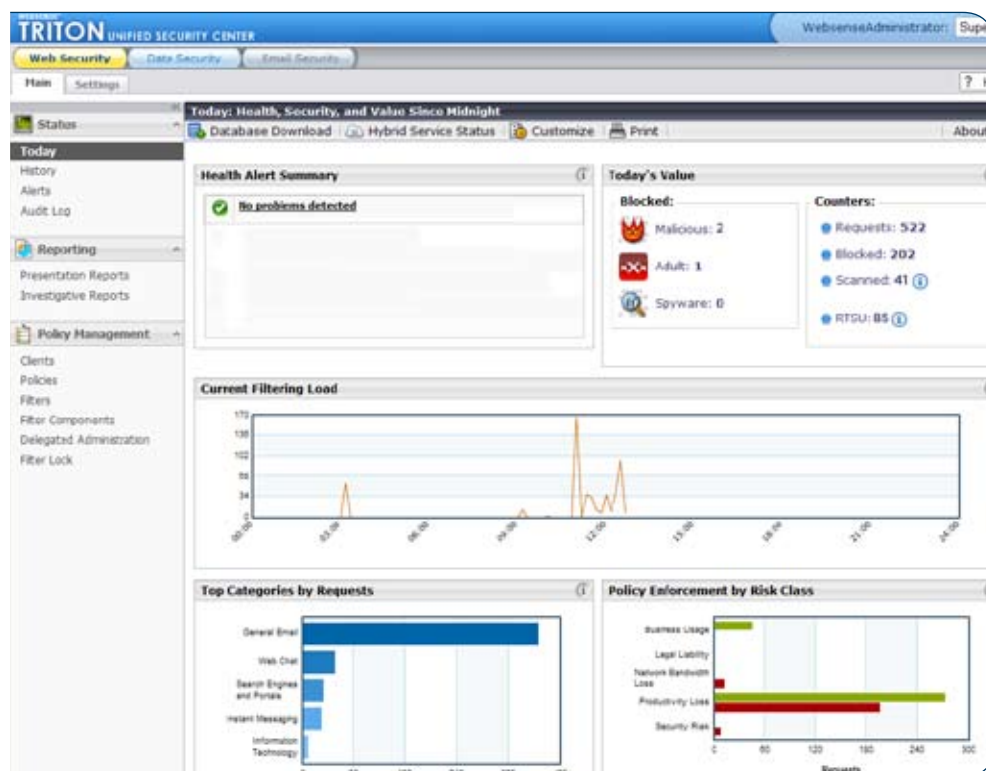
“Facciamo affidamento sull’appliance V10000TM secure Web gateway di Websense per consentire al nostro personale infermieristico di accedere in modo rapido alle informazioni di cui ha bisogno, in modo sicuro e protetto. Con l’attività di scansione in tempo reale e la possibilità di creare policy flessibili sull’utilizzo di Internet, non mi preoccupa che gli infermieri possano capitare su un sito che è stato compromesso con codice dannoso in grado di rubare dati, o che possano inviare involontariamente dati sensibili dei pazienti alla destinazione sbagliata.”

Larry Whiteside

Responsabile
sicurezza informatica
Visiting Nurse Service
di New York

“Il 57% degli attacchi dannosi lanciati via Web contiene codice in grado di rubare dati.”

WebSense Security Labs, 2009



Il pannello di controllo interattivo della console TRITON consente di intervenire immediatamente in caso di minaccia o di attività di violazione delle policy non appena si manifestano.

Visibilità e controllo SSL

Il crescente utilizzo del traffico SSL ha creato punti ciechi per i filtri URL legacy, e apre backdoor per minacce e perdita dei dati. Le soluzioni Web Security Gateway forniscono visibilità e controllo sul traffico SSL permettendo alle organizzazioni di applicare policy a tutte le comunicazioni Web.

Controllo delle applicazioni di livello avanzato

L'aumento delle applicazioni di rete, come quelle di messaggistica istantanea e P2P, ha aperto agli hacker un canale per recare danni all'azienda e rubare dati sensibili. Le soluzioni Web Security Gateway sono in grado di controllare più di 125 protocolli di rete e migliaia di applicazioni, per diminuire il rischio e prevenire la perdita dei dati causata da applicazioni non autorizzate. Il raggio di azione delle policy varia dal semplice blocco delle applicazioni ai controlli altamente granulari della banda.

Gestione unificata della protezione dei contenuti e reportistica

Una importante funzionalità disponibile con le soluzioni Web Security Gateway, e fornita solo da Websense, è la console TRITON. Si tratta di uno strumento in grado di consolidare la gestione di tutte le soluzioni Websense di sicurezza Web, dati ed email in un'unica interfaccia basata sul Web. Un pannello di controllo intuitivo comprende oltre 55 modelli di reportistica e ampie caratteristiche di personalizzazione, per avere a disposizione un miglior monitoraggio dell'attività agli utenti, semplificare la risoluzione dei problemi e ridurre ulteriormente i rischi. L'impegno di gestione richiesto e il costo sono di molto inferiori rispetto ad altre analoghe soluzioni, considerando le numerose funzionalità di facile utilizzo, come l'elevato livello di drill-down, le policy wizard, i template di configurazione, la presenza di un sottosistema di schedulazione e gli aggiornamenti dei contenuti automatici. Dato che un'azienda può avvertire la necessità, con il tempo, di ampliare la sicurezza dei contenuti oltre la sicurezza Web, le funzionalità di gestione unificata della console TRITON possono essere facilmente estese per gestire centralmente la sicurezza email e i sistemi di DLP in modo completo.

Funzionalità	Vantaggi
Implementazione TruHybrid	Riduce il Total Cost of Ownership (TCO) e garantisce policy omogenee su tutta l'azienda attraverso la gestione unificata di implementazioni on-premise e SaaS.
Prevenzione della perdita dei dati di livello enterprise	Previene la fuga di dati all'esterno ed è in grado di stabilire i necessari controlli di conformità alle normative. Diminuisce il TCO evitando l'implementazione di una soluzione di DLP complessa.
Classificazione dei contenuti in tempo reale	Permette l'uso sicuro dei contenuti dei siti web dinamici, protetti da password e misti, attraverso il filtraggio dei contenuti in tempo reale.
Scansioni di sicurezza in tempo reale	Protegge le organizzazioni dal malware Web attraverso l'identificazione di minacce dinamiche, contenenti codice e sconosciute, al volo.
Console TRITON	Riduce il TCO e i costi di gestione di dispositivi di fornitori diversi grazie alla gestione unificata delle soluzioni di sicurezza Web, dati e email.
Antivirus Integrato	Protegge dagli attacchi di virus basati su file tramite l'utilizzo sia di antivirus di terze parti che dell'antivirus Web di Websense, di livello avanzato.
Filtraggio Web con funzionalità evolute di analisi della reputazione leader nel settore	Permette l'attivazione di una linea di base di policy di utilizzo consentito e blocca i siti dannosi conosciuti. Le tecniche di analisi della reputazione multiple comprendono metodi quali property type, lexical reputation, Web 2.0 post, categoria di URL, nearest neighbor, search reputation, history, age e geography.
Aggiornamenti in tempo reale dalla rete ThreatSeeker Network	Riduce l'esposizione a minacce in fase di diffusione fornendo aggiornamenti di sicurezza ogni 5 minuti.
Visibilità SSL	Attiva il controllo del traffico Web criptato con un proxy SSL completo e la gestione integrata dei certificati.
Controllo delle Applicazioni	Diminuisce i rischi, aumenta la produttività e riduce il costo della disponibilità di banda attraverso la gestione dell'uso dei protocolli di rete e delle applicazioni.
Web Proxy /Cache di classe Enterprise	Aumenta le prestazioni e riduce i costi di disponibilità di banda attraverso l'ottimizzazione del traffico. Supporta entrambe le configurazioni di proxy trasparente ed esplicita.
Autenticazione degli Utenti Flessibile	Attiva policy basate sugli utenti e sui gruppi con l'autenticazione flessibile attraverso Active Directory, LDAP, RADIUS, Novell, NTLM v2.
Alta disponibilità e Load Balancing	Abilita la ridondanza del sistema e la scalabilità per grandi aziende, sfruttando il protocollo WCCP o bilanciatori del carico esterni.

Gartner ha posizionato Websense nel quadrante dei leader nel più recente Magic Quadrant in ambito Secure Web Gateway.

Gartner, Inc.

"Magic Quadrant for Secure Web Gateway"* a cura di Peter Firstbrook e Lawrence Orans, 8 gennaio 2010

Websense, Inc.
San Diego, CA USA
tel 800.723.1166
tel 858.320.8000
www.websense.com

Websense Italy
Milan, Italy
tel +39 02 6203 3040
fax +39 02 6203 4000
www.websense.it

Australia
websense.com.au

Brasile
websense.com/brasil

Colombia
websense.com/latam

Francia
websense.fr

Germania
websense.de

Hong Kong
websense.cn

India
websense.com

Irlanda
websense.co.uk

Israele
websense.com

Italia
websense.it

Giappone
websense.jp

Malesia
websense.com

Messico
websense.com/latam

Cina
prc.websense.com

Singapore
websense.com

Spagna
websense.com.es

Taiwan
websense.cn

UAE
websense.com

Disponibilità della piattaforma di implementazione

Le implementazioni on-premise possono essere effettuate con gli appliance V-Series™ di Websense o tramite l'installazione del software su server generici. Le implementazioni in modalità SaaS sono supportate dalla soluzione Hosted Web Security Gateway di Websense.

- **Appliance V-Series** Gli appliance V-Series forniscono prestazioni di livello enterprise, affidabilità e facilità di implementazione di tipo on-premise. Scelti per ambienti di aziende Fortune 100, gli appliance V-Series integrano ridondanza a livello di componenti supportando allo stesso tempo una serie di feature di implementazione di tipo enterprise, tra cui il bilanciamento del carico e l'elevata disponibilità. Gli appliance V-Series sono stati inoltre progettati per supportare le soluzioni Websense future senza il bisogno di upgrade dell'hardware, estendendo la vita e il valore della piattaforma.
- **Hosted Web Security Gateway** Le soluzioni Hosted Web Security Gateway di Websense distribuiscono i processi di controllo della sicurezza tra 10 data center su scala mondiale ad elevata disponibilità, ridondati e ubicati su architettura "in the cloud". Si tratta di una modalità di SaaS che non solo accelera l'implementazione, ma che può ridurre i costi operativi eliminando il bisogno di supporto hardware on-premise in ogni sede aziendale. I data center Websense sono certificati ISO 27001 per rispondere a standard di sicurezza e disponibilità rigorosi, che sarebbero enormemente costosi da rispettare, per le singole aziende, in modalità on-premise, specialmente in sedi e uffici di filiale. Se implementata come soluzione stand-alone in modalità SaaS, Hosted Web Security Gateway di Websense consente in aggiunta l'integrazione e i vantaggi della sicurezza email SaaS.



L'appliance Websense V10000™

Opzioni di implementazione della soluzione Web Security Gateway di Websense

Websense Web Security Gateway Anywhere — Per implementazioni che richiedono gestione TruHybrid on-premise*/SaaS, prevenzione della perdita dei dati Web di classe enterprise, o il client Remote Filtering di Websense.

Websense Web Security Gateway — Per implementazioni on-premise*.

Websense Hosted Web Security Gateway — Per implementazioni SaaS.

Requisiti minimi del server per l'implementazione software:

Sistema operativo

Red Hat Linux v4,
update 5* o Windows Server 2003/
Server 2008†

CPU: 2 x processori Dual-core 2.8GHz

Memoria
4GB RAM

Unità disco fisso

2 dischi fisici:
* 100GB per Sistema Operativo e applicazione dati
temporanei, 100GB per la cache*
* 100GB (consigliato RAID 1)†

Interfacce di rete

2 x 10/100/1000 interfacce Ethernet

* Le implementazioni on-premise possono essere effettuate su appliance V-Series Websense o tramite l'installazione del software su server generici.

*Magic Quadrant è una rappresentazione grafica di un mercato in uno specifico periodo di tempo. Rappresenta l'analisi di Gartner sulle prestazioni di alcuni fornitori rispetto ai criteri di quel mercato, come definito da Gartner. Gartner non sostiene alcun fornitore, prodotto o servizio riportato nel Magic Quadrant e non invita gli utenti di tecnologia a scegliere solamente le aziende produttrici collocate nel quadrante dei "leader". Il Magic Quadrant è unicamente uno strumento di ricerca e non una guida alla scelta. Gartner declina ogni garanzia, implicita o esplicita, relativamente a questa ricerca, comprese eventuali garanzie di commerciabilità o idoneità per uno scopo particolare.

Per una dimostrazione on-line del prodotto o una prova gratuita di Web Security di Websense, consultate la pagina "Evaluation" del sito www.websense.it