



WebSense Enterprise® Panoramica sul prodotto

WebSense Enterprise®, la soluzione leader al mondo per la gestione dell'utilizzo di Internet da parte dei dipendenti, protegge le aziende e i dipendenti dalle minacce nuove ed emergenti quali spyware e malicious mobile code. Websense Enterprise consente di rafforzare la sicurezza, migliorare la produttività dei dipendenti, ridurre i rischi di potenziali responsabilità legali e ottimizzare l'uso delle risorse IT. Websense Enterprise si integra perfettamente con i principali prodotti dell'infrastruttura di rete e offre flessibilità e controllo senza eguali.

RISCHI CRESCENTI E SFIDE LEGATE ALLA PRODUTTIVITÀ

Tutte le aziende con una connessione a Internet hanno prima o poi dovuto affrontare il problema dell'accesso a contenuti Web inappropriati da parte dei dipendenti, cui si aggiungono i rischi legati al download di applicazioni dannose, allo spyware, all'instant messaging (IM), al peer-to-peer (P2P) e altri ancora. Il risultato è un aumento considerevole di costi e rischi associati a una rete priva di protezione. Si consideri quanto segue:

Spyware – Fino a 9 computer su 10 sono infettati da programmi spyware. E voi sapete quanti dei vostri desktop sono infetti? Come si può impedire che da questi spyware vengano reinviati su Internet informazioni confidenziali?

Malicious Mobile Code (MMC) – Il numero degli attacchi di MMC, spesso utilizzato per sottrarre dati riservati, è aumentato del 50% nello scorso anno.

Scambio di file via peer-to-peer (P2P) – Il 77% delle aziende ha almeno un'applicazione P2P presente sulla propria rete. Lo scambio di materiale pornografico è l'obiettivo di oltre il 73% delle attività P2P, che aprono una pericolosa porta a responsabilità legali per le aziende.

Instant Messaging (IM) – 1 dipendente su 5 utilizza un tool IM. Attraverso l'IM si possono trasmettere allegati e informazioni aziendali riservate non criptate, bypassando l'infrastruttura di sicurezza aziendale.

Streaming Media – Il 44% dei dipendenti utilizza applicazioni di streaming media durante l'orario di lavoro per scaricare audio e video. Tali contenuti utilizzano la banda trasmissiva in modo così intensivo da poter sottrarre notevole potenza di rete alle applicazioni aziendali business-critical.

Hacking a opera dei dipendenti – Negli ultimi 12 mesi, il 45% delle aziende ha rilevato accessi non autorizzati a file e risorse da parte di utenti interni. Gli strumenti di hacking sono sempre più facilmente disponibili su Internet, con il conseguente aumento dei rischi legati a possibili responsabilità legali e alla sicurezza derivanti dall'hacking a opera dei dipendenti.

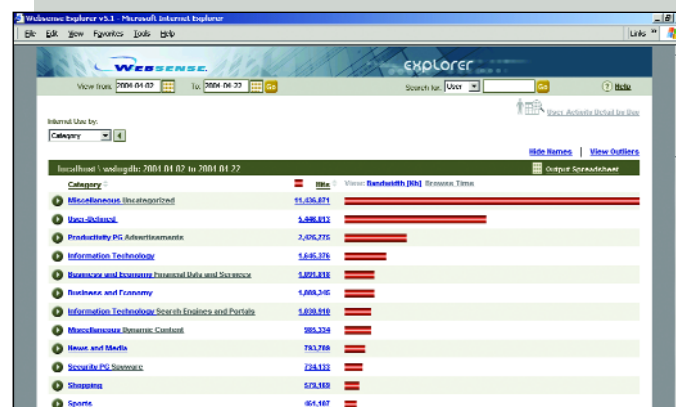
I rischi legati all'attività su Internet da parte dei dipendenti e all'accesso ad applicazioni non autorizzate sono in crescita e devono essere affrontati dai responsabili IT. Ma come può un amministratore di rete o un responsabile della sicurezza informatica sfruttare l'investimento sull'infrastruttura esistente per gestire in modo rapido ed efficace queste nuove minacce? Websense® ha la risposta.

Funzionalità di Websense Enterprise:

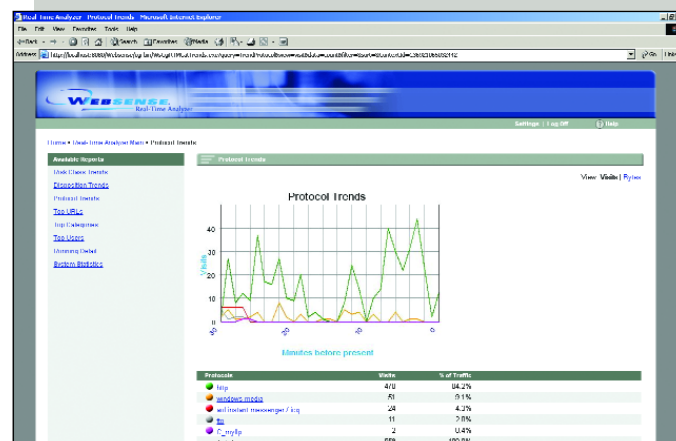
- La migliore funzionalità di Internet filtering, offerta dal leader del settore.
- Protezione da spyware, da siti di phishing e altre frodi, da siti "malicious" e hacking a opera di dipendenti.
- Gestione della capacità di banda.
- Gestione e analisi dell'utilizzo di instant messaging e peer-to-peer.

Vantaggi di Websense Enterprise:

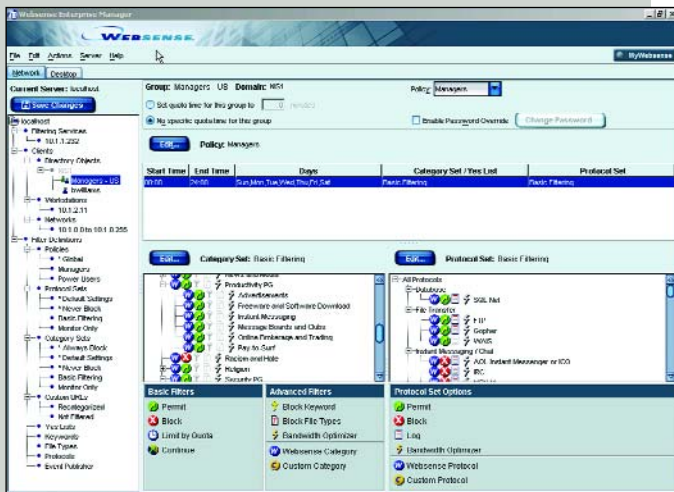
- Riduzione del rischio di minacce alla sicurezza.
- Aumento della produttività dei dipendenti.
- Riduzione dei rischi di responsabilità legali connessi al comportamento dei dipendenti.
- Ottimizzazione dell'uso delle risorse IT, compresi banda e desktop.
- Applicazione di policy sull'utilizzo delle applicazioni e di Internet.



Individuazione dei rischi per la sicurezza o dei problemi di produttività derivanti dall'attività Internet dei dipendenti in modo rapido e semplice grazie a Websense Enterprise Explorer.



Individuazione in tempo reale dei problemi sulla rete aziendale grazie a Websense Enterprise Real-Time Analyzer™.



Personalizzazione semplice delle policy per utenti e gruppi diversi con Websense Manager.

WEBSense ENTERPRISE, PROTEZIONE MULTILIVELLO DELLE RISORSE IT USATE DAI DIPENDENTI

Websense Enterprise è una soluzione completa, che affronta i rischi associati all'utilizzo di Internet e della rete aziendale da parte dei dipendenti.

Websense Enterprise consente di:

- Gestire l'accesso a Internet dei dipendenti
- Bloccare spyware, siti di phishing e MMC
- Impedire il file sharing peer-to-peer
- Gestire instant messaging e relativi allegati
- Gestire l'utilizzo di streaming media e di altre applicazioni a elevato consumo di banda
- Impedire l'hacking a opera dei dipendenti

Il Master Database di Websense

Il nucleo di Websense Enterprise è il Master Database.

Esso contiene i siti e i protocolli Web più frequentemente visitati, ed è il database più ampio, preciso e aggiornato nel settore della gestione dell'utilizzo di Internet da parte dei dipendenti.

Il Master Database contiene oltre 6 milioni di siti, classificati in più di 80 categorie, consentendo una maggiore personalizzazione delle policy sull'uso di Internet da parte delle aziende. Il Master Database include siti in più di 50 lingue, compreso inglese, francese, tedesco, spagnolo e giapponese.

La migliore funzionalità di Internet filtering

Websense Enterprise è la soluzione leader al mondo per la gestione dell'utilizzo di Internet da parte dei dipendenti, che combina potenza e flessibilità con sofisticate funzionalità.

- Offre una funzione di Internet filtering completa e accurata, supportata da un database di URL creato combinando classificazione automatica e umana e dinamicamente adattato ai modelli di navigazione reali, grazie a Websense WebCatcher™.
- Possibilità di bilanciare navigazione per scopi personali e lavorativi, consentendo agli amministratori IT di impostare policy personalizzate per la gestione dell'utilizzo della rete, di Internet e delle applicazioni da parte dei dipendenti.
- Riduzione al minimo del carico amministrativo grazie all'impostazione e all'applicazione delle policy relative all'uso delle risorse IT con uno strumento di facile utilizzo quale Websense Enterprise Manager.
- Fornisce modelli di report, pagine di blocco e categorie di pagine Web disponibili in dieci lingue: cinese (semplificato e tradizionale), inglese, francese, tedesco, italiano, giapponese, coreano, portoghese e spagnolo.

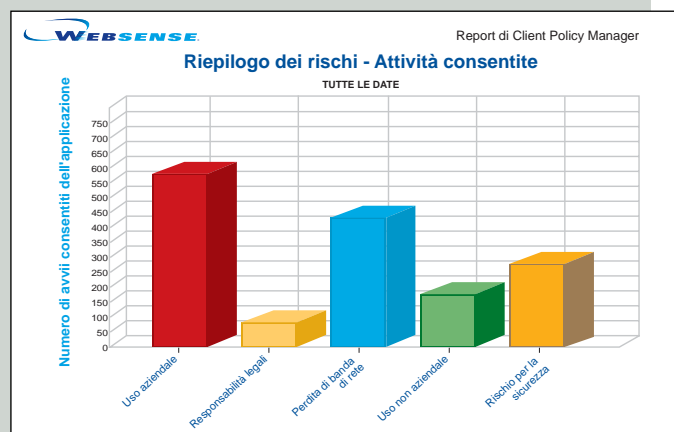
Funzioni di analisi e reportistica avanzate

Websense Enterprise fornisce le più avanzate funzioni di individuazione dei problemi di perdita di produttività e di rischi per la sicurezza associati all'utilizzo delle applicazioni e di Internet da parte dei dipendenti.

Nessun'altra soluzione offre una gamma così vasta di tool per l'isolamento e l'individuazione dei rischi:



Presentazione agli utenti finali di informazioni e messaggi personalizzabili.



Determinazione di rischi di potenziali responsabilità legali e rischi per banda, produttività e sicurezza all'interno dell'organizzazione, grazie a Risk Reports.



Websense Enterprise Real-Time Analyzer™ – Tool di analisi in tempo reale che consente di analizzare il traffico di rete recente e attuale, generando un rapporto istantaneo dell'attività in rete e rispondendo rapidamente ai relativi quesiti.

Websense Enterprise Explorer – Tool di analisi forense e reporting indirizzato a responsabili IT, delle risorse umane, legali e dirigenti d'azienda per un accesso rapido e immediato a statistiche sull'attività in rete dei dipendenti.

Websense Enterprise Reporter – È possibile scegliere tra oltre 80 modelli di report predefiniti grazie a questo motore basato su Crystal Reports®, che consente di personalizzare e programmare la distribuzione via e-mail dei report.

Robusta funzionalità di Internet filtering con Premium Groups™

La linea di prodotti Websense Enterprise Premium Groups™ (PG) migliora le funzionalità di filtering standard di Websense Enterprise con la copertura aggiuntiva di categorie ad alto rischio:

Websense Enterprise Security PG™

Riduzione al minimo dei rischi di indebolimento della sicurezza tramite il blocco dell'accesso a siti di phishing e altre frodi, a spyware e siti infettati da MCC. Blocco della trasmissione di informazioni riservate a host server spyware.

Websense Enterprise Productivity PG™

Per aumentare la produttività dei dipendenti tramite la gestione della navigazione su Internet a fini privati durante l'orario di lavoro (il cosiddetto "cyber-slacking"), per accedere a categorie quali pubblicità online, IM, freeware e siti pay-to-surf.

Websense Enterprise Bandwidth PG™

Aumento delle prestazioni della rete tramite la gestione dell'accesso a download ad elevato consumo di banda. Vengono filtrati, tra gli altri, i siti che offrono streaming media, radio e TV Internet e file sharing P2P.

Gestione della rete e ottimizzazione della banda

Websense Enterprise offre la capacità unica di ampliare il controllo e l'applicazione delle policy a livello di rete. Questo consente alle aziende:

- la gestione delle applicazioni di IM, P2P e streaming media in base ai protocolli di rete;
- l'impostazione di policy basate su protocolli applicativi e tipi di file con Dynamic Protocol Management™. Gli aggiornamenti automatici all'elenco dei protocolli assicurano precisione e riducono al minimo le attività di amministrazione.

Websense Enterprise Bandwidth Optimizer™ (BWO) – Con BWO, uno dei moduli aggiuntivi di Websense Enterprise, è possibile preservare la banda di rete disponibile, migliorandone l'uso. BWO si integra in modo trasparente con Websense Enterprise e consente alle aziende di dare la priorità alle attività business-critical rispetto alle operazioni non legate all'attività lavorativa. BWO blocca l'attività Internet per scopi personali o l'utilizzo delle applicazioni quando le soglie di capacità della banda di rete impostate dagli amministratori vengono superate.

Websense Enterprise IM Attachment Manager™ (IMA) – Per proteggere le aziende dalle minacce alla sicurezza derivanti dal trasferimento di file tramite i programmi di instant messaging. IMA si integra senza problemi nell'ambiente Websense Enterprise per consentire la massima flessibilità di gestione nell'utilizzo dell'instant messaging pubblico all'interno della vostra rete. Gli amministratori di rete possono impostare policy per bloccare l'invio e la ricezione di allegati, riducendo al minimo la possibilità di importare virus o worm trasmessi attraverso le applicazioni IM.

Integrazione trasparente per un'installazione rapida ed economica.

Websense Enterprise può essere distribuito in tre modi, a seconda dei requisiti della vostra rete: in configurazione integrata, incorporata o stand-alone. Le opzioni di distribuzione assicurano facilità di installazione e manutenzione, massimizzando al contempo scalabilità, prestazioni e supporto alle funzionalità.

Websense Enterprise è attualmente integrato/incorporato con:

- 3Com
- Lightspeed
- Blue Coat
- Microsoft
- Check Point
- Nokia
- Cisco
- Juniper Networks/NetScreen
- Crossbeam
- Network Appliance
- CyberGuard
- Novell Volera
- Dell
- ServGate
- F5
- SLMsoft
- Hewlett-Packard
- SonicWALL
- iMimic
- Squid
- Immunix
- Stratacache
- Infolibria
- Sun Microsystems
- Inktomi

Protezione immediata dalle minacce alla sicurezza ancora sconosciute con Websense® Client Policy Manager™ (CPM)

CPM offre protezione da tutte le emergenti minacce alla sicurezza, consentendo l'attuazione di policy per l'utilizzo delle applicazioni da parte dei dipendenti su desktop, notebook e server aziendali, grazie al suo esclusivo e completo database di applicazioni categorizzate. CPM blocca l'esecuzione di applicazioni non autorizzate come spyware, P2P e tool di hacking. Complementare ai firewall e antivirus tradizionali, CPM fornisce un importante componente attivo che chiude la porta all'esposizione alle attuali minacce alla sicurezza miste e in rapida evoluzione.

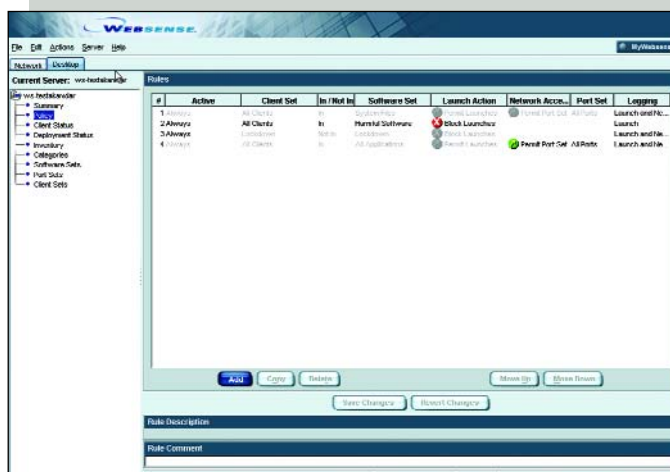
Requisiti di sistema di Websense Enterprise

Hardware:

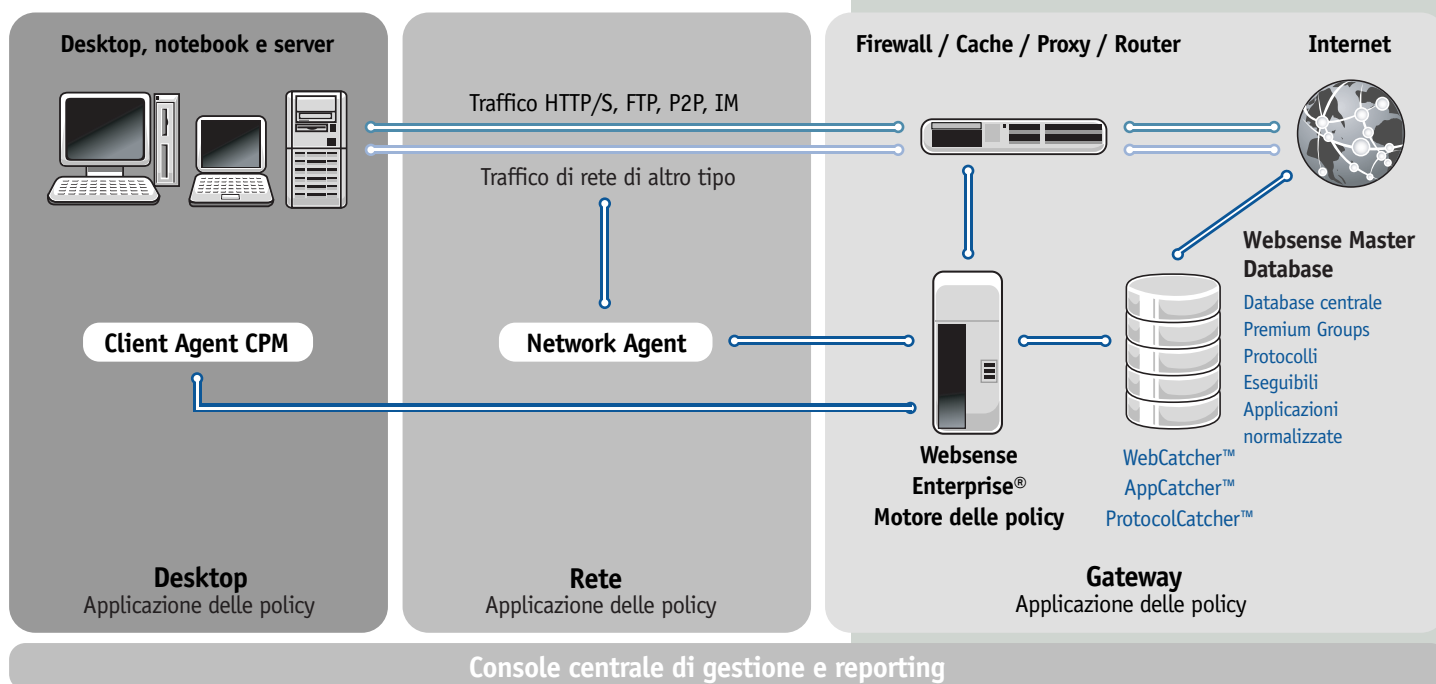
- Processore Pentium III o Sun Ultra 10 o superiore con almeno 512 MB di RAM disponibili. I requisiti hardware possono variare in base alla configurazione. Per ulteriori informazioni fare riferimento alla guida di implementazione.

Software:

- Microsoft® Windows® 2003 Server, Windows® 2000 Server (Service Pack 3 o superiore)
- Red Hat Linux™ 9 o Red Hat Enterprise Linux™ 3
- Sun Solaris™ 8-9



Applicazione di policy flessibili relative ad applicazioni malicious e non autorizzate mediante la console di gestione centrale.



Scaricate subito una versione di prova completa utilizzabile per 30 giorni all'indirizzo www.websense.com/downloads

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

Websense UK
Chertsey, England
Tel +44 (0)1932. 796001
www.websense.co.uk

Websense France
Paris, France
Tel +33 (0)15660. 5814
www.websense.fr

Websense Germany
Munich, Germany
Tel +49 (0)89 24445. 4005
www.websense.de

Websense Japan
Tokyo, Japan
Tel +813.5322.1335
www.websense.co.jp

Websense Australia
Sydney, Australia
Tel +61 2 9006. 1621
www.websense.com.au

Websense Greater China
Hong Kong
Tel +852.2855.8811
www.chinese.websense.com
www.prc.websense.com

Websense Latin America
Sao Paulo, Brazil
Tel +55.11.4612.0798
www.espanol.websense.com
www.portugues.websense.com