Le soluzioni di Web Filtering & Security di Websense®: Funzionalità & Benefici

Prodotti		Modulo/Funzionalità	Funzionalità	Benefici per i Clienti
VEDERE SUL RETRO I DETTAGLI SUGLI ADD-ON WEBSENSE CLIENT POLICY MANAGER & REMOTE FILTERTING				
Websense Web Security Suite™ -- Powered by Websense ThreatSeeker™ Web Threat Intelligence (vedi oltre)	Websense Enterprise® Security	Websense Enterprise	Aggiornamento giornaliero di un database che copre oltre 22 milioni di siti web e 96 protocolli, in oltre 50 lingue	Ottimizza l'uso di Internet da parte dei dipendenti mediante una semplice interfaccia di gestione.
			Gestione delle pagine web che riducono la produttività dei dipendenti, quali message board e club; advertising; download di software/freeware; Instant Messaging; trading on-line; siti a pagamento.	Migliora la produttività dei dipendenti gestendo l'accesso a questi siti.
			Gestione delle pagine web che riducono la banda disponibile, quali Internet radio e TV; P2P; siti di personal storage; telefonia Internet e streaming media.	Migliora l'utilizzo della banda gestendo l'accesso a questi siti.
		Reporter	Tool per l'analisi approfondita e programmata con possibilità di scegliere tra oltre 80 diversi report in vari formati: pdf, Excel, etc.	Aiuta a capire i trend di navigazione di un'organizzazione garantendo che la policy relativa all'utilizzo di Internet sia efficace. Sono disponibili report sia grafici sia analitici.
		Explorer	Tool di reporting web che offre una vista dinamica dei trend del traffico Internet per gruppi, dipartimenti o singoli.	Un portale web consente analisi istantanea delle modalità d'uso di Internet, a livello di dipartimento come di singolo utente, analizzando i trend, i rischi e le possibili falle nella sicurezza. Possibilità di interrogazioni ad hoc da parte di HR, Management e personale IT.
		Real-Time Analyzer™	Rappresentazione grafica dei trend della rete in tempo reale con refresh di default ogni 15 secondi.	Analisi istantanea dei più popolari siti web, degli utenti più attivi e dei protocolli ad alto consumo di banda.
		Dynamic Protocol Management™	Filtra 96 protocolli utilizzando oltre 15 categorie.	Consente all'IT di gestire protocolli quali P2P, streaming media e Instant Messaging.
		Dynamic Bandwidth Optimizer™	Ottimizza la disponibilità di banda gestendo il traffico di rete in tempo reale.	Limita il consumo della banda da parte delle applicazioni non critiche, con migliori prestazioni globali per l'azienda.
		WebCatcher™ & ProtocolCatcher™	Cattura in modo anonimo siti e protocolli non classificati girandoli a Websense per la classificazione.	Per classificare con precisione i siti non classificati acceduti dai dipendenti (Websense classifica siti in oltre 50 lingue).
		File Type Manager	Consente ai dipendenti di visualizzare pagine web prevenendo però il download di diversi tipi di file, quali audio, video, eseguibili, etc.	Gestisce le preziose risorse di banda e protegge da download non autorizzati.
		Keyword Search, Cache & Proxy Avoidance	Consente il search filtering in base a keyword. Websense filtra anche contenuti in cache, siti di traduzione, protocolli e siti Akamai e Proxy Avoidance.	Permette alle organizzazioni di attuare la policy interna sull'uso di Internet anche attraverso keyword search, translation web site, contenuti cache o Proxy Avoidance.
		Search Filtering (SafeSearch)	Applica filtri ai contenuti per soli adulti sui principali motori per la ricerca delle immagini, impiegando anche blocchi thumbnail aggiuntivi.	Previene dall'accesso indesiderato a materiali potenzialmente offensivi.
		Internet Watch Foundation Filtering	Consente alle aziende di prevenire l'accesso a siti con contenuti pedopornografici o ad altri siti ritenuti illegali dalla legge inglese come stabilito dalla Internet Watch Foundation.	Previene l'accesso a contenuti pedopornografici illegali
		Delegated Administration	Consente di gestire le policy tra dipartimenti, organizzazioni e server remoti con distribuzione centralizzata della configurazione.	Semplifica il controllo distribuito delle policy di sicurezza per una maggiore flessibilità nelle organizzazioni di grandi dimensioni o distribuite
		Delegated Reporting	Possibilità di consentire a specifici utenti di accedere ai tool di reporting web su specifici utenti o gruppi.	Accesso a informazioni sui rischi per la sicurezza e la produttività pertinenti alle specifiche responsabilità di ruolo, (es.: il Marketing Manager può vedere solo i report relativi al dipartimento Marketing).
		Auditing	Audit e review di tutte le modifiche alle policy Websense.	Miglioramento della capacità di monitorare le modifiche alla policy per il troubleshooting e le problematiche delle responsabilità legali
		SNMP Alerting	Possibilità di impostare livelli di threshold e di inviarli automaticamente ad altre infrastrutture di sicurezza via simple network management protocol (SNMP).	Possibilità di integrare e condividere le informazioni con i sistemi di Security Event Management e Identity Management accrescendone così il valore
		Anonymous Logging	Possibilità opzionale di mantenere l'anonimato per il logging delle attività.	Protezione della privacy dell'utente e, contemporaneamente, disponibilità di informazioni dettagliate su eventuali rischi potenziali derivati da un particolare uso di Internet
		Selective Logging	Possibilità opzionale di registrare le attività Internet solo per determinate categorie.	Riduzione dei costi hardware grazie alla diminuzione dell'utilizzo dello spazio disco, migliori prestazioni di reporting e viste semplificate sui rischi
		Security Filtering™	Websense effettua la scansione di oltre 600 milioni di siti web la settimana alla ricerca di bot network, codice maligno, spyware, phishing e pagine che ospitano software potenzialmente indesiderato e che vengono bloccate. Evita inoltre che le applicazioni spyware esistenti trasmettano informazioni a qualcuno.	Protezione di organizzazioni e dipendenti dal codice maligno originato sul web e dal crimeware (virus, Trojan, worm, keylogger, bot, etc.), perdita di informazioni confidenziali e accesso a pagine web fraudolente
		Malicious Traffic Management	Consente l'individuazione e la prevenzione di protocolli di traffico di rete maligni generati da applicazioni quali bot, worm e-mail e altre.	Fornisce un livello di protezione aggiuntivo contro i sempre più sofisticati crimeware e malware, comprendenti bot, worm via email, spyware e altro software maligno di nuova generazione.
		Websense Web Protection Services™	SiteWatcher™: Websense informa i clienti nel caso in cui il loro sito sia stato infettato da codice maligno o spyware.	Fornisce allarmi di sicurezza tempestivi in modo che l'IT possa agire subito per proteggere l'organizzazione e i visitatori del sito aziendale
			BrandWatcher™: Websense avvisa i clienti nel caso in cui il loro sito web o marchio siano stati presi di mira da un attacco di phishing o keylogging.	Fornisce allarmi di sicurezza tempestivi in modo che l'IT possa agire subito per proteggere organizzazione e clienti nel caso in cui il sito aziendale sia stato copiato per scopi fraudolenti
			ThreatWatcher™: Websense consente ai clienti una "vista da hacker" sui propri web server, mediante una regolare scansione di vulnerabilità note e minacce potenziali.	Fornisce report dettagliati sulle vulnerabilità del web server, sui livelli di rischio e sui rimedi possibili per aiutare i clienti a prevenire gli attacchi
		Real-Time Security Updates	Un database di sicurezza del cliente cerca automaticamente ogni 5 minuti gli aggiornamenti su nuovo codice maligno, spyware o pagine di phishing.	Riduce il rischio di infezioni da spyware, codice maligno, keylogger o accesso a pagine di phishing, grazie ad aggiornamenti in tempo reale
		IM Attachment Manager™	Blocca gli allegati delle applicazioni di Instant Messaging.	Permette alle organizzazioni di usare le applicazioni di Instant Messaging senza rischio di infezioni a causa di allegati pericolosi

Prodotti	Modulo/Funzionalità	Funzionalità	Benefici per i Clienti
Websense Client Policy Manager™ (CPM)	Client Policy Manager	Definisce quale tipo di applicazione può essere eseguita sui computer (desktop, notebook e server). Gestisce la sicurezza dei desktop da una console centralizzata con un database aggiornato quotidianamente che copre oltre 2,1 milioni di applicazioni organizzate in oltre 50 categorie (escluse quelle miscellanea).	Le applicazioni maligne o indesiderate sui PC sono controllate da CPM. Le sue policy rimangono attive anche quando offline, capacità fondamentale per la protezione dei notebook. Individua, analizza e offre protezione preventiva da minacce alla sicurezza note e sconosciute
	Remote Filtering	Consente l'applicazione di policy sull'uso di Internet a utenti esterni alla rete aziendale senza necessità di collegamento VPN	Previene l'esposizione a siti maligni e materiali inappropriati e l'introduzione di software maligno nella rete aziendale da parte di personale remoto quali telelavoratori, commerciali che lavorano sul campo, dipendenti in viaggio, ecc.
	Removable Media Control	Impedisce che dispositivi quali drive flash, masterizzatori CD/DVD, floppy drive, dispositivi riscrivibili e hard drive esterni siano utilizzati con i PC	Riduce i rischi per la sicurezza e la responsabilità legale connessi ai media remoovibili
	Application Control	Permette l'esecuzione solo delle applicazioni autorizzate	Riduce I rischi per la sicurezza prevenendo il lancio di applicazioni potenzialmente maligne
	Network Control	Blocca l'accesso delle applicazioni a specifici protocolli e porte tramite la rete	Evita che minacce alla sicurezza note e sconosciute si propaghino attraverso la rete
	Express Control	Impedisce istantaneamente l'esecuzione di nuove applicazioni	Blocca immediatamente attacchi quali keylogger, Trojan, worm e altri codici maligni
	Microsoft® Windows® XP Firewall Integration	Gestione semplificata e unificata e sincronizzazione delle policy CPM e Microsoft Firewall	Sfrutta l'esperienza di Websense in material di policy e classificazione per aggiungere gestione dei contenuti e controllo dei firewall, massimizzando la sicurezza e fornendo ulteriore valore
	CPM Explorer	Tool di reporting web che fornisce una vista dinamica dell'utilizzo delle applicazioni per gruppi, dipartimenti o singoli	Il portale web consente analisi istantanea dell'uso di ogni applicazione, dai dipartimenti fino al singolo utente, analizzando trend, rischi e vulnerabilità. Possibilità di interrogazioni ad hoc da parte di HR, Management e personale IT.
	CPM Reporter	Tool per l'analisi programmata e approfondita con possibilità di scegliere tra 80 diversi tipi di report in vari formati: pdf, Excel, etc., oltre a inventari software e hardware.	Inventario hardware e software completo (applicazioni installate o eseguite) per garantire l'efficace attuazione delle policy d'uso all'interno dell'organizzazione. Disponibilità di report grafici e analitici
	AppCatcher™	Indirizza automaticamente in forma anonima a Websense ogni applicazione sconosciuta perché venga classificata	Accurata classificazione delle applicazioni non classificate accedute dai dipendenti

Moduli Websense aggiuntivi a completamento di Websense Enterprise & Websense Web Security Suite

Add-On	Modulo/Funzionalità	Funzionalità	Benefici per i Clienti
Remote Filtering	Remote Filtering	Permette l'applicazione di policy sull'uso di Internet a utenti esterni alla rete aziendale senza necessità di collegamento VPN. (Nota: il Remote Filtering oltre ad essere incluso come funzionalitá all'interno di CPM, puó essere acquistato come add-on delle soluzioni Websense Enterprise Security o Websense Web Security	Previene l'esposizione a siti maligni e materiali inappropriati e l'introduzione di software maligno nella rete aziendale da parte di personale remoto quale telelavoratori, commerciali che lavorano sul campo, dipendenti in viaggio, ecc.

Websense ThreatSeeker™

Websense Web Security Suite sfrutta l'innovativa tecnologia Websense ThreatSeeker. Websense ThreatSeeker offre protezione preventiva dalle minacce del web spesso trascurate o dalle quali è troppo costoso proteggersi in modo preventivo usando le tecnologie per la sicurezza tradizionali. A differenza di questi approcci, Websense scova le minacce su Internet prima che I clienti ne siano colpiti e li protegge prima che patch e firme dei virus siano disponibili.

Websense ThreatSeeker usa oltre 100 procedure e sistemi proprietari per decifrare le minacce emergenti e complesse e sfrutta un insieme di speciali algoritmi matematici, profilazione dei comportamenti, analisi del codice e un'estesa rete di macchine che eseguono il data mining. Componente fondante di tutti i prodotti per la sicurezza di Websense, Websense ThreatSeeker offre intelligence ininterrotta delle minacce e protezione automatica dei clienti nel giro di pochi minuti.

Per ulteriori informazioni sul questo robusto approccio alla sicurezza: www.websense.com/threatseeker