

COMPOSIZIONE WEBSense WEB SECURITY SUITE

WebSense Web Security Suite	Componenti di Base	<p>WebSense Enterprise (WSE): Tramite questo modulo è possibile gestire l'accesso ai siti sfruttando le potenzialità di "content filtering" del software. WSE si appoggia su un database che categorizza URL e protocolli, e ad oggi contiene 10 milioni di siti, a cui corrispondono 2,5 miliardi di pagine Web. Il WebSense Master Database rappresenta il database più completo al mondo per la categorizzazione del web. I siti sono categorizzati in 90 categorie, è così possibile un'avanzata customizzazione delle policy di sicurezza per le diverse utenze. Mediamente ogni settimana vengono aggiunti circa 25000 siti grazie ad un componente, il Webcatcher, che si occupa per ogni installazione di inviare anonimamente ai server centrali tutto ciò che non è categorizzato così da ottenere ad ogni aggiornamento del database tutte le ricategorizzazioni generate dalle richieste in tutto il mondo. Inoltre ogni aggiornamento è depurato di tutti quei siti che non sono più attivi.</p>
		<p>Network Agent: È la sonda capace di "sniffing" del traffico internet di cui si vuole gestire la navigazione.</p>
		<p>Real Time Analyzer: Componente Web based di reporting in tempo reale, per una visione estemporanea di ciò che sta succedendo in rete.</p>
		<p>Explorer: Componente Web Based di reporting sui dati consolidati; consente un'analisi drill down sulle dimensioni di analisi come per esempio classi di rischio, protocolli, categorie.</p>
		<p>Reporter: È la componente basata su Crystal Report per gestione, scheduling e personalizzazione di report complessi sui dati consolidati.</p>
	Security, Moduli e Servizi	<p>Security PG: E' la componente di database per bloccare l'accesso dell'utente ai siti di phishing, pharming, spyware e a quelli infetti da MMC (mobile malicious code).</p>
		<p>Instant Messanging Attachment (IMA): Questo modulo gestisce l'invio e la ricezione di file attraverso i client di Instant Messaging. La necessità nasce dal fatto che gli allegati trasmessi tramite IM non vengono analizzati dai normali strumenti antivirus presenti in rete ma possono essere recapitati liberamente aprendo quindi le porte ad una possibile infezione virale.</p>
		<p>Real TimeUpdate (RTU): Il modulo RTU, relativo cioè al Real Time Update, consente al WebSense Master</p>

		Database di avere un aggiornamento ulteriore a quello giornaliero così da essere sempre arricchito delle nuove categorizzazioni e dei nuovi siti che costituiscono una minaccia per la navigazione, in tempo reale: i siti più pericolosi, specialmente quelli contenenti codice malizioso mobile, devono essere subito tracciati e comunicati così da avere una protezione in tempo reale efficace.
	Componenti per Produttività e Ottimizzazione	Productivity PG: E' la componente di database indispensabile per frenare il fenomeno del cosiddetto "cyber-slacking", ovvero la navigazione su Internet per scopi privati, per accedere a siti di pubblicità online, IM (instant messaging), freeware e siti pay-to-surf.
		Bandwith PG: deve essere impiegato per cautelare l'occupazione di banda da scopi non aziendali, significa avere la possibilità di inibire la navigazione verso siti di streaming media, radio, TV Internet e file sharing P2P.
		Bandwidth Optimizer (BWO): È lo strumento che permette di stabilire le priorità sul tipo di accesso alla risorsa banda per prediligere le attività business-critical a discapito di quelle non legate all'attività professionale. La discriminazione può avvenire secondo due modalità: <ul style="list-style-type: none"> • Soglia in uscita: le nuove richieste di banda vengono rifiutate quando il traffico totale in uscita supera il livello stabilito. • Soglia per applicazione: le nuove richieste per un'applicazione specifica vengono rifiutate quando la banda totale utilizzata per tale applicazione supera la soglia stabilita.
	Servizi dei Web Security Labs	Site Watcher: È un servizio che consente di avvisare le aziende nel caso in cui il loro sito sia stato infettato da codice maligno. Consente alla aziende di prendere contromisure immediate per evitare la diffusione del codice maligno a chi visita il sito. I Websense Security Labs esaminano quotidianamente i siti aziendali degli utenti registrati al servizio e mandano delle notifiche in caso di pericolo.
		Brand Watcher: Avvisa le aziende nel caso in cui il loro sito o marchio sia stato coinvolto in un attacco di phishing, pharming o keylogging. Ai clienti vengono forniti dettagli sugli attacchi e altre informazioni di interesse per la sicurezza: i Websense Security Labs sono ininterrottamente a caccia di phishing, pharming, frodi e codici maligni, quando individuano un attacco perpetrato ai danni di un marchio registrato, ne inviano notifica (completa di tutte le relative informazioni utili) agli utenti registrati.

 Websense Web Security Suite Lockdown	Desktop Protection	<p>CPM: Tramite questo modulo è possibile gestire l'esecuzione delle applicazioni sui singoli client (Workstation, laptop o server) sui quali è deployato in modo centralizzato un agent che regola le applicazioni con delle policy diversificate per quando la macchina è connessa alla rete o per quando è disconnessa. CPM si appoggia sul Websense Master Database che categorizza le applicazioni e ad oggi contiene 700000 eseguibili catalogati in oltre 50 categorie.</p> <p>Il componente Appcatcher si occupa per ogni installazione di inviare anonimamente ai server centrali tutto ciò che non è categorizzato così da ottenere ad ogni aggiornamento del database tutte le ricategorizzazioni generate dalle richieste in tutto il mondo. È possibile con il CPM generare da remoto un Inventory Hardware e Software per poi applicare delle politiche di Lockdown, in modo da inibire sui client remoti l'esecuzione di qualsiasi codice che non sia censito nell'inventory software inizialmente creato.</p> <p>È garantito il blocco dell'esecuzione di applicazioni non autorizzate, quali spyware, peer-to-peer (P2P) e tool di hacking sul desktop permettendo nel contempo una gestione flessibile delle policy relative alle altre applicazioni, che solo utenti o gruppi di utenti specificati possono utilizzare. È lo strumento dedicato alla sicurezza completa per l'elaborazione mobile.</p>
		<p>Real Time Analyzer: Componente Web based di reporting in tempo reale, per una visione estemporanea di ciò che sta succedendo in rete in termini di esecuzioni di applicazioni.</p>
		<p>Explorer: Componente Web Based di reporting sui dati consolidati. Consente un'analisi drill down sulle dimensioni di analisi come per esempio classi di rischio, applicazioni, categorie.</p>
		<p>Reporter: È la componente basata su Crystal Report per gestione, scheduling e personalizzazione di report complessi sui dati consolidati.</p>
		<p>Real TimeUpdate: Il modulo RTU, relativo cioè al Real Time Update, consente al websense Master Database di avere un aggiornamento ulteriore a quello giornaliero così da essere sempre arricchito delle nuove applicazioni che costituiscono una minaccia per la rete, in tempo reale</p>

Websense Web Security Suite Basic:

Componenti di Base + Security, Moduli e Servizi (Security PG, IMA, RTU) + Servizi di Web Security Labs (Site Watcher, BrandWatcher)

Websense Web Security Suite Extended:

Websense Web Security Suite Basic + Componenti per Produttività e Ottimizzazione (Productivity PG, Bandwidth PG, Bandwidth Optimizer)

Websense Web Security Suite Lockdown:

Websense Web Security Suite Basic + Desktop Protection

Websense Web Security Suite Lockdown Extended:

Websense Web Security Suite Lockdown + Componenti per Produttività e Ottimizzazione (Productivity PG, Bandwidth PG, Bandwidth Optimizer)