



Websense Enterprise® Client Policy Manager™ (CPM) offre una protezione immediata dalle minacce alla sicurezza ancora sconosciute e impedisce l'esecuzione di applicazioni non autorizzate. CPM consente l'attuazione di policy relative all'utilizzo delle applicazioni da parte dei dipendenti su desktop, notebook e server aziendali, grazie al suo esclusivo e completo database di applicazioni divise per categorie quotidianamente aggiornate. 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.

Le risorse di elaborazione attualmente a disposizione dei dipendenti comprendono potenti applicazioni Internet e possibilità di download che spesso introducono nuovi rischi per la sicurezza delle risorse IT aziendali. Al crescere della mobilità della postazione di lavoro, i dipendenti sempre più spesso portano a casa e in viaggio il proprio computer. Quando si ricollegano alla rete aziendale, però, rischiano di infettarla con malware. Le aziende hanno la necessità di essere protette da minacce alla sicurezza note e sconosciute rilevando le minacce ai desktop e i tentativi di utilizzare applicazioni non autorizzate. CPM può impedire che le applicazioni non autorizzate vengano eseguite o accedano alla rete e aiutare le aziende ad applicare e gestire le policy per l'uso delle applicazioni per categorie, utenti o gruppi.

## La soluzione Websense Client Policy Manager

Websense Client Policy Manager è un'innovativa soluzione di sicurezza che estende le funzionalità di Websense Enterprise a desktop, notebook e server aziendali. CPM offre una protezione immediata dalle minacce sconosciute, compresi i moderni e sofisticati malware, impedendone la diffusione in rete. CPM blocca l'esecuzione di applicazioni non autorizzate quali spyware, file sharing P2P e tool di hacking. CPM offre una gestione flessibile delle policy per diverse categorie di applicazioni: per gli strumenti di accesso remoto come per le applicazioni individuali quali AOL® Instant Messenger. Tramite l'integrazione con i servizi di directory Websense, queste policy possono essere implementate a livello di gruppo oppure personalizzate in base alle esigenze dei singoli.

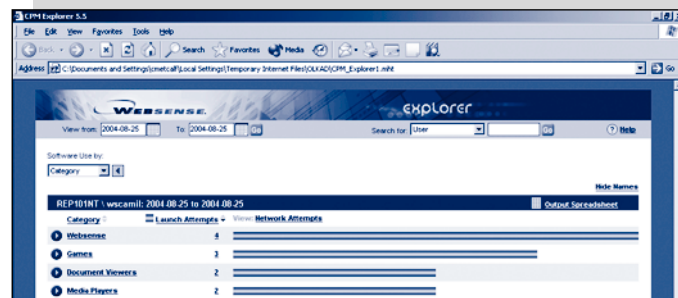
Complementare ai firewall e antivirus tradizionali, CPM chiude la porta all'esposizione alle minacce sconosciute, che spesso mettono in ginocchio le reti prima che le nuove firme dei virus o le patch appropriate possano essere distribuite o quando i sistemi di sicurezza non sono configurati correttamente. Solo CPM consente un rilevamento efficace e attivo delle minacce e un'applicazione flessibile delle policy relative all'utilizzo delle applicazioni, offrendo alle aziende i seguenti vantaggi:

- **Maggiore sicurezza desktop/notebook** – Blocca la diffusione di malware all'interno dell'azienda, a garanzia del massimo uptime di applicazioni e rete.
- **Aumento della produttività dei dipendenti** – Consente alle aziende di impostare policy appropriate relative all'utilizzo delle applicazioni, ottimizzando i livelli di produttività.
- **Riduzione dei costi di gestione dei desktop** – Aiuta a ridurre i costi relativi ai servizi di help desk e amministrazione dei desktop, eliminando le incompatibilità software e le conseguenti chiamate all'help desk.

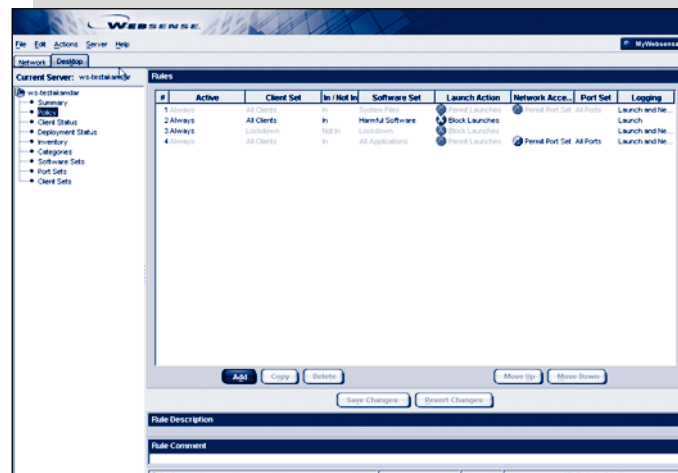
## Websense® Client Policy Manager™

### I vantaggi di Websense® Client Policy Manager

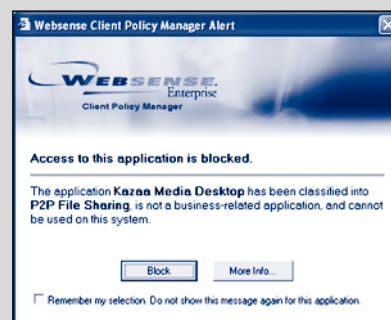
- Protezione attiva immediata dalle minacce sconosciute.
- Rilevamento e analisi delle minacce alla sicurezza dei desktop e dell'attività delle applicazioni.
- Applicazione di policy flessibili e automaticamente aggiornabili per l'utilizzo delle applicazioni da parte di singoli utenti e gruppi.



Rilevamento dei rischi per la sicurezza e dei problemi di produttività legati all'utilizzo delle applicazioni da parte dei dipendenti in modo rapido e semplice con Explorer per CPM.



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



Avvertimento agli utenti finali in caso di tentativo di avvio di eseguibili non sicuri o applicazioni non autorizzate.

## Funzionalità e vantaggi

### Protezione attiva immediata dalle minacce sconosciute

CPM offre un nuovo e importante livello di sicurezza per gestire vulnerabilità non ancora note.

- **WebSense® Network Lockdown™** – Per una protezione attiva immediata dalle minacce sconosciute bloccando l'accesso a porte e protocolli specifici per categoria di applicazione.
- **WebSense® Application Lockdown™** – Per il massimo controllo sugli ambienti desktop consentendo l'esecuzione su PC e server aziendali solo delle applicazioni autorizzate, impedendo così il lancio di applicazioni sconosciute e potenzialmente dannose.
- **Modalità "outbreak"** – Per migliorare l'infrastruttura di sicurezza aziendale quando è più necessario, ovvero durante un attacco di virus e prima che patch e aggiornamenti anti-virus siano disponibili. Blocca l'avvio di specifici malware consentendo ai responsabili IT di applicare in tempo reale le policy ai PC.

### Rilevamento e analisi delle minacce alla sicurezza dei desktop e dell'attività delle applicazioni

CPM fornisce una sofisticata funzione di rilevamento delle minacce ai desktop, notebook e server aziendali.

- **Explorer per CPM** – Consente di rilevare le potenziali minacce alla sicurezza e l'utilizzo improprio del software mediante un'interfaccia browser interattiva e funzionante con un semplice clic del mouse. Questo dinamico strumento di analisi forense e generazione di report fornisce ai responsabili aziendali la possibilità di ottenere report sull'utilizzo delle applicazioni e i tentativi di accesso alla rete per dipendente, reparto, data e categoria dell'applicazione.
- **CPM Reporter** – Consente di programmare la distribuzione automatica "out-of-the-box" di report basati su browser e personalizzabili, comprendenti inventari dei desktop, lanci delle applicazioni, classificazioni dei software, storico dell'utilizzo delle applicazioni e profili sui rischi dell'azienda.
- **Inventory Manager** – Per eseguire inventari hardware e software che forniscano viste classificate e normalizzate di programmi e applicazioni, consentendo il tempestivo rilevamento delle minacce e l'individuazione di potenziali vulnerabilità delle applicazioni.

### Applicazione di policy d'uso flessibili e automaticamente aggiornabili

CPM consente agli utenti di applicare policy aggiornate relative all'uso delle applicazioni, riducendo al minimo di oneri di amministrazione.

- **Database delle applicazioni** – Classifica le applicazioni all'interno del WebSense® Master Database, consentendo l'attuazione di policy flessibili e impostabili per singoli utenti, gruppi e, soprattutto, categorie, utilizzando la nostra completa metodologia per la classificazione di migliaia di applicazioni in oltre 50 categorie.
- **WebSense AppCatcher™ e ProtocolCatcher™** – Inoltra in modo automatico e anonimo a WebSense Master Database qualsiasi applicazione sconosciuta e il suo comportamento in rete, per mantenere le policy sempre aggiornate.

### Integrazione trasparente con l'infrastruttura IT esistente

CPM facilita la gestione dei PC aziendali e l'attuazione di policy adeguate per l'uso delle applicazioni da parte degli utenti finali.

- **Distribuzione automatica degli agenti desktop** – Per distribuire gli agenti CPM sui desktop aziendali, singolarmente o in gruppo, con un semplice clic su un pulsante all'interno dell'ambiente WebSense Manager.
- **Integrazione trasparente con WebSense Enterprise** – Integrazione diretta con WebSense Manager, che gestisce l'utilizzo degli strumenti informatici da parte dei dipendenti a livello di gateway, rete e desktop, senza nuove interfacce da imparare a usare o console da distribuire.
- **Integrazione con i servizi di directory** – Per consentire agli amministratori IT di personalizzare le policy in base alle esistenti definizioni di utenti e gruppi in rete. Interagisce con l'infrastruttura esistente e si integra con i più diffusi servizi di directory.

## Requisiti di sistema di WebSense Enterprise

### Server CPM

**Hardware:** Processore Pentium III 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.

**Sistemi operativi supportati:** Microsoft® Windows® 2003 Server, Windows® 2000 Server (Service Pack 3 o superiore).

### Client CPM

**Hardware:** Il client CPM supporta la maggior parte delle configurazioni desktop. Per ulteriori informazioni fare riferimento alla guida di implementazione.

**Sistemi operativi supportati:** Microsoft® Windows® XP (Service Pack 1 o superiore), Windows® 2003 Server, Windows® 2000 Pro/Server/Advanced Server (Service Pack 3 o superiore), Windows® NT 4 Server (Service Pack 6a o superiore), oppure Windows® 98 SE.



Console di gestione e reporting centrale

Scaricate subito una versione di prova completa utilizzabile per 30 giorni all'indirizzo [www.websense.com/downloads](http://www.websense.com/downloads)

WebSense Inc.  
San Diego, CA USA  
Tel 800.723.1166  
Tel 858.320.8000  
[www.websense.com](http://www.websense.com)

WebSense UK  
Chertsey, England  
Tel +44 (0)1932. 796001  
[www.websense.co.uk](http://www.websense.co.uk)

WebSense France  
Paris, France  
Tel +33 (0)15660. 5814  
[www.websense.fr](http://www.websense.fr)

WebSense Germany  
Munich, Germany  
Tel +49 (0)89 24445. 4005  
[www.websense.de](http://www.websense.de)

WebSense Japan  
Tokyo, Japan  
Tel +81.5322.1335  
[www.websense.co.jp](http://www.websense.co.jp)

WebSense Australia  
Sydney, Australia  
Tel +61 2 9006. 1621  
[www.websense.com.au](http://www.websense.com.au)

WebSense Greater China  
Hong Kong  
Tel +852.2855.8811  
[www.chinese.websense.com](http://www.chinese.websense.com)  
[www.prc.websense.com](http://www.prc.websense.com)

WebSense Latin America  
Sao Paulo, Brazil  
Tel +55.11.4612.0798  
[www.espanol.websense.com](http://www.espanol.websense.com)  
[www.portugues.websense.com](http://www.portugues.websense.com)