

WEBSense CLIENT POLICY MANAGER



WebSense® Client Policy Manager™ (CPM) offre una soluzione di protezione degli endpoint completa per desktop, notebook e server in grado di proteggere in modo efficace le aziende dalle minacce alla sicurezza note e sconosciute.

CPM impedisce l'installazione e l'esecuzione di applicazioni non autorizzate e consente l'attuazione di policy relative all'utilizzo delle applicazioni grazie al suo completo database di applicazioni divise per categorie, aggiornato quotidianamente. Grazie al controllo delle applicazioni, CPM offre un'alternativa semplice da implementare, a basso rischio e altamente efficiente rispetto ai complicati sistemi Host Intrusion Prevention Systems (HIPS) basati sul comportamento. La copertura completa sia di applicazioni "whitelist" (consentite) che "blacklist" (nocive) consente la creazione di policy per un'applicazione granulare, dinamica e altamente flessibile. CPM è complementare alle soluzioni antivirus e firewall dei desktop e blocca le attuali minacce alla sicurezza miste e in rapida evoluzione.

Blocco degli attacchi

CPM fornisce un'immediata "prima linea di difesa" attiva: la protezione inizia e si arresta sugli endpoint.

- Consente la conoscenza delle applicazioni e l'attuazione di policy a livello di endpoint, così da bloccare il software maligno assicurando al tempo stesso conformità e produttività.
- Impedisce alle applicazioni maligne di modificare le impostazioni del registro e tiene traccia delle attività di registro sospette.
- Protegge gli utenti remoti e mobili quando operano all'esterno della rete aziendale o che non dispongono di aggiornamenti standard di sicurezza o di patch.
- Protegge gli utenti remoti e mobili da minacce e rischi di conformità legati all'accesso al Web e ai contenuti degli URL.
- Opera avvalendosi della tecnologia Network Access Control (NAC) per l'applicazione di policy di sicurezza ai dispositivi che tentano di accedere alla rete, negando l'accesso agli endpoint non conformi.
- Attraverso le integrazioni consente protezione a livello di rete dalle minacce in arrivo e crea firewall dinamici application-aware.
- Offre livelli multipli di controllo per impedire l'avvio o ridurre la diffusione di attacchi alla sicurezza:
 - Per il massimo controllo degli endpoint, consentendo l'esecuzione solo delle applicazioni autorizzate e impedendo così l'avvio di applicazioni potenzialmente dannose e indesiderate.
 - Consente di bloccare l'accesso delle applicazioni di rete a porte e a protocolli specifici per categoria di applicazione, impedendo la diffusione di software dannoso o le comunicazioni non autorizzate in uscita.
 - Consente agli amministratori di sistema di prevenire gli attacchi e le vulnerabilità, proteggendo con tempestività le configurazioni degli endpoint in modo da arrestare l'esecuzione di qualsiasi nuovo software che potrebbe risultare inappropriato, dannoso o che cerca di infettare le vulnerabilità dei sistemi operativi o delle applicazioni appena rilasciati.

Controllo sull'utilizzo delle applicazioni desktop

CPM esegue l'inventario delle applicazioni installate sui PC degli utenti e consente di ridurre le chiamate ai servizi di help desk dovute all'utilizzo non autorizzato delle applicazioni:

- Consente l'applicazione di policy flessibili e automaticamente aggiornabili sull'utilizzo delle applicazioni in grado di proteggere gli utenti finali dal software dannoso e indesiderato.
- Impedisce l'installazione e l'esecuzione di applicazioni non autorizzate.

CPM comprende tool di reporting avanzati che consentono di:

- Stabilire i profili sui rischi dell'azienda.
- Rilevare la presenza e la localizzazione sulla rete aziendale di malicious mobile code (MMC), spyware, strumenti di hacking o di altri rischi per la sicurezza presenti su ciascun computer e server.
- Eseguire importanti valutazioni del software che forniscono viste classificate e normalizzate di programmi e applicazioni.
- Agevolare il tempestivo rilevamento delle minacce e l'individuazione di potenziali vulnerabilità nelle applicazioni.

Tutela delle informazioni

CPM offre un ulteriore livello di controllo dei dati a livello endpoint, bloccando la potenziale sottrazione di informazioni personali o le violazioni alla proprietà intellettuale effettuati tramite i supporti rimovibili o le comunicazioni di rete.

- Consente agli amministratori di sistema di impedire l'utilizzo di dispositivi come unità flash, masterizzatori CD/DVD, unità floppy e hard disk esterni sulle workstation client, riducendo in tal modo il rischio di introduzione di software dannoso all'interno dell'azienda. Le aziende possono anche decidere di bloccare l'utilizzo dei supporti scrivibili, a seconda delle policy definite.

Funzionamento semplificato

CPM consente di ridurre la difficoltà nell'installazione e gestione di una soluzione di protezione degli endpoint:

- Si integra con i principali servizi di directory per creare policy in base a utenti e gruppi.
- Si integra con Windows® Firewall in Microsoft® Windows XP Service Pack 2 (SP2) così da semplificare la gestione del firewall ed automatizzare le eccezioni nei programmi, attraverso la consapevolezza delle applicazioni e delle porte in uso.

Estensione della protezione agli utenti remoti e mobili

Le funzionalità di filtraggio remoto di CPM consentono alle aziende di applicare le stesse policy di Web filtering di Websense Enterprise® o di Websense Web Security Suite™ agli uffici remoti e agli utenti mobili che utilizzano i notebook all'esterno della rete aziendale, per garantire protezione dai siti Web maligni o inappropriati.

CPM: realizzato con la tecnologia innovativa Websense ThreatSeeker™

La tecnologia Websense ThreatSeeker offre protezione preventiva dalle minacce alla sicurezza via Web, minacce solitamente non rilevate o troppo costose da bloccare con l'impiego delle tecnologie di protezione tradizionali. A differenza di queste soluzioni, Websense scova le minacce su Internet prima che i clienti possano essere compromessi e garantisce protezione prima che nuove patch e firme siano create.

Websense ThreatSeeker utilizza oltre 100 procedure e sistemi proprietari per decifrare minacce emergenti e complesse e viene eseguito utilizzando una combinazione di algoritmi matematici, profiling comportamentale, analisi del codice, servendosi di una rete estesa di computer per il data mining. Websense ThreatSeeker, alla base di ogni prodotto per la sicurezza Websense, offre informazioni riservate sulle minacce in corso e fornisce protezione automatica ai clienti nell'arco di pochi minuti.

Websense Web Security Ecosystem™

Il Web Security Ecosystem di Websense è un framework completo di integrazioni tecnologiche, il quale offre protezione avanzata e facilità di installazione delle soluzioni di Web security Websense all'interno degli ambienti aziendali. Questa iniziativa si integra con le tecnologie di protezione e di networking a livello mondiale compresi: i gateway Internet, le soluzioni per il controllo degli accessi alla rete, la gestione degli eventi di sicurezza, la gestione delle identità e gli appliance. Il Web Security Ecosystem di Websense, grazie all'integrazione con oltre 40 diverse soluzioni tecnologiche, aiuta le aziende ad individuare e a ridurre le minacce e le vulnerabilità via Web.

Requisiti di sistema

Client Policy Manager server

- Microsoft Windows Server® 2003 Standard Edition o Enterprise Edition, o le stesse versioni con SP1
- Microsoft Windows 2000 Server con SP3 o versioni successive

Client Policy Manager e client di filtraggio remoto

- Microsoft Windows XP Professional con SP1 o SP2
- Microsoft Windows Server 2003 Standard Edition o Enterprise Edition con SP1
- Microsoft Windows 2000 Professional, Server o Advanced Server con SP3 o SP4

Server di filtraggio remoto

- Microsoft Windows Server 2003 Standard Edition o Enterprise Edition, o le stesse versioni con SP1
- Microsoft Windows 2000 Server con SP3 o versioni successive
- Red Hat® Enterprise Linux® 3 o 4: AS, ES o WS, o Red Hat Linux 9
- Sun® Solaris™ 9 o 10

Riepilogo

CPM protegge i computer sia all'interno che all'esterno della rete aziendale rilevando e analizzando le minacce alla sicurezza degli endpoint e l'attività delle applicazioni e attuando policy flessibili, scalabili e automaticamente aggiornabili sull'utilizzo delle applicazioni. CPM, integrandosi in modo trasparente con le infrastrutture IT esistenti, protegge tutti gli utenti dalle minacce alla sicurezza note e sconosciute.

Websense, Inc.
San Diego, CA USA
Tel +1 858 320 8000
Fax +1 858 458 2950
www.websense.com

Websense UK Ltd.
Chertsey, Surrey
(Regno Unito)
Tel +44 (0)1932 796300
Fax +44 (0)1932 796601
www.websense.co.uk

Australia
websense.com.au

Irlanda
websense.ie

Brasile
portugues.websense.com

Italia
websense.it

Colombia
websense.com.es

Messico
websense.com.es

Francia
websense.fr

PRC
prc.websense.com

Germania
websense.de

Spagna
websense.com.es

Giappone
websense.co.jp

Svezia
websense.com

Hong Kong
websense.cn

Taiwan
websense.cn

India
websense.com

Scaricate subito una versione di prova gratuita valida 30 giorni all'indirizzo
www.websense.com/downloads

