

## WEBSense CLIENT POLICY MANAGER



**WebSense Client Policy Manager™ (CPM) stellt eine umfassende Sicherheitslösung auf Desktop-, Laptop- und Server-PCs bereit, die Unternehmen Schutz vor bekannten und neuen Gefahrenquellen bietet.**

CPM verhindert die Installation und Ausführung nicht genehmigter Anwendungen und stellt mit einer umfassenden, täglich aktualisierten Datenbank kategorisierter Anwendungen die Einhaltung von Unternehmensrichtlinien bei der Anwendungsnutzung sicher. Mit seinen Funktionen zur Anwendungskontrolle stellt CPM eine einfach zu implementierende, risikoarme und hoch effektive Alternative zu administrationsintensiven Host Intrusion Prevention-Systemen (HIPS) dar. Das umfassende Leistungsspektrum, das sowohl eine „Whitelist“ mit zugelassenen als auch eine „Blacklist“ mit gesperrten Anwendungen beinhaltet, gestattet fein abgestimmte, dynamische und sehr flexible Regelungen. CPM bietet unverzichtbaren Schutz direkt am PC vor sich rasch ausbreitenden „Blended Security Threats“ und ergänzt vorhandene Desktop-Antiviren-Software und Personal Firewalls auf ideale Weise.

### **Gefahrenvermeidung**

CPM stellt unmittelbar „eine erste Schutzschicht“ bereit – Sicherheitsprobleme beginnen und enden am Endpoint.

- Informiert über vorhandene Anwendungs- und Nutzungsrichtlinien am Endpoint, wehrt Schaden verursachende Software ab und sichert die Produktivität sowie die Einhaltung aller Richtlinien.
- Verhindert eine Veränderung von Registry-Einstellungen durch Schaden verursachende Anwendungen und dokumentiert verdächtige Registry-Modifikationen.
- Schützt Benutzer an externen Standorten und Mobilnutzer, die außerhalb des geschützten Unternehmensnetzwerkes tätig sind oder keine regelmäßigen Sicherheits-Updates bzw. Patches erhalten.
- Bietet externen Nutzern und Remote Usern Schutz vor Gefahrenquellen und sichert die Einhaltung von Nutzungsrichtlinien für den Zugriff auf das Internet und URL-Inhalte.
- Kompatibel mit Network Access Control-Lösungen (NAC) zur Umsetzung von Nutzungsrichtlinien für netzwerkfähige Geräte. Zugriffe nicht freigegebener Geräte werden verhindert.
- Über Integrationen können Schutzfunktionen auf Netzwerkprotokollebene verfügbar gemacht sowie dynamische Firewalls mit Anwendungserkennung bereitgestellt werden.
- Ein Programmzugriff auf Desktop-Ebene kann stufenweise eingeschränkt werden, um Angriffe auf gesicherte Bereiche wirkungsvoll zu verhindern.
  - Es wird maximale Sicherheit für Endpoints gewährleistet, da ausschließlich genehmigte Anwendungen ausführbar sind. Ein Start unbekannter, potentiell schädlicher Software wird zuverlässig verhindert.
  - Je nach Anwendungskategorie wird der Netzwerkzugriff für bestimmte Ports und Protokolle gesperrt, um eine Verbreitung schädlicher Software bzw. den nicht genehmigte Versand von Daten zu verhindern.
  - Systemadministratoren erhalten im Vorgriff auf einen Angriff und bei Bekanntwerden von Sicherheitslücken die Möglichkeit einer umgehenden Sperrung von Endpoint-Konfigurationen. Eine Ausführung von neuer Software wird verhindert, falls diese Software nicht genehmigt ist, Schaden verursacht oder möglicher Weise neu entdeckte Sicherheitslücken in Betriebssystemen oder Anwendungen ausnutzt.

## Regulierung der Anwendungsnutzung auf Desktop-Ebene

CPM überwacht die Liste installierter Anwendungen und deren Nutzung, um so die Zahl von Help Desk-Anrufen aufgrund nicht autorisierter Anwendungsnutzung zu minimieren.

- Gewährleistet die Einhaltung und eine automatische Aktualisierung flexibel definierbarer Richtlinien für die Anwendungsnutzung und bietet dem Endanwender Schutz vor gefährlicher Software.
- Verhindert die Installation und Ausführung nicht genehmigter Anwendungen.

CPM beinhaltet leistungsfähige Analyse-Tools, die Unterstützung bei folgenden Aufgaben bieten:

- Analyse unternehmensspezifischer Risiken.
- Ermittlung, ob und wo Web-Viren, Würmer, Spyware, Hacking-Anwendungen und andere Sicherheitsrisiken auf PCs und Servern vorhanden sind.
- Analyse von Programmen und Anwendungen in standardisierter Form.
- Rechtzeitiges Aufspüren von Gefahrenquellen und möglicher Sicherheitslücken in Anwendungen.

## Schutz von Unternehmensdaten

CPM bietet eine zusätzliche Sicherheitsschicht für die Regulierung von Informationsflüssen am Endpoint und kann den Diebstahl persönlicher oder unternehmenseigener Daten per Wechseldatenträger oder Netzwerübertragung unterbinden:

- Systemadministratoren können den Einsatz von USB-Sticks, CD-/DVD-Brennern, Diskettenlaufwerken und externen Festplatten an Client-Arbeitsplätzen regulieren, um so das Risiko eines Eindringens Schaden verursachender Software in das Unternehmen zu minimieren. Eine Einhaltung der Unternehmensrichtlinien in Bezug auf die Verwendung von Datenmedien wird zuverlässig gewährleistet.

## Rationalisierung

CPM verringert den Aufwand bei der Implementierung und Verwaltung von Sicherheitslösungen für PC-Arbeitsplätze.

- Integration in führende Verzeichnisdienste mit benutzer- und gruppenspezifischen Nutzungsrichtlinien.
- Integration in Windows-Firewall des Microsoft Windows XP Service Pack 2 (SP2) zur vereinfachten Steuerung von Personal Firewalls und zur Automatisierung zugelassener Programme durch die Anwendungserkennung und Port-Überwachung.

## Erweiterte Schutzfunktionen für Remote User

Die Remote-Filtering-Funktionen von CPM gestatten es Unternehmen, die für das Unternehmensnetz geltenden Filter- und Sicherheitsregeln von Websense Enterprise® oder Websense Web Security Suite™ auch auf Benutzer an externen Standorten und Laptop-PCs anzuwenden, um diese vor gefährlichen oder nicht genehmigten Inhalten zu schützen.

## CPM: Jetzt mit präventiver Websense ThreatSeeker™-Technologie

Die Websense ThreatSeeker-Technologie schützt präventiv vor Gefahren aus dem Internet, die mit herkömmlichen Sicherheitslösungen nicht bzw. nur mit überproportionalem Aufwand vermeidbar wären. Anders als bei diesen Verfahren ermittelt Websense Gefahrenquellen im Internet noch bevor der Kunde mit ihnen in Berührung gelangt. So sind Kunden bis zum Eintreffen neuer Patches und Signaturen geschützt.

Websense ThreatSeeker nutzt mehr als 100 proprietäre Verfahren und Systeme. Eine Kombination aus mathematischen Algorithmen, Reaktionsanalysen, Programmcodeanalysen sowie Data-Mining sind die Bausteine eines Frühwarnsystems für neue und komplexe Gefahrenquellen. Darauf aufbauend stellen Produkte mit Websense ThreatSeeker laufend aktuelle Sicherheitsinformationen bereit und schützen Kundeninstallationen innerhalb von Minuten automatisch.

## Kompatibilität und Investitionssicherheit

Das Websense Web Security Ecosystem™ bildet ein umfassendes Programm mit über 40 Technologiepartnern, um die Integration der Websense Software-Lösungen in vorhandene Umgebungen zu erleichtern. Das Web Security Ecosystem beinhaltet Partnerschaften zu führenden Sicherheits- und Netzwerktechnologien aus den Bereichen Internetgateways, Netzwerkzugangskontrolle, Security Event Management, Identity Management und Appliances. Durch eine nahtlose Integration in die unterschiedlichen Technologien hilft das Websense Web Security Ecosystem Unternehmen beim Aufspüren und Beseitigen von Gefahren der Internetnutzung und Sicherheitslücken.

## Systemanforderungen

### Client Policy Manager Server

- Microsoft Windows Server® 2003 Standard Edition oder Enterprise Edition bzw. SP1
- Microsoft Windows 2000 Server ab SP3

### Client Policy Manager und Remote Filtering Clients

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

### Remote Filtering Server

- Microsoft Windows Server 2003 Standard Edition oder Enterprise Edition bzw. SP1
- Microsoft Windows 2000 Server ab SP3
- Red Hat® Enterprise Linux® 3 oder 4: AS, ES oder WS, bzw. Red Hat Linux 9
- Sun® Solaris™ 9 oder 10

## Kurzprofil

CPM schützt Computer sowohl innerhalb als auch außerhalb des Unternehmensnetzwerks. CPM ermittelt und analysiert sicherheitsrelevante Gefahren bei der Nutzung von PCs und gewährleistet die Einhaltung flexibel definierbarer, skalierbarer und automatisch aktualisierbarer Nutzungsrichtlinien für Anwendungen. CPM kann nahtlos in vorhandene IT-Infrastrukturen integriert werden und bietet allen Benutzern Schutz vor bekannten und neuen Gefahrenquellen.

**Websense, Inc.**  
San Diego, CA USA  
Tel.: +1 858 320 8000  
Fax: +1 858 458 2950  
[www.websense.com](http://www.websense.com)

**Websense Deutschland GmbH**  
Kaiser-Wilhelm-Ring  
27-29, 50672 Köln  
Tel.: +49 221 56 94 - 460  
Fax: +49 221 56 94 - 354  
[www.websense.de](http://www.websense.de)

**Australien**  
[www.websense.com.au](http://www.websense.com.au)

**Italien**  
[www.websense.it](http://www.websense.it)

**Brasilien**  
[www.portugues.websense.com](http://www.portugues.websense.com)

**Japan**  
[www.websense.co.jp](http://www.websense.co.jp)

**China**  
[www.prc.websense.com](http://www.prc.websense.com)

**Kolumbien**  
[www.websense.com.es](http://www.websense.com.es)

**Frankreich**  
[www.websense.fr](http://www.websense.fr)

**Mexiko**  
[websense.com.es](http://websense.com.es)

**Grossbritannien**  
[www.websense.co.uk](http://www.websense.co.uk)

**Schweden**  
[www.websense.com](http://www.websense.com)

**Hong Kong**  
[www.websense.cn](http://www.websense.cn)

**Spanien**  
[www.websense.com.es](http://www.websense.com.es)

**Indien**  
[www.websense.com](http://www.websense.com)

**Taiwan**  
[www.websense.cn](http://www.websense.cn)

**Irland**  
[www.websense.ie](http://www.websense.ie)

Download der kostenfreien, voll funktionsfähigen 30-Tage-Testversion unter [www.websense.de/downloads](http://www.websense.de/downloads)

