



Websense® Client Policy Manager™

Der Websense® Client Policy Manager (CPM) bietet Schutz vor bekannten und unbekanntem Sicherheitsrisiken und verhindert die Ausführung nicht genehmigter Programme. Auf Basis einer einzigartigen und umfassenden Datenbank von kategorisierten Anwendungen die täglich aktualisiert wird, gewährleistet Websense CPM die richtlinienkonforme Nutzung von Desktop-, Laptop- und Server-PCs durch die Mitarbeiter. CPM bietet unverzichtbaren Schutz vor sich rasch ausbreitenden „Blended Security Threats“ und kompensiert bestehende Sicherheitslücken.

CPM - die innovative Sicherheitssoftware von Websense

Der Websense Client Policy Manager ist eine innovative Security Software-Lösung für Systeme, die die leistungsfähigen Funktionen der Websense-Datenbank auch auf Desktop-, Laptop- und Server-PCs des Unternehmens bereitstellt. CPM erkennt bekannte und unbekannte Gefahrenquellen und bietet wirkungsvollen und transparenten Schutz. Eine Ausführung nicht genehmigter Programme wie beispielsweise Spyware wird zuverlässig verhindert. Ein Ad-hoc Eingriff des Benutzers bzw. des Administrators ist dabei nicht erforderlich. Die Verwendung von Peer-to-Peer-Filesharing, Keylogging- und Hacker-Tools kann gezielt unterbunden werden. CPM bietet flexible, zentralisierte Steuerfunktionen, die eine Einhaltung von Richtlinien für Anwendungskategorien und individuelle Anwendungen sicherstellt. Durch Integration von Websense®-Verzeichnissen, die den Schutz von Desktop-PCs gewährleisten, kann die Einhaltung unternehmensspezifischer Nutzungsvorschriften auf Gruppenebene implementiert und nach Bedarf angepasst werden.

CPM ergänzt die Schutzmechanismen traditioneller Firewalls und Antiviren-Software. Modernste Lockdown-Funktionen schließen Sicherheitslücken, die ansonsten einen vollständigen Zusammenbruch des Netzwerkes zur Folge haben könnten, bis geeignete Virus-Signaturen oder Patches verfügbar bzw. installiert sind. Nur CPM bietet die Möglichkeit, Risiken wirkungsvoll und umfassend zu begrenzen. Eine Umsetzung flexibel konfigurierbarer Richtlinien für Anwendungen wird gewährleistet.

Funktionsumfang des Client Policy Managers:

Aktiver Schutz vor bekannten und unbekanntem Sicherheitsrisiken.

- **Websense Web-based Threat Mitigation™** - bietet die derzeit besten Schutzmaßnahmen gegen Risiken bei der Internetnutzung wie Keylogging-Programme, Spyware, Trojaner, Bot-Netze, Skripte und ActiveX-Steuerelemente. Websense hat die umfassendste Datenbank im Bereich schädlicher Internet-Anwendungen und bietet mit seinen Analyse- und Sperrfunktionen einen besseren, wirkungsvolleren Schutz vor Gefahren aus dem Internet als jedes vergleichbare Produkt.
- **Websense Network Lockdown™** - Schutz vor bislang unbekanntem Sicherheitsrisiken bietet eine Zugangssperre, die je nach Anwendungskategorie den Zugriff auf bestimmte Ports und Protokolle unterbindet.
- **Websense Application Lockdown™** - Bietet maximale Sicherheit durch exklusive Freigabe genehmigter Anwendungen für unternehmenseigene PCs und Server. Hierdurch wird die Ausführung unbekannter, potenziell schädlicher Software zuverlässig verhindert. Ermittelt und analysiert Sicherheitsrisiken und Anwendungsaktivitäten auf Desktop-Ebene.
- **Websense Removable Media Lockdown™** - Ermöglicht Systemadministratoren die Regulierung der Nutzung von USB-Sticks, CD-/DVD-Brennern, Diskettenlaufwerken und externen Festplatten an Client-Arbeitsplätzen. Eine Einhaltung der Unternehmensrichtlinien in Bezug auf die Verwendung von externen Medien kann zuverlässig gewährleistet werden.

Vorteile des Client Policy Managers:

- Aktiver Schutz vor bekannten und unbekanntem Sicherheitsrisiken.
- Ermittelt, analysiert und begrenzt Sicherheitsrisiken und Anwendungsaktivität auf Desktop-Ebene.
- Gewährleistet die Einhaltung und die automatische Aktualisierung flexibel definierbarer Sicherheitsvorschriften für Anwendungen auf Benutzer- und Benutzergruppenebene.
- Schützt Desktop-PCs im Unternehmensnetz aber auch unterwegs und stellt so für Mitarbeiter im Außendienst eine wertvolle Schutzschicht bereit.
- Eine Management Konsole stellt Funktionen zur Verwaltung sicherheitsspezifischer Richtlinien zentral bereit.
- Die Regulierung der Nutzung von externen Datenträgern mindert Rechts Haftungs- und Sicherheitsrisiken.
- Die Aktualisierung sicherheitsrelevanter Richtlinien erfolgt automatisch und ohne Administrator-Eingriff.
- Bietet unübertroffenen Schutz vor Gefahren im Internet.

Einsatzszenarien für den Client Policy Manager:

Mitarbeiter nehmen Laptop-PCs mit nach Hause oder auf Dienstreise und laden unwissentlich schädliche Software auf den Computer.

Problem: Wie verhindern Sie die Infektion des Netzwerkes durch einzelne PCs bei der Rückkehr des Mitarbeiters in die Firma oder bei Remote-Zugriffen über WAN-Verbindungen?

Lösung: Application Lockdown mit Websense CPM.

Ein neuartiger Malicious Code (z.B. Virus oder Wurm) infiziert das Unternehmensnetzwerk, bevor der Hersteller der Antivirensoftware einen entsprechenden Patch entwickelt bzw. bereitgestellt hat.

Problem: Wie stoppen Sie die Ausführung schädlicher Programme, die (versehentlich) von Mitarbeitern aufgerufen werden?

Lösung: Express Lockdown mit Websense CPM.

Mitarbeiter nutzen ungesicherte USB-Anschlüsse am Firmen-PC für den Datenaustausch.

Problem: Wie unterbinden Sie die Nutzung von externen Datenträgern und USB-Sticks, welche die im Unternehmen vorhandene IT-Security Lösung umgehen könnten?

Lösung: Removable Media Lockdown mit Websense CPM.

Ein Mitarbeiter startet unwissentlich ein Keylogging-Programm, das er per E-Mail erhalten hat und das von der Antiviren-Lösung nicht erkannt worden ist.

Problem: Wie verhindern Sie die Ausführung von Keylogging-Programmen und den dadurch im Netzwerk entstehenden Schaden?

Lösung: Keylogger-Kategorie in Websense CPM.

- Mit **Websense Express Lockdown™** können Systemadministratoren ohne Vorlaufzeit die Ausführung neuer Anwendungen unterbinden und so Angriffe durch Keylogging-Programme, Trojaner, Würmer und andere schädliche Programme verhindern. Anders als beim Application Lockdown ist für Express Lockdown keine vorausgehende Inventarisierung erforderlich.

Mit Hilfe der Websense Reporting Tools können Sicherheitsrisiken und Anwendungsaktivitäten auf Desktop-Ebene ermittelt und analysiert werden.

Sie ermöglichen die Betrachtung aktueller und protokollierter Daten und können potentielle Problembereiche bei der Computernutzung durch Mitarbeiter deutlich machen. Mit Hilfe der so gewonnenen Daten können IT-Administratoren bestehende Nutzungsrichtlinien für PC und Internet anpassen sowie pro-aktiv die Gefahren der Internetnutzung durch Mitarbeiter wirkungsvoll eindämmen. Darüber hinaus lassen sich mit den Berichterstellungs-Tools von Websense leistungsfähige Audit- und Alarmprozesse zur Einhaltung bestimmter Anforderungen und rechtsverbindlicher Vorschriften realisieren.

Websense Reporting Tools

- Erstellen unternehmensspezifischer Risikoprofile.
- Ermittelt das Vorhandensein und die Speicherplätze von Mobile Malicious Code, Spyware, Hacking-Applikationen und anderer Sicherheitsrisiken innerhalb eines Netzwerks.
- Bewertung von Software: Programme und Anwendungen werden nach Kategorien und in normalisierter Form erfasst. Sicherheitslücken in Anwendungen können frühzeitig ermittelt werden.
- Optimierung von Nutzungsvorschriften für Anwendungen anhand der mit den Bericht- und Analysefunktionen gewonnenen Daten.

Definition flexibler, automatisch aktualisierbarer Richtlinien.

Mit Hilfe von CPM kann die Einhaltung tagesaktueller Richtlinien bei minimalem Administrationsaufwand gewährleistet werden.

- **Centralized Policy Management** - Der benutzerfreundliche Websense Manager minimiert den Administrationsaufwand für die Erstellung und Umsetzung sicherheitsbezogener Richtlinien.
- **Anwendungsdatenbank** - Die Einteilung tausender Anwendungen innerhalb der Websense Datenbank in mehr als 50 Kategorien ermöglicht die flexible Definition von Nutzungsvorschriften für einzelne Benutzer, Benutzergruppen bzw. pro Kategorie(n).

- **Websense AppCatcher™** - Unbekannte Anwendungen und deren Verhalten im Netzwerk des Kundenunternehmens werden automatisch und anonymisiert an die Websense-Datenbank gemeldet. Durch diese Methodik bleiben Richtlinien stets aktuell und für Unternehmen relevant.

- **Websense Real-Time Security Updates** bietet Unternehmen einen Echtzeit-Schutz vor neuen Sicherheitsrisiken. Bei Verwendung von Real-Time Security Updates wird CPM innerhalb von Minuten nach Bekanntwerden möglicher neuer Gefahrenquellen aktualisiert und leitet automatisch Maßnahmen ein, die Risiken bei der Internet- und Anwendungsnutzung zu minimieren. Die Kategorien der Websense Datenbank werden dann auch, in Ergänzung zu den sonst üblichen täglichen Updates ggf. mehrmals pro Tag aktualisiert. Real-Time Security Updates sind als Zusatzmodul für CPM erhältlich.

Problemlose Integration

Websense CPM vereinfacht die Administration von Firmen-PCs und die Definition entsprechender, sicherheitsrelevanter Nutzungsvorschriften für Anwender.

- **Automatische Implementierung von Desktop-Agenten** - CPM Desktop-Agenten lassen sich im Websense Enterprise Manager zentral per Mausklick auf allen bzw. den ausgewählten Firmen-PCs installieren. Eine manuelle Intervention seitens des Anwenders oder der IT-Abteilung ist nicht erforderlich.

Systemanforderungen

CPM Server

Hardware: Mindestens Pentium III-Prozessor ab 512 MB RAM. Die Hardwareanforderungen variieren je nach Konfiguration. Weitere Informationen entnehmen Sie bitte dem Installationsleitfaden.

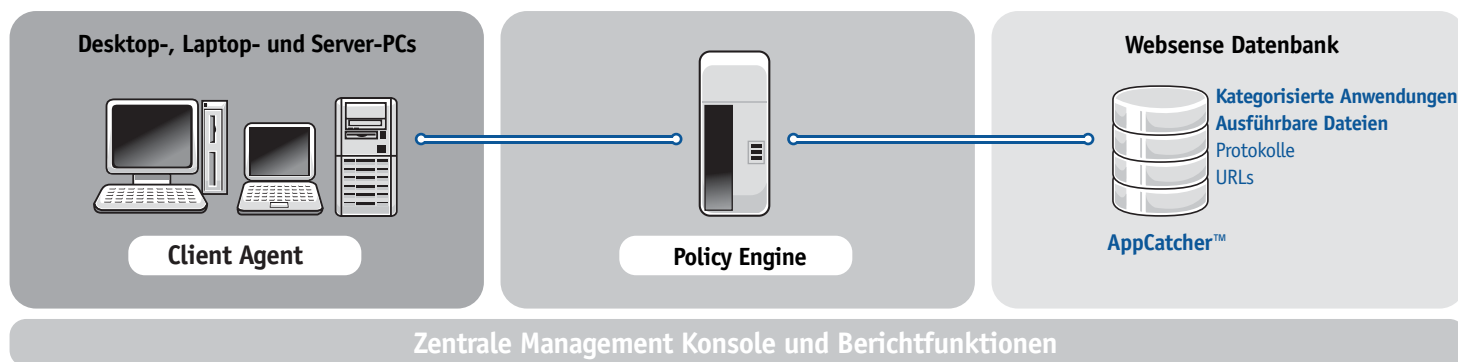
Unterstützte Betriebssysteme: Microsoft® Windows® 2003 Server, Windows® 2000 Server (SP3 oder höher)

Unterstützte Produkte und Dienstleistungen: Alle von Microsoft unterstützten Verzeichnisdienste

CPM Client

Hardware: Der CPM Client unterstützt fast alle Hardwareumgebungen für Desktop-PCs. Weitere Informationen entnehmen Sie bitte dem Installationsleitfaden.

Unterstützte Betriebssysteme: Microsoft® Windows® XP (SP1 oder höher), Windows® 2003 Server, Windows® 2000 Pro/Server/Advanced Server (SP3 oder höher), Windows® NT 4 Server (SP6a oder höher)



Download der kostenfreien, voll funktionsfähigen 30-Tage-Testversion unter www.websense.de

Websense Inc. San Diego, CA USA Tel.: +1 800 723 1166 Tel.: +1 858 320 8000 www.websense.com	Websense UK Chertsey, England Tel.: +44 (0)1932 796001 www.websense.co.uk	Websense France Paris, Frankreich Tel.: +33 (0)15660 5814 www.websense.fr	Websense Deutschland GmbH Köln, Deutschland Tel.: +49 (0)221 5694 460 www.websense.de	Websense Japan Tokio, Japan Tel.: +813.53220.1335 www.websense.co.jp	Websense Australia Sydney, Australien Tel.: +61 (2)9006 1621 www.websense.com.au	Websense Greater China Hongkong Tel.: +852.2855.8811 www.chinese.websense.com www.prc.websense.com	Websense Latin America Sao Paulo, Brasilien Tel.: +55 11 4612 0798 www.espanol.websense.com www.portugues.websense.com
---	---	--	--	--	---	---	---