WEBSENSE CLIENT POLICY MANAGER

Websense® Client Policy Manager™ (CPM) provides a comprehensive endpoint security solution for desktops, laptops, and servers that proactively protects your organization against known and unknown security threats. CPM prevents the installation and execution of unauthorized applications and enforces application use policies with its comprehensive database of categorized applications, which is updated daily. CPM is a critical component in your endpoint security strategy to stop today's fast-moving and blended security threats.

"On the laptops that now have Websense, we have not had any instances of viruses, and we've not had any instances of spyware get installed onto a machine since our deployment…we've also had positive feedback from our end users."

Russell Ryan
Global Windows Administrator
Colorcon

CUSTOMER TESTIMONIAL: COLORCON

Colorcon's Pains:

- Remote laptop users infected in the field bringing malicious software back into the organization.
- NETSKY infection spreading throughout the Colorcon network during a three-hour window while its antivirus updated its signature files.
- Downloads of unauthorized software proving incompatible with business software, leading to increased Help Desk calls.

CPM Benefits for Colorcon:

- CPM exclusive database of categorized applications provides Colorcon with flexible policy management.
- CPM ability to create customized rule sets and categories to build policies for "allowed" applications saves administration time.
- CPM ease of use saves IT time and frustration.
- Colorcon's Help Desk can now be proactive rather than dealing with unplanned and potentially expensive incidents.

Prevent Attacks

CPM provides an immediate "first line of defense"—security starts and stops at the endpoint.

- Addresses weaknesses in your existing antivirus, anti-spyware, personal firewall, and patch management processes to render today's attacks harmless.
- Protects laptop users operating outside your network or without standard security updates or patches.
- Works with Network Access Control (NAC) solutions to enforce policy on devices trying to enter the network, denying access to non-compliant endpoints.
- Provides multiple levels of control to prevent the launch or mitigate the propagation of security attacks:

  Websense Application Lockdown™ – Provides maximum control over desktop environments by allowing only approved applications to run, preventing potentially malicious applications from launching.

  Websense Network Lockdown™ – Blocks application network access to specific ports and protocols by application category, preventing the propagation of malicious software or unauthorized outbound communications.

  Websense Express Lockdown™ – Allows system administrators to preempt attacks by preventing new malware from executing, and limiting the application environment to a known configuration.

Control Desktop Application Use

CPM proactively monitors user application inventories and activity, and reduces Help Desk calls associated with unauthorized application use:

- Enforces flexible, auto-updating application use policies to protect end users from malicious software.
- Prevents the installation and execution of unauthorized applications.

CPM includes advanced reporting tools which help:

- Determine your organization's risk profile.
- Detect the presence and location of malicious mobile code (MMC), spyware, hacking tools, or other security risks on each machine and server.
- Perform critical software assessments that provide categorized and normalized views of programs and applications.
- Enable early threat detection and identification of potential application vulnerabilities.

Safeguard Information

CPM provides another layer of control over information at the desktop by blocking the potential theft of private information or intellectual property via removable media or network communications.

- **Websense Removable Media Lockdown**™ - Allows system administrators to prevent devices such as flash drives, CD/DVD burners, floppy drives, and external hard drives from being used on client workstations, minimizing the risk of introducing malicious software to the organization. Organizations can also block writable media, depending upon your organization's policy.

Streamline Operations

CPM reduces the level of effort to deploy and manage an endpoint security solution:

- Integrates with leading directory services.
- Offers a low-impact agent compatible with Microsoft Windows.
- Optimizes IT and Help Desk operations by eliminating calls and dispatches for desktop and laptop rebuilds due to performance or application compatibility problems.

Support from Powerful and Unique Websense Technologies

The Websense® Master Database – Utilizes a combination of proprietary classification software and human inspection techniques to ensure the most complete coverage. The Websense Master Database has the most accurate and up-to-date classification of URLs, protocols, and applications.

- **Websense AppCatcher**™ **technology** – Allows Websense customers to automatically and privately submit unknown executables for research and categorization. Websense identifies the network components and behaviors of customers' launched applications to determine if malicious code exists. Applications are then added to the database to ensure protection for all customers.
- **Websense Real-Time Security Updates** – Provides security database updates for web-based and application-based threats, within minutes after detection by Websense.

Extend Web Filtering Protection to Remote Users

CPM's Remote Filtering capabilities allow you to apply your same Websense Enterprise® or Websense Web Security Suite™ web filtering policies to remote users and frequent travelers as they would have within the network, to ensure secure employee internet use anytime and anywhere.

- Extends internet usage policies to remote laptop users to protect them from malicious and inappropriate websites.

System Requirements

Client Policy Manager Server

- Microsoft Windows Server 2003 Standard Edition or Enterprise Edition, or the same with SP1
- Microsoft Windows 2000 Server with SP3 or higher

Client Policy Manager and Remote Filtering Clients

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

Remote Filtering Server

- Microsoft Windows Server 2003 Standard Edition or Enterprise Edition, or the same with SP1
- Microsoft Windows 2000 Server with SP3 or higher
- Red Hat Enterprise Linux 3 or 4: AS, ES, or WS, or Red Hat Linux 9
- Sun Solaris 9 or 10

Summary

CPM protects computers both inside and outside of the corporate network by detecting and analyzing endpoint security threats and application activity, and by enforcing flexible, scalable, auto-updating application use policies. Integrating seamlessly with your existing IT infrastructure, CPM protects all of your users against known and unknown security threats.

Websense, Inc.
San Diego, CA USA
tel 800 723 1166
tel 858 320 8000
www.websense.com

Websense UK Ltd.
Chertsey, Surrey UK
tel +44 (0) 1932 796300
fax +44 (0) 1932 796601
www.websense.co.uk

Australia
websense.com.au

Brazil
portugues.websense.com

Colombia
websense.com.es

France
websense.fr

Germany
websense.de

Hong Kong
websense.cn

India
websense.com

Ireland
websense.co.uk

Italy
websense.it

Japan
websense.jp

Mexico
websense.com.es

PRC
prc.websense.com

Spain
websense.com.es

Sweden
websense.co.uk

Taiwan
websense.cn

Download a free 30-day evaluation today www.websense.com/downloads

WEBSENSE
SECURING PRODUCTIVITY™