

ContentProtect™

professional appliance



ContentProtect Professional Appliance (Internet Filtering)

Manage and protect your company's Internet experience with powerful, state-of-the-art Internet filtering. Your organization can increase productivity, reduce liability and preserve precious bandwidth by implementing Internet filtering with the ContentProtect Professional Appliance.

The ContentProtect Professional Appliance is a dedicated inline Internet filtering appliance that manages end user access to Internet-based content. It is a plug-and-play, low maintenance, rack mountable appliance.

Benefits

The ContentProtect Professional Appliance offers the most effective and flexible Internet filter available today! You can easily customize ContentProtect settings to fit the needs of each employee in your organization, for separate groups and departments, or apply settings company-wide. Powerful reporting tools enable administrators to review where employees are spending their time online. You can customize ContentProtect filter settings to block specific Web sites, domains or chat rooms, helping you increase employee productivity, reduce risk and preserve the network resources within your organization.

For organizations with a mobile workforce or remote offices, the ContentProtect Professional Appliance works hand-in-hand with the client version of ContentProtect Professional offering users "end-to-end protection." Intelligent filtering detection means no double filtering if client software is loaded when the client is attached to the corporate network. The ContentProtect Internet filtering solutions are specifically designed for businesses, education, and government organizations. They provide the flexibility you need to deploy on the client computer, inline with the company network or both. No other vendor offers this flexibility.

International Data Corporation (IDC) stated, "Employee Internet Management (EIM) has traditionally been deployed on servers at the gateway. Today's risks dictate that additional policy enforcement points should exist at the desktop and network levels as well as at the gateway."

— IDC Emerging Threats to the
Employee Computing Environment
Doc# 29015, March 2003

ContentProtect Key Advantages Plug-and-Play Configuration

The ContentProtect Professional Appliance is specially designed with ease of use in mind. It is simply connected to the network, and with minimal configuration it is enforcing your company's Internet policy. The appliance will automatically block websites that contain inappropriate content. There is no software to install or settings to configure on each computer.

Intelligent Filtering Detection

No double filtering if client software is loaded when the client is attached to the corporate network.

Multiple Filtering Profiles

The ContentProtect Professional Appliance is highly customizable, permitting administrators to create policies at the organization, group, or individual level, rather than forcing them into a "one size fits all" scenario.

Dynamic Content Analysis

The ContentProtect Professional Appliance uses dynamic contextual analysis to filter Web content. As Web pages are requested, ContentProtect's dynamic analysis engine has the ability to understand content in context and filter appropriately. Based on the filter settings for the user that is accessing the Internet, content is then allowed or blocked.

Time Management

The ContentProtect Professional Appliance includes a powerful time management feature that permits administrators to set the time(s) of day when users can access the Internet. A time quota feature exists that permits administrators to assign a block of time to a user. Once that user's time quota is used up, they will no longer have access to the Internet.

Web Based Reporting

ContentWatch provides the ability for Administrators to view reports anywhere and at any time. Reports are stored in the ContentWatch Data Center (CDC). Having data stored in the CDC permits access to online reports from any Internet connection in the world. Administrators can check on the Internet activity of their employees from work or in a hotel room while traveling.

Customized Lists

ContentProtect permits you to create customized lists of unacceptable or acceptable Web sites. For example, you could set up a white list of sites that you allow your employees to visit, and block all other sites from access.

Easy to Deploy and Manage (Web-based, Single Point of Administration)

The ContentProtect Professional Appliance comes preconfigured with operating system software and Internet filtering software making it easy to deploy. Both run on optimized hardware.

From a single Web-based console, administrators can manage all Internet policies and computers from anywhere, from any computer as long as an Internet connection is available. Web-based management is made possible through the CDC. Administrators can also receive email notifications when employees may be trying to access, override, or in some way violate the user's Internet policy.

1U Rack Mountable

The appliance is a standard 1U, 19-inch rack mountable device, and fits in any standard rack.

Product Data Sheet

For Pricing Options and Ordering

Phone
1.866.765.7233

Email
sales@contentwatch.com
info@contentwatch.com

Website
www.contentwatch.com

**ContentProtect Professional
Appliance supports up to
1,000 users***

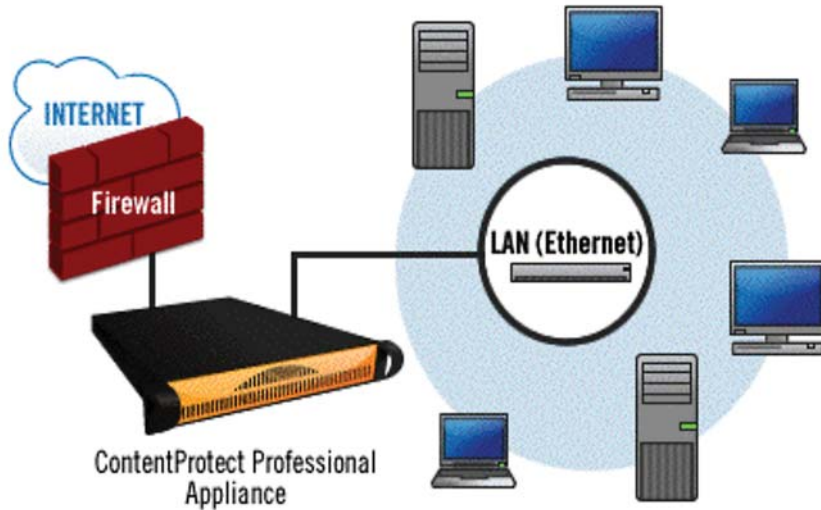
**Based on average
Internet usage*

Toll-Free Technical Support

**ContentProtect is backed
by toll-free technical
support. ContentWatch
also offers email support.**



How ContentProtect Professional Appliance Works



Specifications

System
 CPU: Pentium 4 630 3.0 Ghz
 Memory: PC2-5200; 1GB
 Chipset: Intel E7230 chipset
 Network: 1 x Intel 82573V Gigabit PCI-Express Ethernet; 1 x Intel 82573L Gigabit PCI-Express Ethernet
 Video: Integrated ATI Rage XL

Chassis
 Form Factor: Mini 1U; 14° ± rack-mountable chassis
 Dimensions: 16.7° ±W x 1.7° ±H x 14° ±d
 1 x 100mm 5000RPM fan

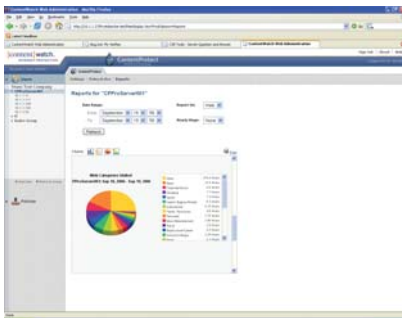
Multiple I/O
 USB: 2 x rear USB ports; 2 x USB header
 Serial ports: 1 x rear serial port; 1 x serial port header
 Parallel port: 1 x rear parallel port
 Keyboard/mouse: 1 x PS/2 Keyboard, 1 x PS/2 mouse
 LAN: 2 x LAN ports, RJ-45

Front Panel
 Power on/off button
 System reset button
 Power LED
 HDD activity LED
 2 x Network activity LEDs
 System overheat LED

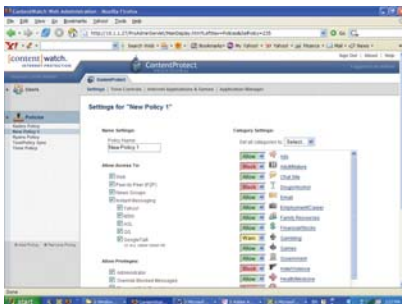
Power Supply
 260 watt AC power supply
 Thermal control with PFC

Regulatory Compliance
 Electromagnetic Emissions: FCC Class B, EN 55022 Class B, EN 61000-3-2/-3-3, CISPR 22 Class B
 Electromagnetic Immunity: EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11)
 Safety: EN 60950/IEC 60950-Compliant; UL Listed (USA); CUL Listed (Canada); TUV Certified (Germany); CE Marking (Europe)

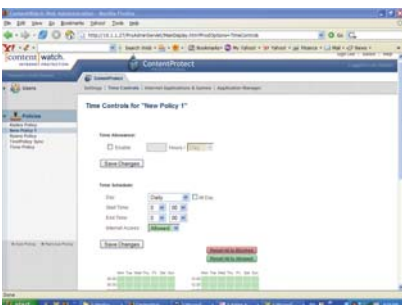
© 2002 - 2006 by ContentWatch Incorporated. All rights reserved. ContentWatch, ContentProtect, ContentCleanup, and VirusProtect are trademarks or registered trademarks of ContentWatch Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information in this document is subject to change without notice.



The ContentProtect Professional Appliance offers powerful online reporting tools, accessible from any Internet connection. These reports offer an insightful view into your company's Internet activity. The reports identify what sites have been visited, when they were visited, how much time was spent on visited sites, and by category including what types of sites were visited.



The ContentProtect Professional Appliance's Remote Management feature equips you with powerful administration capabilities. From any Web browser you can modify your entire organization's settings. You make the call whether to allow, warn or block any of 28 categories for your entire organization, for a particular department, or for an individual user/machine.



The ContentProtect Professional Appliance's Time Management feature allow you to manage the time of day and the amount of time that users can spend on the Internet. Time Controls can be set either by limiting the total number of hours a user can spend on the Internet over a given period, or by setting specific times (in 30-minute intervals) when Internet access is allowed or blocked.