

The Total Solution



Stop Unwanted Content

# SurfControl Enterprise Threat Shield™

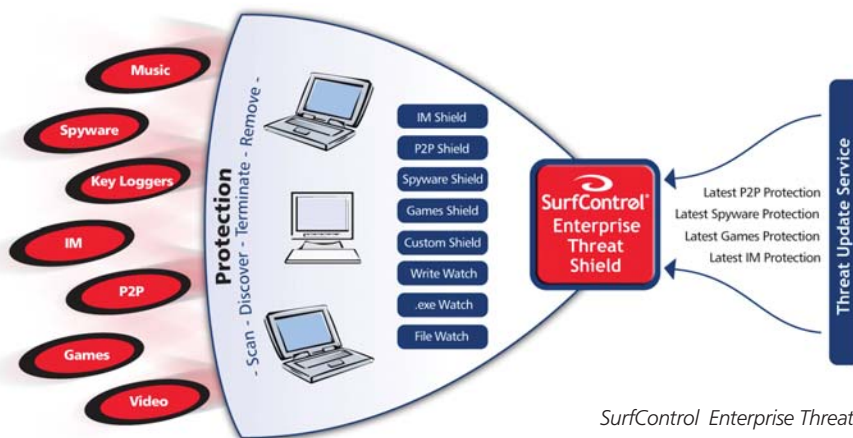
Other products can scan and remove spyware, but that's only half the solution. Only SurfControl Enterprise Threat Shield scans, removes and prevents spyware from infecting machines before it has a chance to jeopardize your organization's:

- Legal Liability
- Security
- Productivity
- Network Resources

## More Than Discovery & Removal - Think Spyware Prevention

Protecting against ever-increasing, insidious and complex Internet threats requires a multi-layered approach. Perimeter security, such as firewalls, Intrusion Detection Systems (IDS) and anti-virus solutions, strengthened by Web and e-mail filtering, provide the first line of defense. SurfControl Enterprise Threat Shield completes this defense by protecting against threats that may penetrate your perimeter, or enter the network by other means, such as via memory sticks or the infected machines of mobile workers.

SurfControl Enterprise Threat Shield delivers protection by continuously discovering, removing and terminating, in real-time, those applications that pose a threat to your network. It provides control over the broad and ever-evolving range of malicious applications and their common routes into the organization. With SurfControl Enterprise Threat Shield, incoming threats are stopped before loading onto users' computers, no matter how they are delivered. Spyware, adware, key-loggers, Instant Messaging (IM), Peer-to-Peer (P2P), games or any other identified company-specific applications are controlled before they jeopardize security. If the threat is already on a user's machine, then SurfControl Enterprise Threat Shield stops the threat from running and can remove it completely.



SurfControl Enterprise Threat Shield

## Comprehensive and Customizable Database

The ability to correctly identify malicious applications is central to managing threats at the desktop. SurfControl Enterprise Threat Shield provides four dynamically updated Threat Shield databases—Spyware, IM, P2P and Games—which are continuously updated and maintained by SurfControl's Adaptive Threat Intelligence Services. The databases contain digital signatures of rogue applications, so any disguise attempts, such as file re-naming, do not compromise security.

The Custom Threat Shield gives organizations the ability to easily create custom business or industry-specific threat databases. By creating digital signatures of any application on your network that is of concern, such as unlicensed software, you can customize your defense and enable the highest possible level of control and management. (See Screenshot No. 1 and 2)

## Centralized Deployment & Reporting – Maximum Control, Minimum Overhead

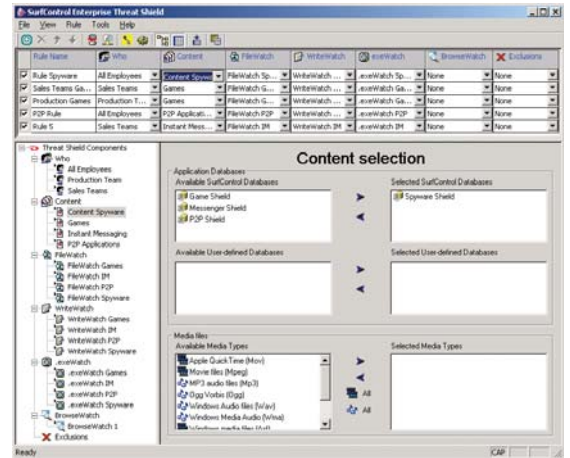
Designed for the enterprise, SurfControl Enterprise Threat Shield integrates with an organization's current directory services, such as Active Directory and Novell eDirectory, to simplify product deployment across the enterprise; end-user involvement is not required. SurfControl Enterprise runs as a memory resident service on the user's machine. Automated anti-tampering technology is used to ensure that the service is persistent on the desktop and that attempts to disable the threat protection are thwarted.

Management, Trend and Summary reports can be printed directly or exported to other applications. This gives visibility into the threats that are detected, cleaned and removed from your network, as well as information on security policy compliance. (See Screenshot No.3)

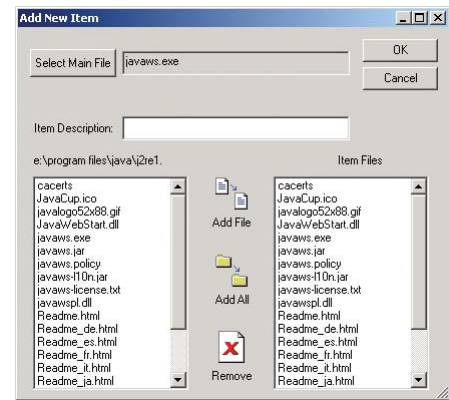
## Flexible Policy Administration

SurfControl Enterprise Threat Shield's rule-based administration gives you the flexibility to implement a security policy to meet the specific needs of your business. You decide how you want to manage potentially malicious applications and files, and create rules and exclusions accordingly. Based on the Threat Shield databases, your rules give you control over the times, users and groups you want to protect. By managing your policies from a single, central point you are able to deploy policy changes quickly and protect against new threats as they emerge.

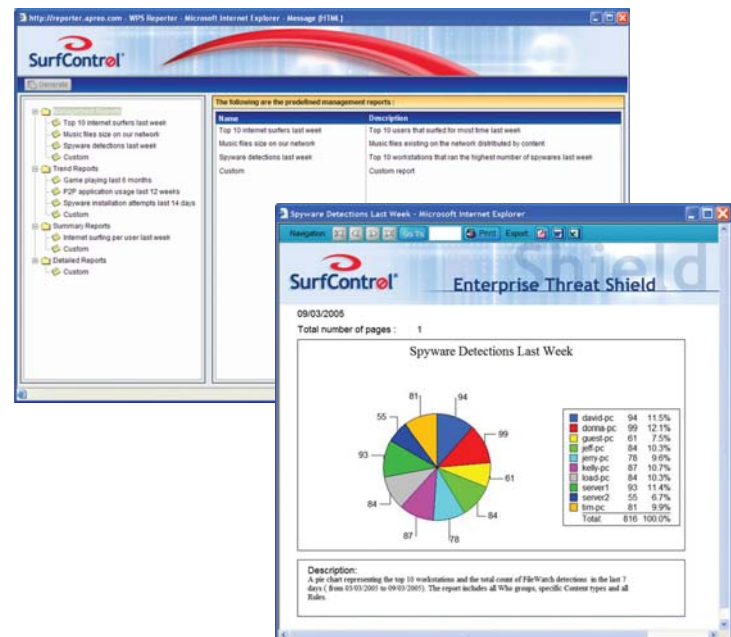
1 Content Selection



2 Custom Threat Shield



3 Reports





## ■ BrowseWatch

BrowseWatch measures the time users actually spend on particular Web sites and pages, and can generate detailed reports on particular Web activity. BrowseWatch can be configured to only record time when the browse window is active, or to record time even when the open window is in the background.

## ■ Music and Video Management

Enterprise Threat Shield's ability to identify music and video files gives you the power and flexibility to create policies that manage your users' media. Allowing media files below a certain size limit may be appropriate for business use, but the presence and use of larger files on the corporate network can pose a serious risk to network resources and expose a business to copyright and liability issues.



**Download and install your FREE  
no-obligation 30 day trial of any  
SurfControl product now.**

**www.surfcontrol.com**