

Those aren't just files you're swapping – the dangers of Peer-to-Peer File Sharing

*A unique multi-layered
solution to combat employee
computing risks*

Abstract

Employees are using company resources to access peer-to-peer (P2P) applications on company time and exposing organizations to serious and potentially catastrophic risks. Swapped files from P2P networks may contain viruses, worms, Trojan horses, and spyware. And, since P2P is primarily used to exchange pirated audio, video, and software files or inappropriate content, companies should be concerned about the potential exposure to legal—even criminal—liability. The effect of running P2P applications, downloading large files, and allowing fellow P2P users to upload files from employee's shared folders can also slow down network performance, negatively impacting the functioning of business-critical applications. All of these threats are real and must be managed.

Due to its unique, layered approach, Websense software allows companies to completely prevent P2P use at the network level, gateway, and desktop. Websense gives companies complete confidence that P2P applications will not operate in their IT environment and cannot be used on any company-owned computers.

Websense, Inc.
World Headquarters
10240 Sorrento Valley Road
San Diego, California 92121
USA
Tel: 858.320.8000
Fax: 858.458.2950
www.websense.com

Contents

Executive Summary	3
Introduction.....	4
Background.....	4
Peer-to-Peer Usage is Prevalent in Corporate Environments	5
Corporate Risks Associated With P2P Use	6
Security threats.....	6
Spyware and adware	6
Exposure to viruses and worms.....	6
P2P vulnerable to hackers	7
Loss of confidential information.....	7
Legal liability concerns.....	7
Copyright infringement	8
Distribution of inappropriate content	8
Employee productivity loss	9
IT resource abuse.....	9
Bandwidth consumption	9
What companies need	9
How Websense Enterprise addresses P2P vulnerabilities.....	10
Detect the usage of P2P file sharing—at the enterprise network level	10
Stop existing P2P activity in the enterprise network.....	11
Block launch of P2P applications—at the desktop.....	11
Prevent downloading of P2P applications	12
Allow access to P2P applications on a case-by-case basis.....	12
The unique advantages of Websense Enterprise	12
Industry-leading integration and flexible deployment	13
Conclusion.....	14
About Websense, Inc.	14
Appendix: The Websense Enterprise Solution	16

Executive Summary

Employee use of peer-to-peer (P2P) applications on company time and with company resources exposes organizations to serious and potentially catastrophic risks. From security threats due to exposure to viruses and worms, to loss of proprietary company data, to the introduction of spyware into the enterprise and avenues for hackers to exploit, these concerns are daunting and very real. When a single audio file takes 5MB of disk space and a video file can be as large as 700MB, it is easy to see what the effect might be on a company's network bandwidth and storage facilities. And, since P2P is used primarily to exchange pirated or inappropriate audio, video, and software files, companies must take appropriate measures to guard against the associated legal liability. Companies should also be concerned about employee use of P2P applications that have no direct positive business impact. The effects of running P2P applications, downloading large files, and allowing fellow P2P users to upload files from shared desktop folders can slow down network performance and negatively impact the performance of business-critical applications. All of these threats currently exist in a significant number of enterprise networks and must be managed.

To address these concerns, companies need the ability to set and enforce policies for P2P use within their organizations. Websense Enterprise[®], the leading employee Internet management solution, provides organizations with a multilayered platform for managing today's growing list of employee computing risks, including P2P file sharing. The Websense solution includes an award-winning database of categorized Web sites, network protocols, and desktop applications that is updated daily. Using this highly granular database IT administrators can create employee-based policies to manage a variety of activities, such as Instant Messaging (IM), P2P file sharing, and inappropriate Web surfing, as well as stop spyware or other malicious code. These policies can be implemented with a high degree of precision, including by individual or group, time of day, and length of time.

Further, Websense is unique in providing P2P management policies on the desktop, including remote laptops. When laptops are disconnected from the network and used for P2P file-sharing activities at home or while away from the office, they can introduce security breaches around the organization's existing security infrastructure when passed back into the network. To effectively address security concerns from P2P, including serious security concerns, organizations must be able to stop P2P activities on their systems completely. To do this, policies should be automated to protect all corporate assets, including disconnected laptops, from becoming nodes in P2P networks.

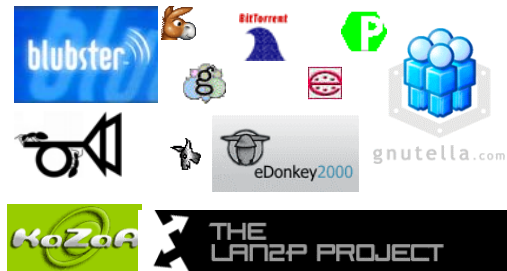
Introduction

Background

Peer-to-peer (referred to as P2P) file sharing networks are transient Internet networks that allow computer users with the same P2P networking program to connect with each other and use sophisticated searching techniques to directly access and download files from one another's hard drives.

At any given moment, roughly 5 million users are swapping more than 900 million files via P2P networks.¹

To date there have been four distinct generations of P2P clients. The first mainstream P2P system was Napster. Individual music lovers “joined” and gave Napster access to audio files on their computers. After Napster’s central server indexed all Napster user files, a user could search Napster, determine which users had a copy of the sought-after file, and then download it. Using a central server model allowed Napster to handle searches efficiently and retain control over the network. Unfortunately for Napster, shutting the service down was as easy as simply shutting down its central servers, which it was forced to do after suits were filed by the music recording industry for piracy.



Following Napster, second-generation P2P networks such as Gnutella emerged. Having learned a lesson from the Napster debacle, the creators of Gnutella decided to create a decentralized network—one that could not be shut down by simply turning off a server. Gnutella worked by connecting users directly to each other, without requiring any central servers. When a user started the Gnutella client, he or she would be connected to a certain number of other users, then those users to other users, etc., in one giant network. As a result, file searches in Gnutella were more complicated than in Napster. The Gnutella network, however, had one advantage over Napster—there was no central awareness by Gnutella of the on-going activity on its network, including no central awareness or compilation of information relative to the unauthorized transmission and use of copyrighted materials—so it could not be shut down for promoting copyright infringement practices. However, searches were slow and inefficient due to the decentralized architecture, and its popularity faded.

The third generation of P2P technology was created to alleviate some of the problems with the Gnutella network. These third-generation clients, like Kazaa, Grokster, and Morpheus, use the FastTrack Network. FastTrack added a number of enhancements to the P2P networks, including Supernodes, clients with more bandwidth and CPUs available to store cached files and connect users. These changes have improved the efficiency of searches and download speeds. FastTrack is currently the most popular P2P network.

More people looked for information about the file-swapping program Kazaa than any other topic on the Net in 2003, according to search site Yahoo.²

¹ Source: International Federation of the Phonographic Industry (IFPI), 2002

² Source: <http://news.bbc.co.uk/2/hi/technology/3356397.stm>

In P2P networks like Kazaa, users connect directly to each other to download files. This potential security flaw has had some extreme consequences, with well over 1,000 users being sued for piracy via IP logging. The fear and paranoia introduced by these lawsuits, and the innate desire for privacy, have spawned the fourth generation of P2P clients. Some, including BitTorrent, MUTE, Blubster, and Filetopia, attempt to mask the origin of the traffic (IP address) and encrypt the traffic, making it difficult to detect transferred files.

Peer-to-Peer Usage is Prevalent in Corporate Environments

P2P use is not restricted to music-loving teenagers and college students. In a survey of more than 175,000 PCs at 560 companies in various industries, ranging from 10 to 45,000 employees, P2P software such as Kazaa, eDonkey, and Morpheus was found to be installed at least once in 77 percent of companies. The survey found that every company in its sample of more than 500 employees had at least one installation of file-swapping software. The survey also found that some companies had P2P activity on more than half of their computers.³

With audio files typically 4 to 5MB and video files as large as 700MB, the temptation for employees to use high-bandwidth company resources for their P2P downloads is too great to resist. While at work, employees can launch their favorite P2P applications to locate the audio or movie file they are interested in, and then download the files to their personal drives on their company's network. They can then use the rewritable drives on their company computers to copy the files to CD or DVD, for listening or viewing at home.

This paper explores the use of P2P file sharing in a corporate environment and examines the associated risks.

By the numbers
People who use file-sharing services in the USA: 57 million
Number of times Kazaa's software has been downloaded worldwide: 230 million
Users sharing files Wednesday afternoon on Kazaa: 4.2 million
Files being shared on Kazaa Wednesday afternoon: 900 million
Songs sold in two months at Apple Music Store: 5 million
<i>Source: The Yankee Group, RIAA, USA TODAY research</i>

³ Source: AssetMetrix, July 2003

Corporate Risks Associated With P2P Use

The legal battles involving Napster and Kazaa brought P2P use to the attention of the general CD-buying, video-viewing public. Business enterprises are only now becoming aware of the many other risks involved with employee use of P2P applications in the corporate world. These concerns fall into four main areas:

- Security
- Legal liability
- Employee productivity
- IT resources

Security threats

File-sharing networks are unregulated, and files that claim to be music or movies may actually contain any number of other types of content. Once a P2P application is operating within an organization's network, it is impossible to be sure that the downloaded files will not bring with them a virus or worm that will infect the organization's network or spyware that is designed to track employees' actions, and possibly collect confidential information.

Spyware and adware

Spyware is any technology used to gather information about computer users or their activities, secretly or without consent, and relay that information to interested and potentially undesirable third parties over the Internet. Adware also sends information to third parties, though with the user's often uninformed permission. Examples of spyware and adware include keylogging, Web bugs, and tracking cookies.

Many file-sharing programs contain adware/spyware that tracks individual users' Internet-related activities. These stealth software programs run in the background, even when the file-sharing software is not running, and are often installed without the user's consent or understanding. For example, when a user downloads and installs the free Kazaa software, additional software from third-party providers, such as Cydoor, Topsearch, and GAIN AdServer, is also downloaded.

Kazaa's terms of service agreement points out that Cydoor, a maker of adware software, may use the "Internet connection to update its selection of available ads and store them on [the user's] hard drive." But this information may be buried within thousands of words, and most people blindly click the "Agree" button without reading all the fine print.⁴

Since adware/spyware is a piggyback program that runs separately from the program it accompanies, it uses additional processing power, hard drive space, and bandwidth, and may have security flaws itself, opening an avenue of attack for hackers or viruses. When it is downloaded surreptitiously, as in the case of the Kazaa download, it can bypass corporate firewalls and enter the network, rendering sophisticated perimeter security technology ineffective.

Exposure to viruses and worms

P2P networks can be, and are, easily exploited to distribute viruses and worms, allowing them to bypass normal security and filtering barriers. Viruses and worms can hitch a ride on files transferred using P2P applications and make their way into corporate networks. P2P applications allow users to send files directly to

⁴ Source: http://www.kazaa.com/us/help/resource_usage.htm

each other, effectively circumventing perimeter security mechanisms, such as firewalls and antivirus scanners deployed at the network perimeter, e-mail gateways, or e-mail servers, and enabling viruses to easily penetrate and then propagate within a network.

Grokster, like many P2P software vendors, bundles advertiser applications with its software to generate revenue. One of these adware programs, ClickTilUWin, installed a Trojan horse called W32.DIDer. Grokster's antivirus software did not pick it up, and the infected software was downloaded by Grokster users for three weeks.⁵

*45 percent of the most popular files shared on Kazaa—including “cracks” that let users break copy protection on commercial software—actually contain viruses, worms, or Trojan horses.*⁶

P2P vulnerable to hackers

Hackers can easily take advantage of P2P vulnerabilities, including buffer overflow, to spread worms and viruses. A buffer overflow is a software glitch that causes problems for users and software developers. In May 2003, version 2.02 of Kazaa software was reported to have buffer overflow vulnerability. Computers running Kazaa and acting as Supernodes are vulnerable to attacks if they receive packets with more than 200 IP addresses of other Supernodes. “A remote user can send 203 entries to the target Supernode to trigger the flaw and cause the Supernode to crash” or execute code on the victim's computer.⁷

Vulnerabilities in P2P networks also occur during the process of transferring files. When a user transfers files, his or her IP address is revealed. Using this IP address, hackers can potentially attack the system.

Loss of confidential information

Employees can accidentally or intentionally make confidential information available to P2P users around the world in one of two ways. They can place confidential files (which should be properly safeguarded) in a shared folder. Or they can configure the P2P file-sharing application incorrectly so that their entire hard disk, computer, or even network drives are set up as available to share. When this happens, anyone on the P2P network may be just moments away from downloading personnel files, financial results, or a customer database.

Legal liability concerns

The danger of allowing employees to use P2P applications at work goes beyond the ominous exposure to viruses and worms. Enterprises face significant legal risks when employees share copyrighted, illegal, or inappropriate content via corporate networks.

Copyright violations resulting from the presence of pirated audio, video, and other files on company-owned computers and networks are only one emerging threat. Another type of policy violation can result from the transfer and viewing of pornography and other objectionable files, including the criminal offense of viewing and distributing child pornography.

A recent study of Gnutella network searches at a university found that 97 percent of activities occurring on a P2P network could expose the university and/or its members to criminal or civil liabilities. In the analysis of

⁵ Source: <http://www.grokster.com/dlderinformation.html>

⁶ Source: TruSecure, Dec. 2003

⁷ Source: <http://www.securitytracker.com/alerts/2003/May/1006846.html>

over 22 million searches, the study found that 55 percent of all search requests were for copyrighted materials, 42 percent of all search requests were for pornography, and 6 percent of the searches were specifically for child pornography.⁸

Copyright infringement

Many of the files shared over P2P networks are copyrighted materials that are distributed without authorization, including pirated audio, movies, and software.

The most obvious and widespread example is the proliferation of music files. The Recording Industry Association of America (RIAA) has made it clear that it intends to actively and aggressively protect the copyrights of its members. The RIAA won a court ruling allowing it to identify Internet Service Provider subscribers and seek as much as \$150,000 per pirated file if a company is allowing employees to use the corporate network to download copyrighted material.⁹ Companies that do not have policies in place to prevent employee P2P file sharing of pirated material may be demonstrating tacit approval of this illegal activity.

In 2002, the RIAA settled a case out of court with an Arizona software company for \$1 million in damages, after alleging that the company had let its employees trade copyrighted files over its internal network.

Source: cnetnews.com

Newly released movies and books are also being pirated and shared via P2P. Movie and audio versions of the popular series of Harry Potter books can be easily obtained on file-swapping services such as Kazaa. The Motion Pictures Association of America says that 400,000 to 600,000 movies are distributed illegally around the world daily on P2P file-sharing networks.

Warner Bros.' fears that a pirated copy of the new Harry Potter flick would surface online were apparently well founded. In the days leading up to the film's release, and less than two weeks after its London premiere, file traders posted dozens of copies of Harry Potter and the Chamber of Secrets, the second installment in the popular series, on peer-to-peer networks.

Source: Wired.com

The Business Software Alliance (BSA) has estimated global losses due to all forms of software piracy at just over \$13 billion in 2002. The BSA's investigator easily located a P2P site offering multiple versions of popular (and expensive) titles like Macromedia's Dreamweaver, Adobe's Go Live!, and even a full version of Microsoft Office XP.

Distribution of inappropriate content

In addition to music files, many P2P networks are also used to share pornography, including illegal child pornography, as well as drug-related or violent materials. As some of this content is criminal in nature, employers may be held legally liable for the distribution and possession of such material and are also open to hostile workplace or sexual harassment lawsuits.

A recent study showed that 42% of all searches on one of the most common file sharing networks were for adult or child pornographic movies or images.

Source: Palisade systems, March 2003

⁸ Source: Palisades Systems

⁹ Source: TechNewsWorld

Employee productivity loss

In today's competitive corporate environment, reduced employee productivity can have a significant negative impact on a company's bottom line. The temptation for employees to use company resources for P2P file sharing is overwhelming. Employees want to take advantage of the available bandwidth on a company's network, where they can download a movie in an hour or so over high-speed connections instead of spending several hours for the same download from home. Unlike other Internet-based activity, time spent downloading, uploading, and viewing or listening to files from P2P networks has no business benefit. In fact, it is a complete waste of time—the company's time—as well as IT resources.

IT resource abuse

Intensive P2P file sharing negatively impacts the network performance, resulting in poor performance of business applications and often leading to employee calls to the organization's help desk.

Bandwidth consumption

P2P file sharing can severely limit available bandwidth on the network. Most of the content found in P2P networks is audio and video files. Audio MP3 files are typically 4MB or greater, while video files can easily reach 700MB. These files consume a great deal of bandwidth and can create bottlenecks and consume tremendous amounts of an organization's bandwidth.

In P2P networks, each client acts as a server. Network bandwidth is not only consumed by employees downloading files (an employee downloading the latest Harry Potter movie, for instance); it is also consumed by other P2P users outside the organization (for example, 10 other P2P users accessing the employee's shared folder and uploading the movie for themselves). This traffic places an undue burden on company systems, seriously impacting legitimate and business-critical applications.

What companies need

Companies need the ability to:

- Detect the extent of usage of P2P within their organization.
- Formulate policies regarding P2P usage, and educate employees on these policies.
- Stop existing P2P traffic in their enterprise network.
- Block the launch of P2P applications, even if the computer is not connected to the network.
- Prevent the downloading of P2P applications from the Internet.

Companies need Websense Enterprise, which provides all of these capabilities and more.

How Websense Enterprise addresses P2P vulnerabilities

Using Websense Enterprise, IT administrators can prohibit employee use of P2P applications within their organizations. Traditional firewalls and network security devices are not capable of identifying and stopping P2P activity without disrupting authorized activity. P2P applications, such as Kazaa, can dynamically choose an open port and are capable of tunneling over open ports such as port 80, which is generally used for legitimate HTTP traffic and therefore must be made available. Only Websense Enterprise provides a layered solution to help companies address P2P concerns in the most effective manner, by blocking P2P protocols at the network level and applications on the desktop.

Detect the usage of P2P file sharing—at the enterprise network level

Websense Enterprise helps identify potential problem areas with monitoring and reporting tools that offer real-time and historical views of company risks related to employee Web activities. The first step toward solving the problem of P2P file sharing in the enterprise is to understand the extent of its usage and impact.

Administrators can use the unparalleled reporting and analysis options available through Websense's three reporting tools—Reporter, Explorer, and Real-Time Analyzer—to easily generate real-time and historical reports on employee P2P file sharing. Forensics and analytics, along with “what if?” analysis, can be produced using Websense Enterprise Explorer.



Figure 1 Websense Enterprise Explorer detects P2P usage in the organization.

Reports can be scheduled for routine e-mail or intranet distribution to key recipients in IT, management, and human resources. In this way, management can attain a sense of how P2P is impacting the organization.

Stop existing P2P activity in the enterprise network

Websense Enterprise features the ability to stop P2P activity at the network level. Using Websense Enterprise Manager, IT administrators can set enterprise-wide policies to stop P2P traffic in their network. Thus, administrators can now control P2P protocols right at the corporate network and block employees' ability to share files over the corporate network.

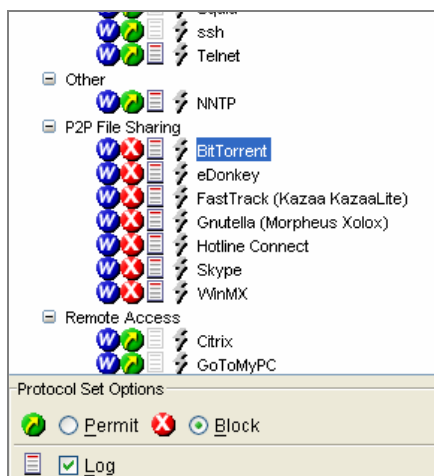


Figure 2 Setting policies using Websense Enterprise Manager blocks P2P file sharing on the network.

Websense Enterprise actively updates and delivers the latest protocols used by P2P applications with the daily download of the Websense Master Database. Thus, organizations can have complete confidence that their entire network is always protected from the threats of P2P application use. Once the policy of disallowing P2P use within the organization is set, it will be automatically enforced.

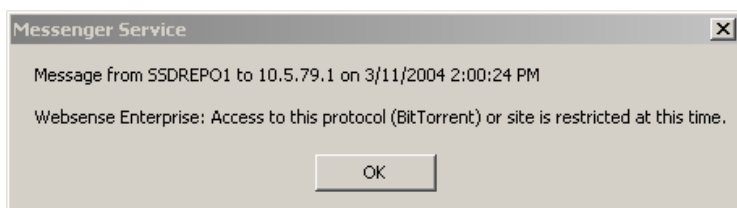


Figure 3 Websense Enterprise presents block message to employees trying to access P2P applications.

Block launch of P2P applications—at the desktop

With the Client Application Manager (CAM) module, companies can define policies that block the launch of P2P applications right at the desktop. This means that even if employees are running their laptops remotely, they will not be able to launch the applications. Instead, employees will receive the message shown in Figure 4.

CAM controls P2P use at the desktop even when a computer is disconnected from the company network. When an employee takes a company laptop away from the office and downloads a P2P client, he or she will not be able to launch the application. This capability is important for organizations that are concerned about the security threats posed by the downloading of files using P2P from remote locations, such as an employee's home or hotel room. These threats are real and significant, as the same computer may be connected to the organization's network and even though the user may not attempt to launch a P2P

application immediately, the downloaded P2P content may contain damaging malware, including worms, Trojan horses, or spyware that may propagate over the network.

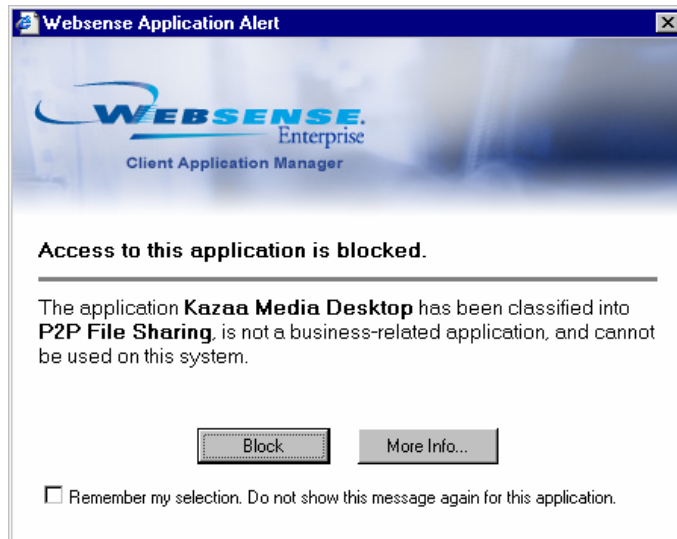


Figure 4 CAM blocks the launch of P2P applications on all employee computers, even when they are not connected to the network.

Prevent downloading of P2P applications

By blocking P2P activity in the network and prohibiting P2P application from launching, organizations successfully mitigate threats due to P2P applications. In addition, enterprises can prevent future problems by preventing employees from downloading P2P applications from P2P Web sites. The Websense add-on module, Bandwidth PG, blocks access to download sites and servers for P2P applications. Websense Enterprise makes it easy for IT administrators to block employee access to Web sites that contain P2P applications and block file attachments with popular formats of swapped files, such as MP3, .mpg, and .avi.

Allow access to P2P applications on a case-by-case basis

Although there is no business application for the use of P2P file sharing in most organizations, there may be cases where P2P applications should be made available to some employees. For example, a university may choose to allow P2P access for research purposes, or a company's IT Security department may need to investigate new P2P applications. Websense Enterprise's flexibility allows policies to be set on a case-by-case basis, so that exceptions like these can be handled easily. In these cases, policies can be set in Websense Enterprise to allow specific users or groups to access P2P Web sites and/or download and run client P2P applications.

The unique advantages of Websense Enterprise

Websense Enterprise provides a comprehensive solution for blocking P2P use and offers superior benefits and value over all other currently available solutions.

- **Complete coverage of P2P and other network protocols**—Websense Enterprise uses up to four different methods to identify network protocols: by port, destination IP address, user agent (a field that identifies the application), and signature (a pattern unique to the specific protocol). This ensures a high

degree of confidence that administrators have full network visibility and that all protocols are correctly identified, monitored, and controlled.

- **Automated dynamic protocol management**—Websense Enterprise’s list of network protocols can be updated as frequently as every night. During the nightly update of the Websense Master Database, the product also checks for updates to the network protocol database. Updates are added immediately when new or changed protocols are identified for an existing category (for example, if a new P2P client is released). This significantly reduces administrative overhead for IT administrators—since software upgrades are not required in order to manage new protocols—and provides a truly “dynamic” protocol database.
- **Included with Websense Enterprise**—The ability to block P2P protocols (as well as IM, spyware, and other protocols), by group or person, and by other integrated management options, is included with Websense Enterprise subscriptions.
- **Comprehensive solution for threats from employee computing**—The Websense product components that address P2P also effectively address other threats, including IM, spyware, and employee hacking, in addition to managing Web site access. Customers may use the same set of management and reporting tools to manage all the threats that result from the convergence of employee computing and the Internet, thereby maximizing their investments.
- **Additional layer of P2P policy management for mobile laptops**—Many organizations want to block P2P use on their mobile computing devices such as laptops when they are disconnected from the network. Websense Enterprise Client Application Manager provides this additional layer of security and policy enforcement for P2P, IM, spyware, and other applications. Without this additional and important protection layer, P2P threat mitigation cannot be complete.

Industry-leading integration and flexible deployment

As Figure 6 shows, Websense Enterprise offers integrated filtering at multiple points throughout the enterprise to provide complete protection against threats from P2P use. It allows organizations to easily assess risk areas, identify problem users, manage user and group privileges, and enforce corporate policies for appropriate use of the Internet and other computing resources, such as P2P.

Websense Enterprise integrates with a wide range of leading security and network products, including firewalls, proxy servers, caches, switches, routers, and appliances, providing organizations with flexible options for deployment in their network. The Websense Enterprise solution can be implemented in any of three ways, depending on specific network requirements: in an integrated, embedded, or standalone configuration.

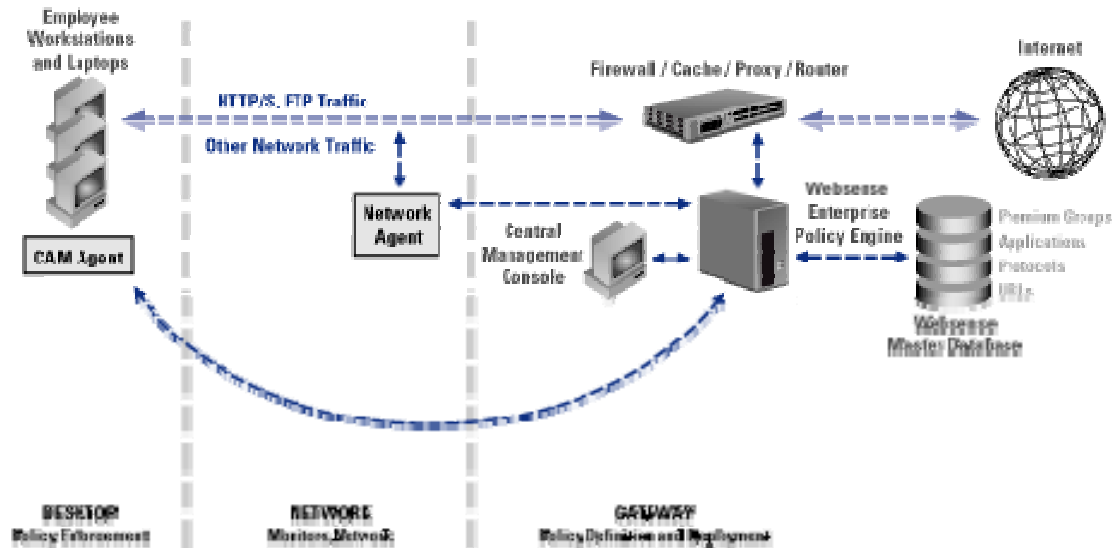


Figure 6 Websense Enterprise filters at multiple points on the gateway, network, and desktop.

Conclusion

When P2P networks and applications are used on an organization's equipment to swap files, organizations must be concerned about the files being shared and the resulting risks. Recent litigation with the RIAA has demonstrated clearly that organizations as well as individuals can and will be held accountable for unauthorized distribution of copyrighted materials. Organizations can be held accountable for the actions of their employees. Concerns about viruses, worms, Trojan horses, and spyware must also be taken seriously. Running P2P applications, downloading large files, and allowing fellow P2P users to upload files from employee's shared folders can slow down network performance and negatively impact the performance of business-critical applications. All of these threats are real and dangerous, and must be managed.

Websense offers a best-in-class solution that allows organizations to enforce flexible corporate policies at multiple points in their networks, resulting in layered, comprehensive protection from emerging threats. Websense offers the only such complete solution. Websense's solution also offers companies integrated reinforcement of their security infrastructure. Websense Enterprise is the only tool to help administrators easily, effectively and completely control P2P use within their organizations, including disconnected laptops.

For more information and to download a free, fully functional 30-day trial, visit www.websense.com/downloads.

About Websense, Inc.

Websense, Inc. (NASDAQ: WBSN), the world's leading provider of employee Internet management solutions, enables organizations to optimize employee use of computing resources with Web filtering in addition to mitigating threats related to Internet use including instant messaging, peer-to-peer, and spyware. By providing usage policy enforcement at the Internet gateway, on the network and at the desktop, Websense Enterprise enhances productivity and security, optimizes the use of IT resources and mitigates legal liability for our customers. Websense, awarded PC Magazine's Editors' Choice and listed on Forbes Magazine's 2004 "Top 25 Technology Companies," serves more than 20,600 customers worldwide, representing 16.4 million seats. For more information, please visit www.websense.com.

© 2004, Websense, Inc. All rights reserved. Websense and Websense Enterprise are registered trademarks of Websense, Inc. in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Appendix: The Websense Enterprise Solution

Websense Enterprise software enables organizations to manage the way employees use corporate computing resources, including the Internet and corporate desktops. Organizations of all sizes can optimize Internet usage, network protocols, and desktop application usage, via administrative options that define what may be accessed, by whom, at what time of day, and for what length of time. Other administrative management options include warning pages to notify employees that a requested Web site, protocol, or application may fall outside of their organization's defined usage policy.

The Websense Enterprise platform includes a highly accurate, award-winning database of categorized Web sites, network protocols, and desktop applications that is updated daily. Using this highly granular database, IT administrators can use the Websense Enterprise central management console to create employee-based policies to effectively:

- Manage employee Internet access.
- Manage instant messaging (IM) and IM attachments.
- Control P2P file sharing.
- Manage the use of streaming media and other high-bandwidth applications.
- Block spyware and malicious mobile code.
- Mitigate exposure during Zero Day malware attacks.
- Prevent employee hacking.

Websense Enterprise also provides the most advanced capabilities for detecting productivity issues and security risks arising from employee Internet and application use in an organization.

- **Websense Enterprise® Real-Time Analyzer™**

A Web-based real-time investigation and analysis tool for IT administrators that enables the analysis of Internet and network activity, including that which may be contributing to security risks or slow network performance.

- **Websense Enterprise® Explorer**

A powerful, Web-based forensics and analytics tool that provides a highly dynamic interface for analyzing employee use of computing resources. It removes bottlenecks caused by reporting processes that require IT to generate and deliver reports to various departments, supports role-based reporting, and is easy enough for corporate managers to use themselves.

- **Websense Enterprise® Reporter**

A full-featured reporting engine for IT administrators, with predefined and customizable report templates for viewing detailed, historical Internet-access and application-access data.

Websense Enterprise features the following value-enhancing modules to control P2P applications:

- **Websense Enterprise® Premium Groups™ (PG)**

Extends the URL filtering capabilities of Websense Enterprise by providing enhanced, high-value categories for productivity (Productivity PG), bandwidth conservation (Bandwidth PG), and security (Security PG).

- **Websense Enterprise® Client Application Manager™**

Delivers desktop protection from emerging and blended desktop security threats, such as virus outbreaks, spyware, P2P file sharing, IM, and employee hacking. Client Application Manager (CAM) mitigates costly security threats by blocking unauthorized and malicious applications from running on corporate PCs. Going beyond traditional firewall and antivirus tools, CAM shields the corporate network from internal security threats, resulting in zero-day threat response and higher employee productivity.

- **Websense Enterprise® IM Attachment Manager™**

Extends the IM management capabilities of Websense Enterprise by enabling organizations to effectively implement employee policies that oversee IM file attachments. IM Attachment Manager enables network administrators to define custom file attachment policies for any combination of IM client, users, groups, or workstations, using options such as time-based quotas, password authorization, and warn/continue.

- **Websense Enterprise® Bandwidth Optimizer™**

Adds adaptive policy enforcement to Websense Enterprise in response to changing real-time network conditions. Bandwidth Optimizer gives organizations the flexibility to permit non-business critical employee Internet activities until a predefined network bandwidth threshold is reached. When this threshold is reached, the activities such as viewing streaming media are temporarily restricted, to ensure ample bandwidth is available for business-critical applications. When adequate bandwidth becomes available, employees are automatically allowed to access high bandwidth applications.

Figure 5 summarizes Websense Enterprise and its associated modules.

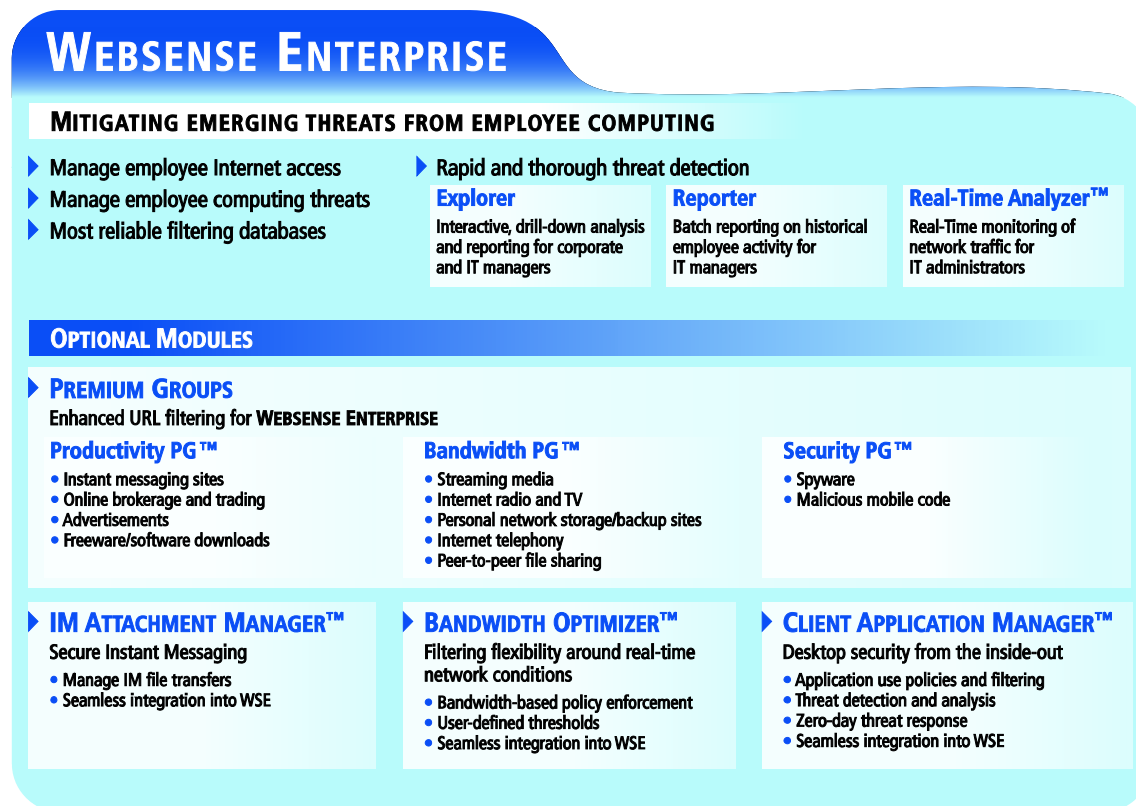


Figure 5 Websense Enterprise and optional modules