

Emerging Threats in Employee Computing

*Mitigating Risks in Today's
Corporate Organizations*

Abstract

Organizations face a complex challenge in securing the computing environment they rely on to conduct business. The employee computing environment has changed dramatically over time, offering access to rich content and tempting new applications on the Internet, as well as more powerful hardware and software solutions. Because of this evolution, organizations now must deal with even greater risks across key areas such as security, legal liability, productivity, and IT resources. Previously benign applications such as instant messaging and peer-to-peer file sharing can be diverted to nefarious purposes. Spyware, mobile malicious code, and hacking tools are becoming far more prevalent and accessible. Emerging threats in this new computing environment pose increasing challenges that IT needs to address.

This paper examines these emerging threats in detail and explains how Websense Enterprise can be used to combat them. Because Websense Enterprise filters at multiple points on the network, gateway, and desktop, this comprehensive solution can provide organizations with complete protection against the emerging threats discussed in this paper.

Websense, Inc.
World Headquarters
10240 Sorrento Valley Road
San Diego, California 92121
USA
Tel: 800.723.1166 or 858.320.8000
Fax: 858.458.2950
www.websense.com

Contents

Executive Summary	1
Background	2
The Emerging Threats	3
Instant messaging	3
Peer-to-peer applications	3
Spyware and malicious mobile code	4
Employee hacking	4
Streaming media	4
Complexities of today's threats.....	5
The Websense Enterprise Solution	7
Websense Enterprise overview.....	7
Unique advantages.....	9
Mitigating today's threats with Websense Enterprise.....	9
Instant messaging.....	9
Peer-to-peer applications.....	9
Spyware and malicious mobile code.....	10
Employee hacking.....	10
Streaming media.....	10
Industry-leading integration and flexible deployment	11
Conclusion.....	12
About Websense, Inc.	12

Executive Summary

The Internet has evolved over the years to become an essential resource for employees, enabling easy access to powerful new applications and information. At the same time, the number and power of computing resources available to the average corporate worker has increased dramatically. As a result, many organizations have adopted policies to manage Internet access and measures to protect against threats from external sources, such as viruses, worms, hackers, and malicious mobile code. These measures have included Internet management solutions that manage, monitor, and report on employee access to Web sites outside an organization's Internet use policy, including those containing spyware, malicious mobile code, and other inappropriate and dangerous material and applications.

Today's increasingly sophisticated and mobile, yet networked, employee workplace poses new threats to security, productivity, legal liability, and IT resource use—often introduced not from external, unknown sources, but from employees themselves. New worms and viruses are capitalizing on the growing use of instant messaging (IM) clients and peer-to-peer (P2P) networks, according to a recent Internet security threat report. Of the top 50 viruses and worms encountered in the Spring and Summer of 2003, 19 used P2P and IM applications—a 400 percent increase over all of 2002¹. Unbridled Web access exposes users to sophisticated attacks from spyware and malicious mobile code, and puts easy-to-use hacking tools at a disgruntled employee's fingertips. Streaming media, like many of these non-standard but enticing applications, continues to grow in popularity as an Internet-based application and, with the others, can impact productivity and drain corporate bandwidth.

As a result, organizations must extend their corporate acceptable use policies beyond the Internet to all computing resources that may present a threat directly or indirectly. Today's business computing environments require a new type of management solution, one that focuses on employee use of corporate computing resources. Websense Enterprise[®], the leading Internet filtering solution, provides organizations with a comprehensive strategy and platform for managing the new threats arising from employee use of computing resources.

¹ Symantec Internet Security Threat Report, October 2003.

Background

Almost from the inception of Internet use, organizations have recognized the need to establish employee Internet access policies and implement security measures to protect themselves from the Internet and its inherent risks. Companies have been concerned—justifiably so—about the effect of Internet access on employee productivity and IT resources. They have also acknowledged the necessity of establishing computing use standards to protect against legal liability concerns and to ensure the security of the organization’s computing environment. One way that organizations have enforced these use standards has been the deployment of filtering solutions to actively manage or block access to sites deemed to be outside the policy.

As the Internet continues to evolve, the computing resources readily available to employees have also changed dramatically, leading to new IT management challenges that require solutions beyond simply Web filtering. In the early days of the Internet, the browser was virtually the only tool used to access information. Employees are now accessing a variety of content using new applications aside from the browser, such as real-time streaming media players, instant messaging (IM) clients, and peer-to-peer (P2P) networks.

Corporate computing environments now include PCs and storage devices with increasingly more powerful processors, CD-ROMs, and hard drives, encouraging the installation of software and the storage of personal files on corporate assets. It has also become quite common for organizations to provide their employees with powerfully equipped laptop computers, making it easier for employees to work in less-managed environments, such as at home or on the road.

“Three out of every four home and work Internet users ... access the Internet using a non-browser-based Internet application. Media players, instant messengers and file sharing applications are the most popular Internet applications.”

(Nielsen/NetRatings, December 30, 2003)

What do all these changes mean to the organization? Essentially, corporate IT organizations face a growing management challenge, as the installation of unauthorized software by employees changes the standard configuration of corporate desktops and mobile computers become “perimeter killers” that can introduce threats into a corporate network, effectively bypassing the traditional security infrastructure found at the network perimeter.

These changes introduce the following emerging threats to the organization computing environment from employees, *not outsiders*:

- Instant messaging
- Peer-to-peer applications
- Spyware and malicious mobile code
- Employee hacking
- Streaming media

The Emerging Threats

Most organizations view security threats from an “outside-in” perspective: ‘How can we protect our corporate computing environment from risks and threats from the outside world?’ Organizations deploy or configure firewalls, demilitarized zones, and intrusion detection systems, and implement a myriad of other security devices in an attempt to stop intruders from entering their corporate networks.

As we’ve discussed, there are significant emerging threats to security that are not being introduced from external, unknown sources, but from employees themselves. It’s critical that organizations acknowledge these “inside-out” risks.

Instant messaging

Less expensive than the phone and quicker than even email, instant messaging (IM) allows employees to easily communicate with other IM program users in a kind of private chat room. Most employees are using public IM chat tools from AOL, MSN, and Yahoo! to communicate with both colleagues and company outsiders. This presents significant challenges to IT organizations because, in addition to being a potential productivity drainer, public IM tools can relay company-confidential information over the Internet and contain exploitable vulnerabilities, making them a serious security threat to an organization.

Peer-to-peer applications

Peer-to-peer (P2P) applications like Kazaa make it possible for a user on one computer to directly access files—such as MP3 music—on another user’s computer anywhere on the Internet and download them. P2P application use is extremely popular² and is not solely a home-use phenomenon. A survey by AssetMatrix in July 2003 showed that 77% of companies had detected at least one P2P file-sharing application on their network³. With little, if any, business justification for P2P networks in the organization, organizations face a significant security threat, in addition to the threats of network bandwidth misuse and legal liability.

Forty-five percent of the executable files downloaded through Kazaa, the most popular file-sharing program, contain malicious code like viruses and Trojan horses.

(TruSecure study, January 2004)

In October 2002, the RIAA, along with the Motion Picture Association of America, the National Music Publishers’ Association and the Songwriters Guild of America, sent letters to Fortune 1000 companies warning that they are at risk when employees illegally distribute copyrighted works over corporate networks.

(Raleigh News & Observer, January 14, 2004)

² Kazaa, the most popular gnutella-based P2P network, is the most searched term on the Internet, as well as the most downloaded executable. Search term statistic as reported by Yahoo!: <http://search.yahoo.com/top2003>. Download statistic as reported by Downloads.com in December 2003.

³ “Corporate P2P Use Is Common, Study Says”, c|net News.com, July 16, 2003.

Spyware and malicious mobile code

Spyware is any technology used to gather information about users or their activities, secretly or without consent, and relay that information to interested and potentially undesirable third parties over the Internet. These programs are often downloaded automatically and unintentionally from Web sites or P2P sites. Examples of spyware include adware, Web bugs, and tracking cookies. Although many of these programs are harmless and simply annoying, some more insidious spyware, such as keystroke loggers, records and transmits information about keystrokes and specific user actions on the computer to outside third parties. Since keystrokes and user actions can include usernames and passwords, bank account numbers and PINs, or other access codes, these programs pose a significant security threat to the organization and, depending on the information relayed, may present a legal concern as well.

Similar to spyware, malicious mobile code (MMC) can infect an end user's computer simply by visiting the URL to the Web site that distributes it. Perhaps the most well known example of this type code was the Nimda worm that spread throughout the Internet in 2002. Among other means of distributing itself, Nimda could infect computers that merely visited Web sites which had its payload embedded as an ActiveX component. MMC includes any executable delivered via a Web site that changes system settings without the end user's knowledge or approval. The consequences of MMC are as variable to an organization as the nature of the payload and can result in anything from a security threat to a legal liability concern.

Employee hacking

Organizations have always been concerned about the ability of outsiders to "hack" into their computing environments and gain access to proprietary information. Interestingly enough, the threat of hacking is primarily a threat from the *insider*. In fact, security experts often say that over 70% of hacking exploits are from insiders.⁴ Employee hacking is a bigger problem than ever before, because dangerous "how-to" information is now so readily available and easily accessible over the Internet. Newly available hacking portals target novice users and offer tools such as scripts and programs, as well as message boards that would-be hackers can use to learn about and discuss their hacking exploits.

45% of companies have suffered an unauthorized access by an insider in the previous 12 months.

(Source: 2003 CSI/FBI Computer Crime and Security Survey)

Motivated employees can find ingenious ways to access information to which they should not be privy—private customer data, confidential corporate information, or intellectual property, to name just a few. And employees willing to go to such lengths to obtain this type of information almost never keep the information to themselves, thus presenting a legal risk from the information breach to compound the security risk.

Streaming media

Streaming media includes interactive and high-bandwidth applications that use the Internet to run. Media players, Internet radio, and Internet television are three examples. While it may be useful for employees to view Web-based training sessions on their office computers, it is difficult to see the company benefit of employees watching concert highlights or clips from their favorite TV shows. When used inappropriately,

⁴ Based on informal consensus. An Information Week Global Information Security Survey in November 2003 found the figure to be 30% based on a formal survey of security experts.

streaming media also presents a risk to organizations in the IT resource domain, as precious network bandwidth is consumed by non-work-related activity, thus adversely impacting business-critical applications.

As seen from the discussion above, these threats can pose risks to employee productivity, legal liability, IT resource use, and security. The following table summarizes the many activities and actions that employees engage in and assesses the corporate impact and risks associated with them.

Emerging Threats in Employee Computing

Activity / Application	Threat	Corporate Impact / Risk
Instant messaging	Introduction of viruses, worms, or Trojan horses to corporate network	Security (high)
	Interception of confidential information (customer, privacy, IP, financial disclosure)	Security (low)
	Introduction of illegal or inappropriate content into corporate environment (through file attachments)	Legal liability (moderate)
	Employee distraction	Productivity (high)
Peer-to-peer application use	Introduction of virus or worm into corporate network	Security (high)
	Lawsuit from illegal exchange of copyrighted digital material on corporate network	Legal liability (low)
	Saturation of network bandwidth (possibly impacting business-critical applications)	IT resource (varies)
	Probability of pornography (possibly child porn) existing on the corporate network	Legal liability (high)
Spyware and malicious mobile code	Interception of system password through keystroke logging program (possible use in identity theft)	Security (low but increasing)
	Transmission of sensitive data to outside party	Security (high)
	Non-optimal utilization of network bandwidth or desktop CPU cycles	IT resource (high)
Employee hacking	Unauthorized access to systems by an insider	Security (high)
	Confidential customer information security breach (possible use in identity theft)	Security (varies)
	Theft of corporate secrets or valuable confidential information	Security (varies)
	Legal liability from affected outside parties	Legal liability (moderate)
	Damage to computing systems by hacker	IT resource (moderate)
	Public disclosure of executive compensation packages and bonuses	Security (low)
	Saturation of network bandwidth	IT resource (varies)
Streaming media	Employee distraction and loss of productivity	Productivity (moderate)
	Legal liability from viewing of or listening to illegal copyrighted movie or material	Legal liability (low)
	Installation/execution of unauthorized applications	IT Resource (high)
Installation/execution of unauthorized applications	Desktop incompatibilities	IT Resource (high)
	Use of pirated/unlicensed software programs	Legal liability (high)

Complexities of today's threats

The emerging threats described above are becoming increasingly complex and difficult to resolve. Like the newest viruses and worms, the threats can be blended, where one threat facilitates another. For example, although an organization may have policies in place to stop the use of traditional hacking tools on unauthorized systems, an employee hacker might use a keystroke-logging application (a form of spyware) to uncover a colleague's password and thus gain access to unauthorized information.

Consider the following additional scenarios that demonstrate the comingled and compounding nature of the emerging threats:

- **Spyware:** An organization sets URL policies to block access to spyware Web sites. Spyware is still acquired when an employee downloads a P2P application on a corporate desktop.
- **Pornography:** An organization protects itself from pornography using Web filtering at its Internet gateway, but encounters a problem with pornography when an employee receives porn images as file attachments while using a public IM application.

In addition, the emerging threats may originate from employee use of various computing resources. Consider the following scenarios:

- **Remote use:** An employee takes a laptop home and visits a Web site with malicious mobile code. When the employee reconnects the laptop to the organization's network upon returning to work, the malicious code—a virus—quickly spreads throughout the corporate network.
- **Unauthorized installation of desktop software:** An employee uses the CD-ROM drive on his or her desktop to load a powerful hacking application, increasing the threat of a successful employee hacking exploit, despite the fact that anti-hacking Internet access policies are in place.

As the above scenarios illustrate, these threats necessitate new, forward-thinking requirements in a solution. Their blended nature requires a solution that manages and solves all employee computing threats, not just one. The solution must also be capable of enforcing policies beyond simple Internet access, covering all computing resources to which employees have access.

The Websense Enterprise Solution

Websense Enterprise overview

Websense Enterprise software enables organizations to manage the way employees use corporate computing resources. Organizations of all sizes can optimize the use of the Internet, network protocols, and desktop applications by employees by means of 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 their organization's defined use 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. Relying on this database, IT administrators can use the Websense Enterprise central management console to create employee-based policies to effectively:

- Manage employee Internet access.
- Manage 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 hacking.

Websense Enterprise also provides the most advanced capabilities for detecting productivity issues and security risks arising from employee use of the Internet and computer applications.

- **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 those problematic activities that 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 generate reports independent of IT staff.
- **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 Policy Manager™**

Delivers zero-day protection against unknown security threats, including today's sophisticated malware at desktops, laptops, and servers. CPM stops the execution of unauthorized applications such as spyware, P2P file sharing, and hacking tools, while enabling flexible policy management of applications such as instant messaging or remote access tools, which only designated users or groups are allowed to use. Only CPM enforces employee application use policies for corporate desktops, laptops, and servers with its unique and comprehensive database of categorized applications, which is updated daily. Complementing traditional firewall and antivirus tools, CPM closes the window of exposure to today's fast-moving blended security threats.

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

Extends the IM management capabilities of Websense Enterprise by enabling organizations to effectively implement 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, activities such as viewing streaming media are temporarily restricted, helping to ensure that ample bandwidth is available for critical business applications. When adequate bandwidth becomes available, employees are automatically allowed to access high-bandwidth applications.

Figure 1 summarizes Websense Enterprise and its associated modules.

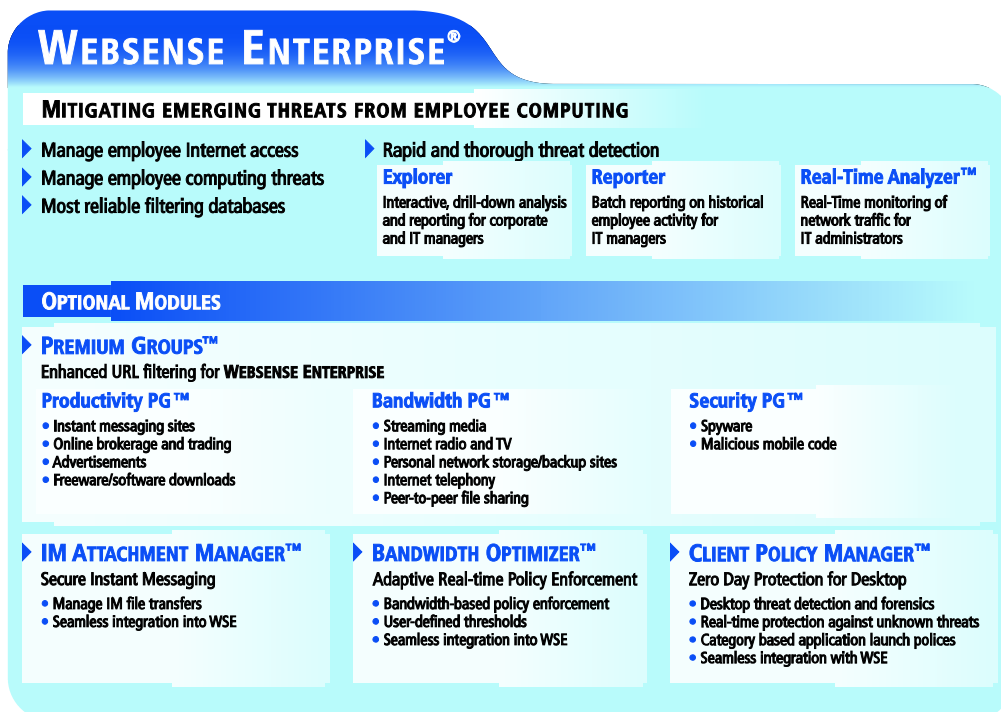


Figure 1 Websense Enterprise and optional modules

Unique advantages

Websense Enterprise provides a comprehensive solution for managing emerging threats, including:

- **The highest-quality filtering product available today**—The Websense Enterprise URL, Protocol, and Application databases take advantage of the company's unique strengths in information retrieval and classification, and provide organizations with the most reliable filtering solution available.
- **Multi-layer protection for comprehensive employee computing threat mitigation**—Administrators can enforce computing-use policies at the gateway, network, and desktop to combat threats that can originate from multiple points across the corporate network.
- **State-of-the-art end-point security**—Websense Enterprise includes an optional module, Client Policy Manager, a unique security offering for desktop clients that protects organizations from security threats from the inside out.
- **Unmatched threat detection and reporting**—Websense analysis and reporting modules provide corporate managers and IT administrators with the most innovative and extensive capabilities for identifying, analyzing, and reporting on Internet activity, application usage, and the overall risks associated with employee computing.

Mitigating today's threats with Websense Enterprise

Let's explore how Websense Enterprise helps administrators manage specific threats from employee computing.

Instant messaging

Most organizations are unaware of just how much instant messaging occurs on their corporate networks. Websense Enterprise enables IT departments to manage IM in their organizations and provides powerful, organization-level reporting on instant messaging use that identifies users, bandwidth, and protocols used.

Unlike other security threats, instant messaging can play a positive role in the organization, allowing instant customer credit approval by a customer service representative or a price check by a commodities broker on the phone with an investor. Instead of completely blocking its use, many organizations may elect to manage its use. Because of this, managing IM requires a flexible solution. Websense Enterprise allows administrators to limit employee use to only the specific IM tools they deem secure, and also allows administrators to assign IM usage rights to only specific users or groups within the organization. In addition, administrators have the flexibility to permit instant messaging and only block IM traffic during peak bandwidth loads, reserving traffic for higher-priority, business-critical processing (using Bandwidth Optimizer).

Peer-to-peer applications

Websense Enterprise provides administrators with comprehensive and scalable methods to manage employee P2P activity. With Websense Enterprise, administrators can limit access to Web sites that contain P2P applications and block file attachments to popular formats of swapped files, such as MP3, .mpg, and .avi. Websense Enterprise features the ability to detect and block P2P activity by protocol, thus providing administrators with ultimate control over an employee's ability to share files over the corporate network.

Instant messaging

One in every five corporate users is using public IM tools.

Peer-to-peer file sharing

77% of companies have at least one P2P file sharing application on their network.

Spyware and malicious mobile code

As many as 9 out of every 10 computers are infected with spyware.

More than 2 million servers and PCs were affected worldwide by the Nimda virus.

Employee hacking

In the last 12 months, 45% of businesses detected unauthorized access by insiders.

Streaming media

To completely block P2P file sharing and storage of illegal copyrighted materials on corporate-owned PCs and networks, administrators can use Websense Enterprise's Client Policy Manager to block the launch of a P2P application at any time, particularly during connection to the Internet from outside the corporate gateway.

Spyware and malicious mobile code

One of the biggest challenges associated with spyware is actually identifying the type and potential impact of the spyware. Most spyware detection software is designed for single PC use. Websense Enterprise allows administrators to view spyware activity such as HTTP activity, and spyware application launches at the organization level, so administrators can view their spyware exposure globally and respond quickly.

The spyware category in Websense Enterprise includes adware, Web site tracking software, and keystroke logging applications. The Security PG module in Websense Enterprise enables administrators to set policies that make spyware Web sites off limits to end users, and eliminates transmissions from spyware programs to their hosts, should corporate PCs become infected while outside the corporate network. For ultimate protection and spyware reporting, administrators can use Client Policy Manager to generate reports summarizing spyware activity and completely block spyware applications from running on any PC.

Websense Enterprise also scans over 13 million lines of code a day in order to identify malicious mobile code from Web sites on the Internet. Websense is the only vendor with a solution that scans the Internet and categorizes Web sites based on potentially dangerous executable elements.

Employee hacking

Websense Enterprise helps stop hacking by arming IT organizations with unique tools to block the most potentially dangerous hacking culprit—the employee. Web sites containing hacking information or programs can be made off limits entirely. Websense Enterprise reports also easily identify the employees who attempt to visit hacking sites.

For increased protection, organizations using Client Policy Manager can find out more about potential employee hackers in their environment and set more rigid policies to curb these employees' activities. The ability to search by unique software categories allows administrators to identify employees who have run hacking tools or have hacking programs installed on their desktops. Using this information, administrators can take proactive steps to avoid a security break-in such as setting a policy to block access to sites with hacking scripts or applications, making it harder for a malevolent employee to access dangerous information or tools. For complete protection against a hacking attack from within using a corporate PC, Client Policy Manager can completely block the launch of hacking programs on any managed PC.

Streaming media

Websense Enterprise provides a number of different options for defining corporate use policies for streaming media. In most cases, a connection to the site that is streaming data must be constant. Using Bandwidth PG (a part of Websense Enterprise's Premium Group family), IT administrators can set a policy to completely block access to the streaming source sites, effectively blocking the use of streaming media in the organization. For some organizations, this level of policy may be too restrictive. In these cases, a policy can be established that blocks only certain file types (for example, media types) and not others. As a result, only the transmission of media files is prevented, but content on a site containing streaming media can remain available.

Additionally, administrators have the choice of using Bandwidth Optimizer to allow streaming media when network bandwidth conditions allow it. Bandwidth Optimizer automatically manages network traffic in real time,

ensuring that business-critical applications are given priority to network resources, including the capability to temporarily disable non-business-related traffic, when network usage thresholds reach certain levels.

Employee use of streaming media applications can also be controlled through the use of Client Policy Manager, where policies can be set for the desktop that prohibit the use of media players and other unauthorized, high-bandwidth applications. Should high-bandwidth applications be needed for work-related activity, the Client Policy Manager offers a “continue” option that employees can choose when appropriate.

Industry-leading integration and flexible deployment

As Figure 2 shows, Websense Enterprise offers integrated filtering at multiple points throughout the organization 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.

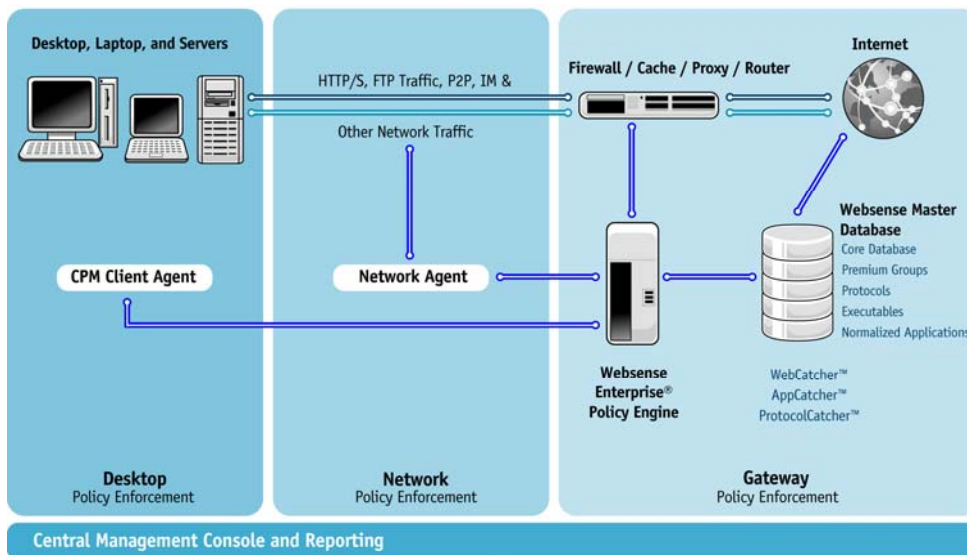


Figure 2 Websense Enterprise filters at multiple points on the gateway, network, and desktop.

Conclusion

Organizations face a growing number of risks associated with the intersection of the Internet and employee use of corporate computing resources. With the aggressive growth projections for future use of applications such as instant messaging, P2P applications, and spyware, the challenge to IT organizations to manage these threats will only become more and more daunting in the future.

Organizations must implement a solution that defends against the increasing risks from use of the Internet and other computing resources in their environments. As this paper has shown, these risks pose real threats to security, in addition to traditional concerns around productivity, legal liability, and misused IT resources (including network bandwidth).

Websense Enterprise provides a premier solution that allows organizations to enforce corporate policies at multiple points in their networks, resulting in comprehensive protection from emerging threats, and offers an integrated way for organizations to reinforce their security infrastructure.

For more information and to download a free, fully functional 30-day trial, [click here](#).

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 and mitigate new threats related to Internet use including IM, P2P, and spyware. By providing policy enforcement at the Internet gateway, on the network, and at the desktop, Websense Enterprise software enhances productivity and security, optimizes the use of IT resources, and mitigates legal liability for our customers. Websense serves more than 21,200 customers worldwide, representing 16.8 million seats. For more information, 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.