

Instant Messaging: An Instant Threat

Abstract

Instant messaging (IM) applications allow employees to easily communicate and share files with other IM users in a real-time session similar to a private chat room. Employees use public IM applications such as AOL, MSN, Yahoo!, and ICQ to communicate with both fellow employees and company outsiders.

In addition to being a potential drain on productivity, public IM tools used in a corporate environment can be used to relay company-confidential information over the Internet, undetected by IT administrators. When used to send file attachments, the tools themselves are also inherently vulnerable to viruses, worms, and Trojan horses, making them a serious security threat to an organization.

In an organization where IM is used for personal use only, the solution seems simple: disallow IM use completely. But in environments where IM communication is part of the corporate culture and presents significant business advantages, organizations need a more flexible solution. Websense Enterprise® allows organizations to set policies for IM use: which IM tools can be used, which specific users or groups of users should be given access to IM, and whether and when IM attachments should be allowed.

Contents

Executive Summary	1
Introduction	2
Challenges With IM Use in Organizations	3
Security threats	3
IM vulnerable to hackers	3
Viruses, Trojan horses, and worms	4
Loss of intellectual property, confidential data	4
Legal liability concerns	4
Employee productivity loss	5
IT resource abuse	5
What organizations need	5
How Websense Enterprise Addresses IM Vulnerabilities	6
Detect threats and analyze IM use at the organization level	6
Set granular policies across multiple points in the network	6
Safeguard the organization with Websense Enterprise IM Attachment Manager	6
A winning combination	6
Corporate IM standardization	6
Internal and external communications	7
Monitoring and managing	7
The unique advantages of Websense	8
Industry-leading integration and flexible deployment	9
Conclusion	10
About Websense, Inc	10
Appendix: The Websense Enterprise Solution	11

Executive Summary

Use of instant messaging (IM) in the corporate environment is rising steadily, as organizations come to accept IM as a viable communications tool. IM promotes collaboration and real-time communication among employees, business partners, and customers. It also introduces new threats to corporate network security and subjects organizations to potential liability risks when employees share illegal or inappropriate content via the corporate network. Organizations are also faced with reduced employee productivity when IM is used indiscriminately and for personal communications. When IM use is unmonitored and uncontrolled, it can result in a significant drain on IT resources, as the IT staff struggles to identify which IM applications are being used and by whom. And, when instant messaging is used to send and receive files, not only can the resulting drain on bandwidth negatively impact network performance, but the files themselves can pose a serious security threat.

To address these concerns, organizations need the ability to set and enforce policies for IM use within their organizations. Websense Enterprise®, the leading Internet filtering solution, provides organizations with a comprehensive platform for managing today's growing list of employee computing risks and challenges. The Websense solution includes an award-winning database of categorized Web sites, network protocols, and desktop applications that is updated on a daily basis. Using this highly granular database, IT administrators can create employee-based policies to control what Internet-based content may be accessed, at what time of day, and for how long. Websense Enterprise, as a core component of its integrated offering, provides administrators with the ability to manage IM within their organizations. Additionally, with the Websense Enterprise® IM Attachment Manager™, company-sanctioned IM applications can continue, while file transfers via IM are filtered out. Organizations are protected from the security, legal liability, and bandwidth concerns associated with IM attachments, while supporting and managing the real-time collaboration benefits of IM.

Introduction

IM applications have rapidly become accepted by businesses as viable employee communications tools. IM is more immediate than email, remarkably easy-to-use, and provides the real-time collaboration organizations need to ensure quick decisions.

Using IM, remote workers and business partners can "talk" and share files and information effortlessly over the Internet. And, within the organization, IM conversations among project team members can resolve issues and questions in an instant—something that might have taken a series of emails, telephone calls, or face-to-face meetings to accomplish. IM can be used to provide immediate replies to requests. It can also help promote personal relationships with customers and remote employees, and assist customers in completing transactions with Web-based businesses.

Most importantly, unlike email and the telephone, IM introduces the concept of "presence," enabling 400

users to be aware of the availability of others in real-time. Communications can be timed

accordingly, without needing to call or email several times to connect with someone. For many day-to-

email or phone communications. Instead, it

provides a complementary communications channel to the established system.

IM use in the corporate environment is rising steadily. Some 70 percent of all organizations will use IM in some form this year, according to market research firm Gartner.¹ And IDC estimates that

already 29 percent of traffic on today's consumer IM networks is for business use.

Figure 1 illustrates the projected, burgeoning use of IM by businesses.

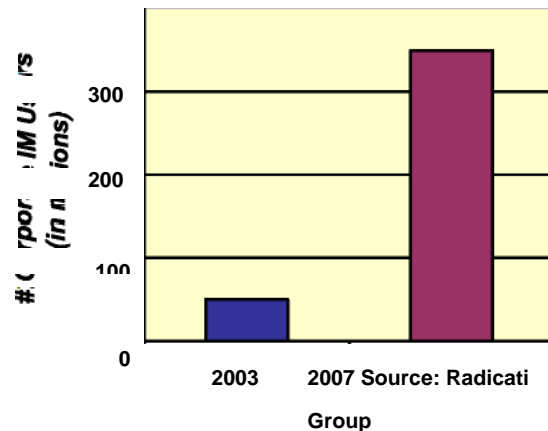


Figure 1 IM use projected to increase sevenfold by 2007

¹ Source: <http://comment.cio.com/comments/10296.html>

Challenges With IM Use in Organizations

IM promotes collaboration and community building among employees, partners, and customers, which can result in significant business benefits. Despite such benefits, however, many organizations are hesitant to adopt IM because of the threats and inefficiencies that unmanaged IM usage can introduce, including:

- Security threats
- Legal liability concerns
- Employee productivity loss
- IT resource abuse

Security threats

Most of the free public IM systems were designed with the consumer market in mind—enabling teenager chats

and online personal connections. With these consumers in mind and in an effort to gain and retain market share, IM vendors are adding more and more features to their

IM applications. Marketability—not security—has been the primary consideration, with designers electing not to include significant security measures within these

consumer-centric applications.

Despite the growing adoption of this originally consumer-centric application by employees, as Figure 2 shows, a wide range of concerns still exist, with security foremost

among them.

IM vulnerable to hackers

Hackers can easily take advantage of IM vulnerabilities, including buffer overflow or cross-site scripting, to spread

worms, Trojan horses, and viruses. Here are some examples:

Attackers may trigger a buffer overrun on machines running Yahoo!® Messenger by sending a long stream of data in the form of a Web page URL to a vulnerable function in `yauto.dll`, crashing the application or allowing the attacker to place his or her own malicious code on the machine.

Buffer overflow vulnerability in the ActiveX control for MSN® Messenger (versions 4.5 to 4.6) could allow an attacker to supply arbitrary code, and have it executed under the privilege of the current user.²

Vulnerabilities in public IM networks occur during the process of transferring files. When a user transfers files or uses other IM features like file sharing or voice chat, his or her IP address is revealed. Using this IP address, hackers may potentially focus on attacking the system.

Some organizations configure their firewalls to block ports used by IM applications or block the external addresses of IM network servers. But IM applications can be configured to change ports automatically and are

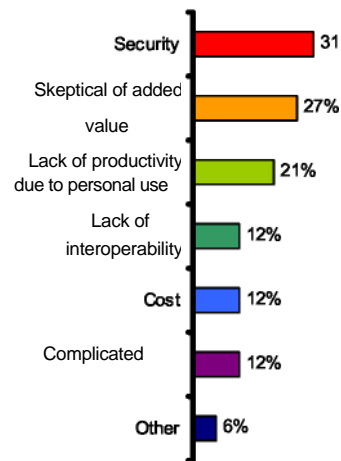


Figure 2 Concerns relating to IM use in the workplace

1 Source: PC World - <http://www.pcworld.com/news/article/0,aid,113723,00.asp>

2 Source: eEye Digital Security - <http://www.eeye.com/html/Research/Advisories/AD20020508.html>

capable of penetrating firewalls through ports used by other applications (port 80, for example). A simpler, automated, and comprehensive IM management solution is required.

Viruses, Trojan horses, and worms

As in the case of email and peer-to-peer (P2P) file sharing, viruses, Trojan horses, and worms can hitch a ride on IM attachments and make their way into corporate networks. Many IM clients allow users to send files directly to each other, effectively circumventing perimeter security mechanisms, such as firewalls and antivirus scanners deployed at the network perimeter, email gateways, or email servers, and enabling viruses to easily penetrate and then propagate within a network.

Here are a few examples:

The w32.Choke.worm used MSN Messenger to send itself as a reply to incoming messages.³

The Aplore worm spread using AIM[®] by asking users to click a link to a worm residing on a remote server.⁴

The Goner worm, which is capable of deleting certain computer programs, distributed itself through online chat program ICQ[®].⁵

The Fizzer worm used IM as a backup for its email infection. It entered via email, but was capable of spreading via IM through a user's IM contact list (e.g., "Buddy" list).⁶

Two new viruses, smbmsn and Jitux, hijack MSN Messenger accounts and distribute copies of themselves to everyone on a user's IM contact list.⁷

"In its latest Internet Security Threat Report, [Symantec] found that, of the top 50 virus threats during the first six months of the year, IM and peer-to-peer technology played a role in 19—a 400 percent increase from the previous year." (Report: IM Viruses on the Rise, October 1, 2003, Christopher Saunders)

Loss of intellectual property, confidential data

Organizations face a significant security risk from disclosure of intellectual property or business-critical information using IM's file attachment capability. Because IM is a highly informal means of communication, employees can inadvertently or otherwise send critical company-confidential information, such as product specifications, code, and blueprints, or private customer data, to friends, colleagues, and competitors. The growth of IM usage within the organization, and the potential for sustaining material damage, has rendered this issue a problem worthy of inclusion in every organization's security strategy.

Legal liability concerns

The danger of allowing employees to use IM at work goes beyond the ominous exposure to viruses and worms. Organizations face legal and, in many cases, compliance risks when employees share copyrighted, illegal, or inappropriate content via corporate networks. Unmonitored IM applications allow employees to freely transfer files and information that could lead to significant corporate liability. Transferring copyrighted MP3 files, movies, and software using IM is common among friends and bypasses the file size restrictions of email.

3 Source: Symantec Security Response - <http://www.symantec.com/avcenter/venc/data/w32.choke.worm.html>

4 Source: Symantec Security Response - <http://securityresponse.symantec.com/avcenter/venc/data/w32.aplore@mm.html>

5 Source: CERT Coordination Center - http://www.cert.org/incident_notes/IN-2001-15.html

6 Source: F-Secure - <http://www.f-secure.com/v-descs/fizzer.shtml>

7 Source: IM Planet - <http://www.instantmessagingplanet.com/security/article.php/3295441>

Even in environments where IM is permitted, managing IM attachments is a requirement if organizations are to reduce their liability risk.

Employee productivity loss

Many employees have adopted IM as their preferred means of personal communications with friends and family, because it is not as obvious as using the telephone and conversations cannot be overheard. Employees can appear to be working, typing away at their keyboards, all the while exchanging personal communications with friends and family.

A recent study by dating site Lavalife found that 52 percent of its users who are single office workers admitted to using IM for personal use during the business day.

In today's competitive corporate environment, reduced employee productivity can have a significant negative impact on a company's bottom line.

IT resource abuse

Most organizations have no idea which IM clients are installed on desktops, which employees are using IM, or how often. Nor do they know *how* employees are using IM—to communicate for business, to communicate for personal use, or to send or receive files, applications, videos, etc. Unsanctioned IM applications can increase the support costs of employee desktops since they are not centrally managed. In addition, it is not uncommon for intensive file sharing via IM applications to negatively impact network performance, resulting in poor performance of business applications. Attempts to block IM clients at the firewall—as many organizations try to do—are wholly inadequate, and an overwhelming task for the IT staff. Central management of IM is mandatory.

What organizations need

To summarize, use of consumer IM solutions in the organization presents organizations with significant risks and exposures; therefore, employee use of instant messaging must be managed. Manual attempts at IM management, such as implementing firewall policies, are inadequate. Organizations need the ability to:

- See which IM applications are being used, by whom, and for what purposes.
- Set and enforce policies about which IM applications are acceptable and which should be banned.
- Set and enforce policies about who can use IM, when, and for how long.
- Allow or prevent employees from sending and receiving IM file attachments.

Organizations need Websense Enterprise, which provides all of these abilities and more.

How Websense Enterprise Addresses IM Vulnerabilities

Using Websense Enterprise, IT administrators can manage how employees use IM within their organizations. Websense Enterprise provides a layered solution to help organizations address IM concerns in the most effective manner.

Detect threats and analyze IM use at the organization level

Using Websense Enterprise's comprehensive reporting tools (Explorer, Reporter, and Real-Time Analyzer), administrators can first detect and analyze IM usage.

Set granular policies across multiple points in the network

Appropriate policies can then be set for any combination of users, group of users, workstations, or networks. Productivity PG can also be used to block access to IM Web sites, and administrators can use Client Policy Manager to block the launch of unsanctioned IM applications on all desktops—even on laptops when they are not connected to the network.

Safeguard the organization with Websense Enterprise IM Attachment Manager

The IM Attachment Manager module offers exceptional granularity of control by allowing IT administrators to specify whether employees are allowed to exchange files using the accepted IM clients. This level of management control is critical for organizations that endorse or at least accept IM use, but also want to reduce the risk of viruses and other corporate and technical maladies associated with the transfer of file attachments.

A winning combination

The combination of Websense Enterprise with the IM Attachment Manager gives organizations of all types, sizes, and configurations a great deal of flexibility. Websense administrators can create IM attachment policies based on:

- Individual employees
- Group / department
- Time of day, day of week
- Specific IM client
- Available bandwidth

The examples that follow demonstrate Websense Enterprise's flexibility and capabilities in greater detail.

Corporate IM standardization

Many organizations want to take advantage of the business benefits of IM but understand the need to control its use within their networks. Written corporate IM guidelines often restrict employee use to a specific IM client, so the IT/Help Desk staff can focus on supporting a single application, instead of five or six disparate IM clients. Using Websense Enterprise, an administrator can create a policy that enforces this rule, restricting usage to a single, corporate-sanctioned IM client, such as AOL® Instant Messenger, while blocking all others. The policy can be further refined so that only certain departments or groups of employees are able to use AOL Instant Messenger, while other groups—those without a business need for IM use—are blocked from all IM usage.

The administrator also has the option, using the IM Attachment Manager, of allowing chat conversations with AOL Instant Messenger but disallowing the transfer of files via IM. This powerful combination enables the real-time collaboration benefits of IM, while ensuring that security, liability, bandwidth, and productivity threats related to IM file attachments are effectively mitigated.

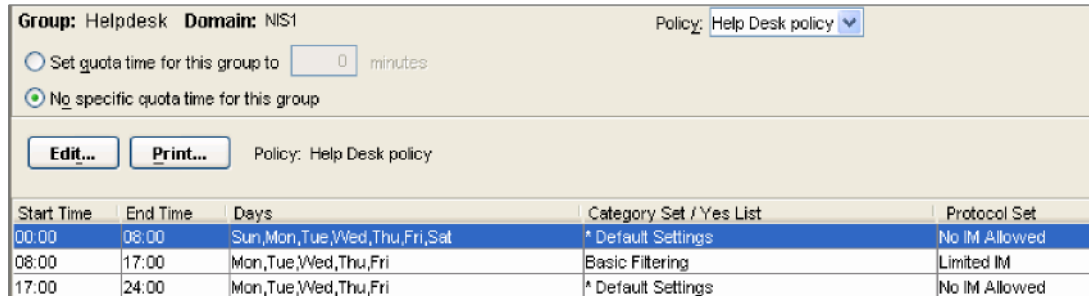


Figure 3 Access and time restrictions can be set for individual users or groups of users.

Internal and external communications

The Websense solution allows organizations to manage IM conversations and the sending of file attachments, whether such communications are with an external party or contained entirely within the internal network.

For example, policies can be set to allow the customer care team in an organization to use three specific, company-sanctioned IM clients to communicate with customers outside the organization during business hours only. While conversations are allowed, file attachments are blocked, reducing the threat of viruses infecting the organization from external sources.

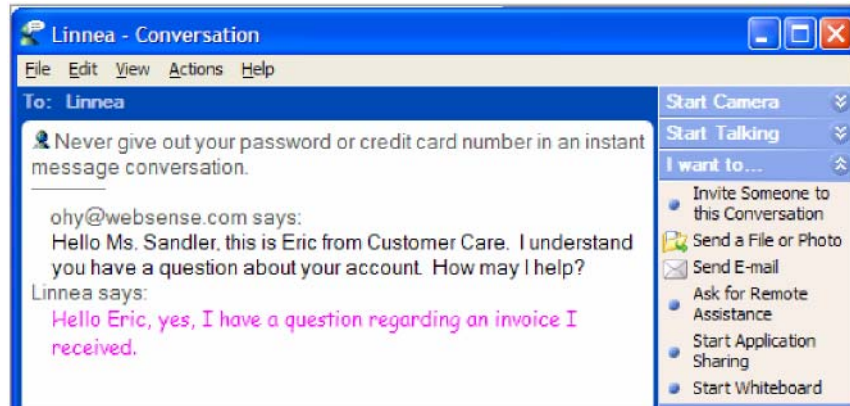


Figure 4 A Customer Care department uses IM to communicate with customers.

Monitoring and managing

While some organizations have an existing IM policy that requires enforcement, others are either unaware of IM usage by their employees or are uncertain of the degree to which it is being used. Using Websense Enterprise, 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 IM activity and IM file attachment usage. Forensics and analytics, along with “what if?” analyses, can be produced using Websense Explorer.

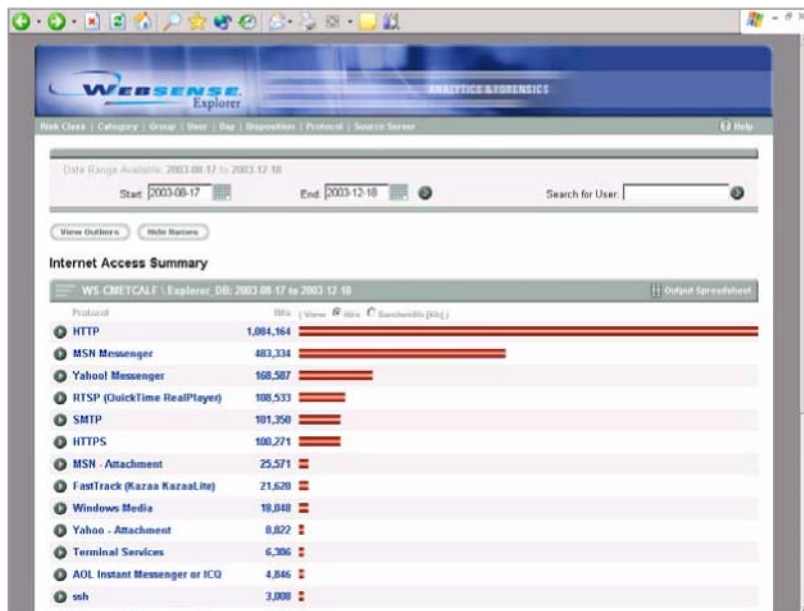


Figure 5 Websense Enterprise Explorer monitors IM usage in the organization.

Reports can be scheduled for routine email or intranet distribution to key recipients in IT, Management, and Human Resources. In this way, an organization can attain a sense of internal IM usage even before a company policy is established to govern the use of IM. In some cases, such foundational data can help an organization define its first IM usage policies.

The unique advantages of Websense

Websense provides a comprehensive solution for managing IM, offering superior benefits and value over all other currently available solutions.

Complete coverage of IM and other network protocols—Websense uses up to four different methods to identify network protocols: 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 managed.

Automated dynamic protocol management—Websense’s list of network protocols can be updated as frequently as every night. During the nightly update of the URL 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 IM 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.

IM management fully integrated with Websense Enterprise—The Websense solution provides organizations with a multi-layered, flexible, policy-based method for managing access to Web sites. Customers use the same Websense Enterprise Management console and policy model to manage IM, with no new interfaces to learn or management consoles to deploy. Since Websense’s IM management capability is directly integrated with its Web-filtering solution, an organization’s existing infrastructure can be leveraged, thus requiring almost no deployment effort.

Included with purchase of Websense Enterprise—The ability to manage IM protocols (as well as P2P, spyware, and many other protocols), by group or person, and by other integrated management

options available through Websense, is included with the purchase of a Websense Enterprise subscription.

Comprehensive solution for threats from employee computing—The Websense product components used to address IM issues—Websense Enterprise and certain add-on modules—also effectively address other emerging threats including P2P, spyware, and hacking tools, in addition to managing Web site access. Customers may use the same set of management and reporting tools to manage all the emerging threats that result from the convergence of employee computing and the Internet, thereby maximizing their investments.

Additional layer of IM policy management for mobile laptops—Many organizations want to manage IM use on their corporate computing assets, even when those assets, in the form of laptops, are disconnected from the network. Websense provides an important, additional level of security and policy management. If organizations are concerned with the security threats posed by the downloading of files using IM from remote locations, such as the employee’s home or hotel room, it is critical to manage the use of IM applications on laptops, even when those laptops are not connected to the organization’s network. Websense Enterprise Client Policy Manager provides this additional layer of security and policy enforcement for IM, as well as P2P file sharing, spyware applications, and much more.

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 IM 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 IM.

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

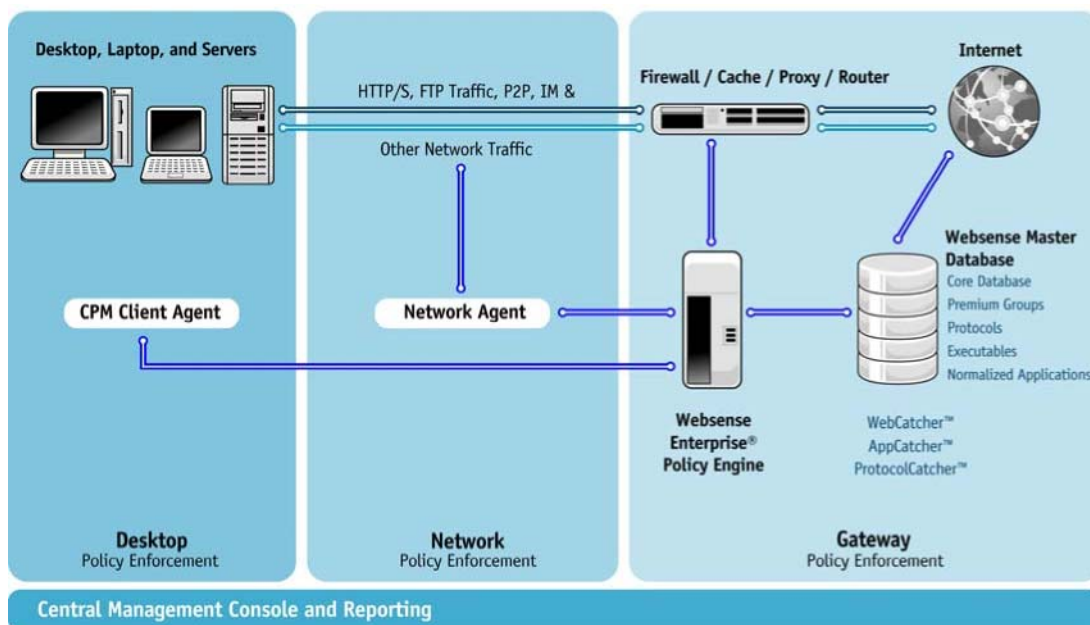


Figure 6 Websense Enterprise filters at multiple points on the gateway, network, and desktop.

Conclusion

Organizations facing a growing number of risks associated with employee use of instant messaging applications should consider implementing a solution that defends against these risks. As this paper has demonstrated, these risks pose real threats to security, in addition to traditional concerns regarding productivity, legal liability, and IT resource abuse.

Websense offers a best-of-class solution that allows organizations to enforce corporate policies at multiple points in their networks, resulting in layered, comprehensive protection from emerging threats. It also offers organizations integrated reinforcement of their security infrastructure. Websense Enterprise customers already have IM policy management included in their subscription benefits, and should extend their policies to include management of IM attachments, as well as other key protocols such as P2P file sharing and streaming media.

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.

Appendix: The Websense Enterprise Solution

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 7 summarizes WebSense Enterprise and its associated modules.

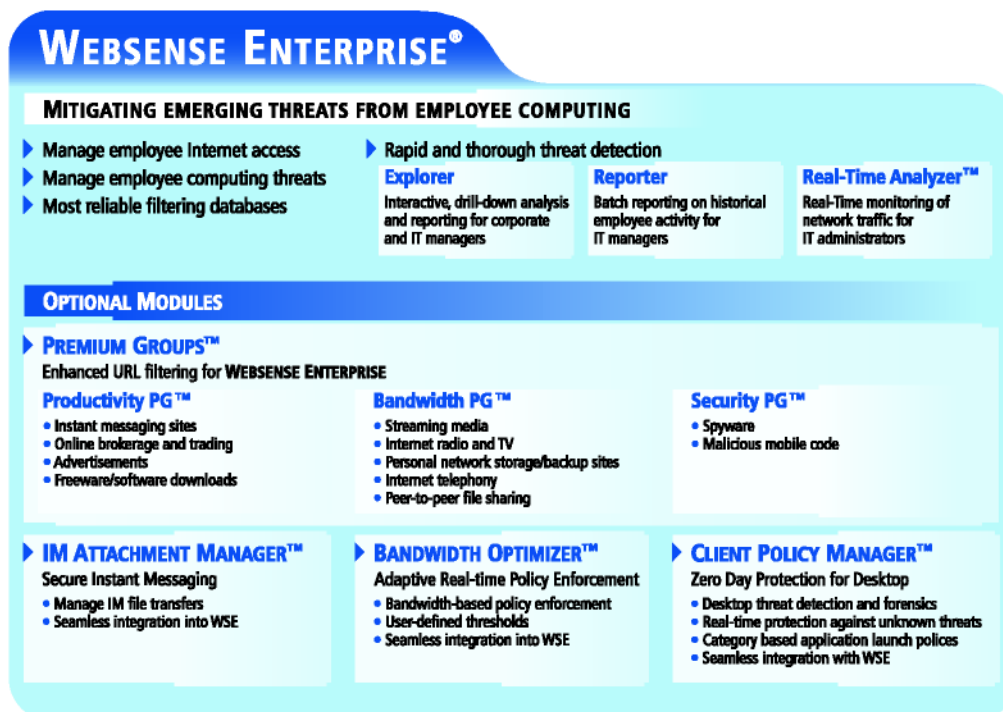


Figure 7 WebSense Enterprise and optional modules