



A Websense® White Paper

Desktop Security

Abstract:# Today's employee computing environment offers access to powerful applications and downloads, which can introduce new security challenges for corporate IT. With the nature of the employee workplace becoming increasingly more interconnected and mobile, the frequency and cost of the resulting security intrusions can be high. Perimeter security and antivirus solutions cannot adequately protect against these threats. Websense provides innovative end-point security solutions that identify and block known and unknown threats automatically, and prevent unknown applications, such as spyware, keyloggers, peer-to-peer transmissions, and hacking tools, from launching.

Table of Contents:#	Introduction.....	3#
	Risks to the Corporate Desktop.....	4#
	• # Peer-to-peer file sharing applications.....	4#
	• # Spyware, keyloggers, and Trojan horses.....	4#
	• # Hacking tools.....	4#
	• # Some applications need to be managed.....	5#
	• # Instant messaging applications.....	5#
	• # Other applications such as games and media players.....	5#
	• # Mobile storage devices need to be controlled.....	5#
	How Websense Addresses Desktop Security Concerns.....	6#
	• # Proactive protection.....	6#
	• # Reporting tools.....	6#
	• # Easy deployment and administration.....	7#
	• # Flexible and auto-updating user and group application use policies.....	7#
	• # The unique benefits of the Websense Desktop Security Solution.....	8#
	Case Studies.....	8#
	Conclusion.....	9#

Introduction

#

The corporate computing environment has changed dramatically over the last few years. With the internet now an essential business resource, employees have instant access to exciting new applications. Employees are comfortable managing their individual workplaces, accessing the internet, installing applications on their desktops, burning files onto CDs, and exchanging files of all kinds with clients and colleagues. This independence poses formidable new risks to the IT departments that must support employees' computing needs, while at the same time protect the business computing environment.

Adding additional complexity to this rapidly evolving work environment, employees can access information, network resources, and the internet from their homes, hotels, or remote offices. These remote users often circumvent IT investments in perimeter security, opening an access channel to the corporate network for external threats. This creates an enormous challenge for the IT departments that manage remote users' computer resources.

There will be 35 million remote users by 2005 and 14 billion devices on the Internet by 2010.¹

Employees often use peer-to-peer and instant messaging programs to send and share files. They may also use mobile memory devices to transfer files from one computer to another. In addition to making it easier for end users to send confidential information outside the company, all of these activities create a path for worms, viruses, and Trojan horses to enter directly into the heart of an organization's network.

#

90 percent of viruses in 2004 carried a "backdoor" mechanism compared with less than half in 2003.²

Unrestricted web access also exposes employees to sophisticated attacks from spyware and malicious mobile code, which often accompany applications downloaded from the internet. To make matters worse, many of these threats are designed explicitly to circumvent the traditional IT security infrastructure. They tunnel through firewalls and exploit delays in patch or antivirus signature deployments or security mis-configurations.

#

Most organizations rely on a combination of a firewall and antivirus solutions to protect their corporate desktops from viruses, worms, and Trojan horses, and from threats such as hacking and malware. However, the security weaknesses that expose system applications to threats often involve vulnerabilities that these solutions cannot address, or impose an administrative burden that renders these solutions impractical.

#

Since a significant amount of any organization's intellectual capital now resides on employee computers, protecting corporate desktops is a high-priority concern. Organizations need a multi-layered solution that complements their traditional security investments and goes one step further to anticipate and automatically address these threats to the desktop.

#####

1 Source: Forrester Research, 2003
2 Source: Alfred Huger, Symantec, 12/30/#

Risks to the Corporate Desktop

Some applications should never be allowed to run. Some applications have negligible business benefit and, based on a company's application use policies, should not be allowed to launch. Others are executable malware, which should be prevented from launching at all costs.

Peer-to-peer file sharing applications

Peer-to-peer (P2P) file sharing applications have found their way into many organizations, although no significant business uses for this technology currently exist. P2P file sharing is commonly used for downloading music or video files, often including commercially available and copy-protected content. P2P networks can be easily exploited to distribute viruses and worms because they bypass normal security and filtering barriers. Configuring firewalls to block ports used by P2P applications or to block the external addresses of P2P network servers does not solve the problem.

P2P applications can easily be configured to change ports automatically, and they are capable of penetrating firewalls using ports legitimately used by other applications. The danger of allowing employees to use P2P file sharing applications goes well beyond the exposure to viruses and worms; organizations also face significant legal risks when employees download, use, or distribute copyrighted, illegal, or inappropriate content.

#

Spyware, keyloggers, and Trojan horses

Spyware, keylogging software, and Trojan horse viruses can easily be acquired by downloading infected files or by visiting websites infected with malicious code. Spyware is used to gather information about computer users and their activities, and then relay that information to third parties over the internet. It is typically acquired during P2P application or file downloads. A keylogger is a software application that captures a user's keystrokes. Cyber crooks often use keyloggers to obtain passwords or encryption keys that allow them to bypass security measures. Keyloggers can be distributed as a Trojan horse or as part of a virus or worm. A Trojan horse is a malicious program that is disguised as legitimate software. Trojan horses can be designed to do various harmful things, such as erasing or overwriting files, corrupting files, spreading other malware such as viruses, or installing a backdoor on a computer system.

#

Hacking tools

#

Organizations have always been concerned about the ability of outsiders to hack into their computing environments and gain access to proprietary information. Surprisingly, the threat of hacking is primarily a threat from an insider. Employee hacking is a bigger problem than ever before because dangerous "how to" information is so readily accessible over the internet. Hacking portals target novice users and offer tools, such as scripts, programs, and message boards that would-be hackers can use to learn about and discuss their hacking exploits.

#

The "Stress of Security" survey questioned 500 IT managers across Europe. According to this survey, 60 percent of respondents have no measures in place to detect internal hackers.³

#####

3 Independent research conducted by Dynamic Markets and commissioned by Websense

#

Some applications need to be managed

Some applications may be appropriate for some departments in a company, but not others. For example, an organization may want its IT group to be able to run remote access applications, but because of the security issues involved, giving the marketing group the same permissions would not be advisable. There may even be applications, such as media players, which IT may want to allow to run without accessing the network. These very real application-use scenarios go well beyond the capabilities of any firewall or antivirus software. Providing the context in which an application or category of applications may be executed by an individual or a group provides a powerful and unique benefit to IT organizations, CXOs, and business managers alike.

#

Instant messaging applications

Instant Messaging (IM) applications have quickly become an essential communications and business productivity tool for many organizations worldwide. For example, IM may provide a way for the sales group to maintain real-time contact with customers and management. However, IM can also have a significant downside within organizations. It can act as an avenue that threat vectors can exploit because it often bypasses virus-scanning software, or it may become a conduit through which confidential company information may be distributed or unknowingly exposed through the sharing of attachments. Viruses and worms can also hitch a ride on files transferred using these applications and make their way into corporate networks. Last but not least, IM applications can act as a serious employee productivity drain.

Organizations need a tool that provides a significant degree of flexibility in authorizing the use of such applications while maintaining security.

Other applications such as games and media players

Employees bring computer popular games with them to work (on disk, CD, DVD, Flash drives, or even downloaded from the internet) and generously share them with their coworkers. The prevalence of free media players, like Windows® Media Player and RealPlayer, also makes it easy for employees to download and play music or videos on their desktops.

Aside from the most obvious impact—drain on worker productivity—game playing, music listening, and video viewing on the job has other costs as well. These activities consume hard disk space, processor time, and network bandwidth capacity; they introduce potentially incompatible applications into the organization; and they may even open doors through which outsiders can introduce viruses, Trojan horses, or worms.

#

Mobile storage devices need to be controlled.

Mobile storage devices offer a convenient way for employees to transfer files and applications from one computer to another. These devices also make it much too easy for employees to steal intellectual property. Devices such as flash drives, CD/DVD drives, memory sticks, floppy drives, and external hard drives typically have more than a gigabyte of storage capacity—more than enough space for documents, databases, graphics, and even proprietary or copyrighted applications.

#

An organization's security may be compromised when employees connect USB drives to infected home computers, or upload files containing malicious code onto a mobile device then introduce them back into the organization, enabling the malware to propagate in the organization's network. To assure information security, organizations must be able to set policies on the use of removable media and have the ability to disable them completely.

#

How Websense Addresses Desktop Security Concerns

Proactive protection

Websense offers a desktop security solution that protects the internet gateway, network, and the desktop.

Websense Client Policy Manager™ (CPM) delivers desktop security protection against known and unknown security threats and prevents the execution of unauthorized applications. CPM enforces application use policies for corporate desktops, laptops, and servers with its unique and comprehensive database of categorized applications, which is updated daily. CPM provides a proactive, critical component that stops today's fast-moving and blended security threats.

#

Websense provides flexible enforcement of your company's application use policies. It prevents the execution of unauthorized applications such as spyware, P2P file sharing, and hacking tools, while enabling flexible policy management of applications such as IM or remote access tools, which only designated users or groups should be allowed to use. Through Websense directory integration, these policies can be implemented at a group level or tailored to individual needs, ensuring that all desktops are protected and adhere to company standards.

#

Working alongside firewalls and antivirus tools, Websense advanced lockdown features close the window of exposure to unknown security threats—threats that could bring down networks before virus signatures or patches can be deployed or where security systems are mis-configured.

Websense mitigates web-based threats. With the most comprehensive and effective database of web-based applications, Websense detects and blocks more web-based threats than any other solution.

Websense blocks access to the corporate network. Websense blocks application network access to specific ports and protocols by application category.

#

Websense prevents unauthorized applications from launching. Websense provides maximum control over desktop environments by allowing only approved applications to run on corporate desktops and servers, thereby preventing potentially malicious applications from launching.

#

Websense prevents new applications from launching. Websense allows system administrators to block new applications—applications that are acquired after a particular point in time—from launching. This protects individual desktops or the entire network from attacks by keyloggers, Trojan horses, worms, and other malicious code threats. Websense gives system administrators control over removable devices. With Websense, administrators can control whether and how all or specific devices (such as CD/DVD burners, floppy drives, flash drives, and external hard drives) can be used. This feature can be tailored to reflect your company's policies. For example, a policy may allow these devices to be used to upload work product, but not applications, or copy files from the desktop, but not applications, and so on.

Reporting tools

Websense reporting tools help determine your company's risk profile. These tools determine the presence and location of malicious mobile code, spyware, hacking tools, and other security risks in your network. Using these tools, your IT administrator can perform critical desktop inventories that provide categorized views of applications and executables, enabling early threat detection and identification of dangerous applications. Websense takes application inventories

#

one step further by normalizing executables into application names that IT professionals can actually understand. For example, even though Microsoft® Outlook™ is composed of multiple application components, Websense inventory assessments will identify and report one application called “Microsoft Outlook.”

#

Using these reporting tools, business and IT managers can identify application use and network access attempts by employee, department, date, disposition, and most importantly, by application category. Reports also identify desktop security threats such as spyware and hacking tools, and detect the use of unauthorized applications such as IM, P2P, and games. Websense helps managers answer important questions such as:

#

- # How much spyware is on my network? Which systems are infected?
- # Is P2P file sharing application use a problem in my organization?
- # Who is using or has attempted to launch hacking tools internally?
- # Do I have the right employee application use policies in place for my organization?

Easy deployment and administration

Websense makes it easy to begin managing your corporate desktops. You have the option of deploying desktop agents onto desktops individually or globally with just a click of a button in Websense Manager.

#

Once Websense CPM is deployed, enforcing up-to-date security policies requires minimal administration. Best of all, Websense provides this security for all computing resources, whether they are connected to the network or not.

Flexible and auto-updating user and group application use policies

Hundreds of thousands of executables from thousands of applications, as well as scripts, temporary internet files, and applets, have been classified into 50 categories to support establishing and applying unique and powerful desktop management and control policies. Categories of applications include P2P, IM, spyware, hacking, malicious software, and games. Websense is unique in providing a complete list of categorized applications and is updated with uncategorized applications regularly by mining software and download sites for new applications. In addition, Websense AppCatcher™ automatically and anonymously forwards all uncategorized applications from interested customer sites, along with their network and protocol access behavior, so they can be categorized. Essentially, AppCatcher helps “tune” the database to each customer’s unique desktop application environment. Other Websense customers benefit from these technologies, as their databases are enriched as well.

Policies can be customized to enforce particular corporate policies, and application use permissions can be specified based on application category, user, group, workstation, or IP address. For example, an administrator can create an IM application policy that restricts use to a single approved IM client, such as AOL® Instant Messenger™, while blocking all others. The policy can be refined further 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.

#

Only Websense enables organizations to enforce policies such as:

- # Do not allow hacking tools to run on any (disconnected or connected) corporate desktop or laptop.
- # Allow only the Professional Services organization to use MSN Messenger.
- # Allow employees to play games, but warn them that gaming is not an appropriate activity.

#

These policies can be customized based on existing user and group definitions in a company's network. CPM interoperates with the existing infrastructure and can integrate with popular user directory services, such as Microsoft Windows Active Directory and Windows NT 4.0. In addition, these policies can be enforced on laptops that are disconnected from the organization's network.

The unique benefits of the Websense Desktop Security Solution

Websense provides comprehensive threat detection and policy enforcement that enables organizations to enjoy the following important business benefits:

#

- **# Stronger desktop / laptop security**—Websense helps stop unknown viruses or worms from spreading in the organization, leading to higher application and network uptime. It also protects sensitive corporate data by limiting access to unregulated communication via IM, P2P, and spyware. In addition, it allows IT administrators to control how and whether removable media devices, such as flash drives, can be used, reducing the risk of information theft and misuse of copyrighted products, such as software.
- **# Higher employee productivity**—Websense enables IT and business managers to set appropriate application use policies for desktops. By blocking access to inappropriate or unauthorized applications, such as games and instant messaging, employee productivity, is maximized.
- **# Lower desktop management costs**—Websense reduces help desk and desktop administration costs by eliminating software incompatibilities and subsequent help desk calls by providing better visibility into the desktop environment through application use and inventory reports.

Case Studies

Case studies from companies for whom desktop security is a primary concern.



Sharp HealthCare, San Diego's most comprehensive health care provider and a recognized leader in the use of internet-based technologies, uses Websense to protect the computing environment and confidentiality of its patients' health information from emerging threats such as spyware, keystroke logging programs, employee internal hacking, and internet-borne virus outbreaks. Sharp HealthCare's implementation of Websense helps enable the company to comply with HIPAA's privacy and security rules.

"Sharp HealthCare has been honored for the fifth year in a row as one of the nation's most wired health care systems. As we continue to increase our use of internet technology to improve efficiency and patient care, it becomes both more important and more difficult to protect the privacy of our health information," said Patric Thomas, vice president, enterprise architecture and support, Sharp HealthCare. "Caring for our patients is at the heart of every technology initiative we implement, and we see Websense as an essential solution to defending the security of our patients' and employees' confidential information."

Websense also enables the highest degree of end-point security with its lockdown mode. This feature enables IT administrators to easily create an approved "white list" of software applications for each desktop and prevent the launch of any application not included on the list. In the health care environment, Websense also prevents unauthorized employees from launching patient data applications or hacking tools to gain access to restricted information.

#

NORTHCLIFFE NEWSPAPERS GROUP LTD

Northcliffe Newspapers is one of the largest regional newspaper publishers in the UK. Northcliffe knew that they had to solve the issue of malicious applications and hacking tools being inadvertently launched by users at a desktop level. Websense Client Policy Manager (CPM) increases desktop security by blocking unauthorized applications, such as spyware and hacking tools, and boosts employee productivity by preventing the unauthorized installation of inappropriate and non-business related applications. Northcliffe swiftly purchased 300 licenses for his region on the condition that his region proved the test-case for a group-wide roll-out.

Even though the company had just completed a roll-out of Microsoft Windows XP operating system and, therefore, had some security features already installed, CPM extended the capabilities of Websense Enterprise to provide a more secure environment at Northcliffe. "The trouble is an employee might not even know that they have installed a program, so they might not know that they have downloaded a piece of spyware onto their system. But this could be giving out their keystrokes and confidential information to an external party," explains Antony Wiltshire IT Manager, South-East region, "Websense CPM helps us deal with the worry of employees inadvertently disclosing information."

Conclusion

Client Policy Manager™ (CPM) delivers desktop security protection against known and unknown security threats and prevents the execution of unauthorized applications. Websense enforces employee application use policies for corporate desktops, laptops, and servers with its unique and comprehensive database of categorized applications, which is updated daily. Websense provides a proactive critical component that closes the window of exposure to today's fast-moving and blended security threats.

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

About Websense, Inc.

Websense, Inc. (NASDAQ: WBSN), protects more than 25 million employees from external and internal computer security threats. Using a combination of preemptive ThreatSeeker™ malicious content identification and categorization technology and information leak prevention technology, Websense helps make computing safe and productive. Distributed through its global network of channel partners, Websense software helps organizations block malicious code, prevent the loss of confidential information and manage Internet and wireless access. For more information, visit www.websense.com.

#

© 2007 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. [29 January 2007]

#