CERBERIAN®

INTELLIGENT WEB FILTERING

The Increasing Risks of Internet Computing

Securing the Internet Within Your Organization

Despite great benefits of the Internet, organizations of every kind assume substantial risks and costs when they provide Internet access, particularly when those connections are used to access sites containing information or images that are inappropriate, illegal or dangerous. Unrestricted Web access can result in excessive non-productive Web surfing, creating tremendous losses in productivity and potential exposure to security breaches and legal liability.

Traditional Web filtering solutions are insufficient when dealing with a dynamic Internet, relying on static databases of URLs requiring the deployment of costly filtering hardware which in turn necessitate ongoing IT management to support and maintain.

This paper examines these increasing risks in detail and explains how Cerberian Web Manager provides a new approach using patent-pending intelligent technology to deliver the highest level of protection and productivity, limiting organizational liability and risk to Internet security, while lowering the total cost of ownership and burden on IT staff.

Cerberian, Inc.
World Headquarters
13997 So. Minuteman Dr.
Suite 140
Draper Utah, 84020
USA
Tel. 801.999.2900
Fax. 801.999.2999
info@cerberian.com
www.cerberian.com

Contents

Executive Summary

The Web is a dangerous place. No other medium in history places at the fingertips of its audience the breadth of information or potential for harm like the Internet. The Web's grasp extends practically everywhere one goes, from the home, to the office, to the airport, to the library; and today's users, though educated and sophisticated, are torn between the Internet as an unprecedented resource or a time-consuming and often inappropriate waste.

In an effort to manage Web access, consumers and employers have implemented Web filtering software to screen and exclude access to Web pages that are objectionable or not business related. Businesses have begun to adopt corporate access policies in an effort to outline the appropriate use of the Internet within the organization in order to protect themselves from legal liabilities, ensure network security, sustain network resources and boost employee productivity. Unfortunately, corporate ignorance on the exact scope and scale of the Internet problem and the lack of policy enforcement have delayed the mass adoption of such filtering solutions and corporate access policies. Adding to this problem is the fact that traditional Web filtering companies have created a false sense of security for their users by delivering ineffective and burdensome systems that require additional hardware and maintenance. The time has come where Internet management is no longer an important luxury; rather it is now an urgent necessity. Fortunately, the rules have changed and technology has caught up with the content filtering industry.

Background

Since the introduction of the Internet into the corporate environment, organizations have faced many challenges created by allowing employees access to the Internet. Developed as a communications and research tool, the Internet has quickly become an entertainment medium and a security risk. As a result, employers have been forced to take a more proactive approach in an effort to regain control of dwindling employee productivity, reduce legal liability, minimize drain on information technology (IT) resources, and bolster network security. All this, while trying to maintain a balance between personal privacy and "big brother" corporate governance.

Unfortunately, the inherent risks of Internet access are evolving quickly as the Internet continues to advance. Service providers and Web developers regularly add new, bandwidth-draining ways of distracting employees and hackers continue to develop more damaging schemes to penetrate corporate networks. Internet access policies and internal security measures are now being bypassed with the growth of new Web applications, such as streaming media, peer-to-peer networks and instant messaging clients. Add the fact that corporations are providing employees with new ways to access the Web through a variety of mobile hardware, including laptops, personal digital assistants and digital cell phones, and the challenges facing corporations continue to mount.

> *"Corporate concerns with employee productivity, legal liability, and network resources continue to fuel the growth of the Web filtering market. IDC believes 30% to 40% of Internet use in the workplace is not related to business."*
>
> *IDC, Secure Content Management Forecast Report, March 2004*

The Internet is obviously here to stay. Now, the goal within today's organizations is to manage the Web across all fronts and position it as a productive and powerful resource for employees without it becoming a legal and productivity burden or a management problem. Without an Internet management strategy, including an enforceable Internet access policy, combined with an efficient and reliable filtering solution, organizations will continue to face the inherent and increasing risks of Internet computing. These risks include:

- Security breaches
- Legal liability
- Lost productivity
- Bandwidth consumption

The Increasing Risks

Just as organizations protect access through the back door of their offices, organizations need to recognize that the Internet often creates unmonitored, back-door access to vital corporate information. With the increasing popularity of the Internet as an entertainment and communications medium, employees are continually leaving the virtual back doors open with non-work-related browsing, downloading and installing of peer-to-peer and instant messaging applications, and changing the secure, standard configurations of corporate-assigned hardware.

As a result, organizations face even greater risks than they may be aware of, both in what the Internet provides and what employees do to bypass corporate policies and side-step embedded security measures.

Security Breaches

Unregulated Internet access opens the door for damaging downloads, which can impact everyone on the network. Malicious mobile code, Trojan horses, spyware and adware have caused billions of dollars in damage, placed billions more worth of intellectual property at risk and forced internal IT departments, Internet Service Providers and security firms to spend days cleaning up after attacks. According to the Computer Crime and Security Survey conducted by the Federal Bureau of Investigation and Computer Security Institute, 99 percent of the companies surveyed in 2003 used antivirus software, 98 percent used firewalls, and 92 percent used some measure of access control. Despite the investment in security measures, 82 percent of those same companies were hit by viruses and worms.[1] A majority of these hits came as a result of employee misuse of email and Internet privileges.

> *"MyDoom remains at the number one position of most damaging malware of all time, having caused between $73.3bn and $89.6bn of damage worldwide."*
>
> *mi2g, Security Report, March 2004*

> *"27 percent of Fortune 500 companies have battled sexual harassment claims stemming from employee misuse and abuse of corporate e-mail and Internet systems, according to the ePolicy Institute."*
>
> *Newsday.com, "Junk e-mail slows work, invites suits," April 4, 2004*

Personal surfing habits can create an unsafe environment for others by exposing unassuming individuals to everything from violence and hate to information on terrorism and drugs. Additionally, access to pornographic sites, downloading of freeware, and the sharing of pirated music, films, or software not only exposes the organization to potential liability, it also exposes the network to potential spyware, including keystroke loggers, dialers, and other worms and viruses. The potential damage to personal information, corporate intellectual property and overall network security is limitless.

Legal Liability

When corporate hardware, software, Internet access and facilities are involved in the exchange and storage of offensive material or copyrighted music and movies, the organization opens itself up to serious legal concerns.

Organizations have the responsibility to provide an amicable working environment for all employees, while honoring personal privacy and individuality. Most managers rely on their employees' integrity and professional responsibility to maintain a decent and stable environment. Unfortunately, organizations face significant security and legal challenges when company networks are used to download, store and illegally distribute protected material or when peer-to-peer file-sharing applications to download pirated software or copy-written entertainment are permitted using company hardware and services. Additionally, organizations face new security measures and standards with recent HIPPA and GLLA legislation that require stricter security and privacy procedures.

Lost Productivity

Possibly the most obvious challenge facing organizations when it comes to Internet access is the loss in employee productivity. The hidden costs of Internet abuse for companies of all sizes can be significant. One European study found that on average, a small company "that makes £700,000 ($1.28m) profit on a turnover of £10-12m could be

[1] Computer Security Institute, "CSI/FBI 2003 Computer Crime and Security Survey", 2003 Report

losing 15 percent of its profits because of abuse of net and e-mail"[2]. According to recent statistics, more than 37 percent of workers with Net access have visited adult Websites while on the job[3], and 70 percent of all porn traffic occurs during the 9-5 workday[4].

> *Non-work-related Internet use in the workplace includes: booking holidays (52%), pursuing education (42%), researching hobbies (41%), shopping (28%) or watching sports events (27%).*
>
> *Taylor Nelson Sofres, Internet Use Survey, March 2004*

Unlike any other medium, the Internet combines elements of television, radio and print to provide an always-on information and entertainment network. Most work environments provide broadband Internet connections, giving employees free reign to all that the Internet has to offer. Whether employers are aware or not, employees may be spending too much time shopping, reserving vacation plans, trading stocks, chatting on IM or participating in fantasy sports or online games. The Internet offers an enormous amount of distractions for employees, and more content is being added daily.

Bandwidth Consumption

High-speed Internet access is a precious commodity, which explains the growth in residential broadband access, as well as why many people use their high-speed corporate networks to download music, high-quality graphics, games and software applications. IT departments usually do not have to look very far for reasons behind poor network performance. One Nielsen//NetRatings study found that more than 56 percent of employees run streaming media applications during the workday[5], and another report suggested that in July 2003, 77 percent of companies had found at least one P2P file-sharing application on their networks[6].

If employees are using the network pipe for surfing, peer-to-peer exchanges and streaming media, instead of processing e-commerce transactions, running sales webinars or supporting customers, then they may be impacting business-critical functions and applications. The concern then grows beyond employee productivity, and security and legal liability issues to activities that affect day-to-day business operations and bottom-line revenues.

The Increasing Risks of Internet Computing

Risk	Cause
Security Breaches	Harmful malicious content contracted from surfing inappropriate Web sites
	Potential virus or worm invasion into corporate network through instant messaging and peer-to-peer applications
Legal Liability	Illegal download of copy written movies, music, and pirated software
	Exposure to offensive themes and pornographic images
	Hate, crime, violence and other offensive sites exposed to employees
Lost Productivity	Personal pursuits of online shopping and auction sites during business hours
	Personal management of finances and financial portfolios
	Excessive online gaming during work time
Bandwidth Consumption	Use of streaming media and real-time applications
	Oversized downloads of copy written movies and music files

Complexities of Today's Risks

Despite organizations' valiant attempts to face these increasing risks head on with new security measures, technology continues to improve equally as fast for the opposition. As soon as security service providers and hardware manufacturers release updates, revisions and patches; new sites, new peer-to-peer applications and new online games place many Web filtering solution providers, and their customers, one step behind. Traditional Web filters are finding it difficult to keep up with the phenomenal growth of the Web because they monitor the growth with inefficient human review and key word search systems. Additionally, these solutions are bulky and costly, requiring filtering and reporting servers along with ongoing IT management and support.

[2] BBC News, "Internet Abuse Costs Big Money", November 1, 2002
[3] AVN, "Somebody is Looking at all that Porn", April 5, 2004
[4] BusinessWeek, "Workers, Surf at Your Own Risk", June 12, 2000
[5] NetRatings, Inc., "Nearly 56 Percent of U.S. Office Workers Access Streaming Media", October 11, 2001
[6] CNET News.com, "Businesses boosting anti-P2P software", August 27, 2003

Security continues to be top priority among corporate America as malware and virus developers stay a step ahead of organizations' anti-virus and anti-spam counterparts. One industry expert estimated that 1,000 viruses are created every month[7]. While security is reason enough for organizations to invest in Web filtering; the inherent risks and consequences of the Internet can be the extra incentive needed to address the complexities of Internet risks with an enforceable Internet access policy and a dynamic Internet management and filtering solution.

Today's Internet risks require a next generation Internet management solution – one that fights the many faces of these risks with a multi-layer, real-time approach that can keep pace with the growth of the Web while minimizing burden and overhead to the organization.

The Cerberian Breakthrough Solution

Cerberian has revolutionized web filtering by providing an intelligent solution to help organizations gain full control of the way employees use the Internet. Built upon a managed service architecture, a comprehensive and growing database of more than 1 billion Web pages, and a patent-pending dynamic real-time site rating technology, Cerberian Web Manager delivers the most accurate, most cost effective, and most advanced filtering solution available.

Cerberian Web Manager includes the following core components:

- **Cerberian Service Platform**
  As a managed service, Cerberian eliminates the cost and burden that traditional locally hosted, server-based filtering solutions place on an organization's IT department, offering businesses a worry-free system. Cerberian's global technology datacenters deliver a fully load-balanced and redundant solution, assuring a 99.999 percent system uptime, meeting the growth and demands of business. Updates to Cerberian's ratings database are made instantly, impacting all users and without service interruption or hassle to IT staff. Changes to an organization's access policy can be made securely through Cerberian's Web interface.

- **Cerberian Dynamic Real Time Rating (DRTR)**
  Unlike other filtering solutions, Cerberian's patent-pending Dynamic Real-Time Rating™ (DRTR) technology analyzes all requested Web pages in real-time, blocking new unrated content on-the-fly, while feeding the Cerberian ratings database with constant updates to ensure that Cerberian Web Manager has the most relevant ratings database available. Processing time is so quick it is transparent to users.

  Cerberian DRTR captures more than 99 percent of all new and unrated porn sites, with more than 1 million new porn pages coming online every week[8], and refutes competitive claims of not being able to distinguish, for example, between a Web site advocating the abuse of drugs and one offering a sociological study of drug abuse. Cerberian Web Manager does indeed make this distinction and can distinguish between numerous cross-over categories, such as gambling sites, sites of gambling commissions, and sites dealing with the treatment of gambling addiction. In fact, Cerberian's advanced technology has been proven to be more accurate than human review due to human inconsistencies and personal opinions.

- **Cerberian Master Ratings Database**
  Cerberian Web Manager provides users with the most relevant and effective ratings database available, built by the Internet activity and surfing habits of its users. Cerberian's massive database contains more than 5 million ratings and domains resulting in effective coverage of more than 1 billion Web pages, which are sorted into 52 unique content categories and cover 44 different languages. As a result of Cerberian's managed service model, the ratings database is continuously updated, requiring no daily or weekly downloads/updates by the organization. In the event that a user's request is not found in the database, Cerberian's unique second line of defense, Dynamic Real-Time Rating, is activated.

- **Cerberian Policy Manager and Reporter**
  Cerberian allows organizations the ability to customize Internet access policies from a list of 52 unique content categories, while enforcing the desired level of access for groups and individuals, approving and

[7] ZDNet, "Staying Ahead of the Hackers", April 12, 2003
[8] The National Research Council, September 2003

denying access by category, individual or time of day. Cerberian includes coverage for all categories and does not break down or charge extra for additional coverage, as seen with competing solutions. Organizations are covered completely with one comprehensive subscription. Organizations can also monitor and enforce their Internet use policies with up-to-the-minute reports presented in both graphic and tabular formats.

Cerberian 52 Content Categories

Potential Liable and Objectionable	**Potential Non-Productive**		
Adult/Mature Content	Abortion	Gay/Lesbian	Restaurants/Dining/Food
Alcohol/Tobacco	Arts/Entertainment	Government/Legal	Search Engines/Portals
Gambling	Auctions	Health	Shopping
Hacking/Proxy Avoidance	Brokerage/Trading	Humor/Jokes	Society/Lifestyle
Illegal/Questionable	Business/Economy	Job Search/Careers	Software Downloads
Illegal Drugs	Chat/Instant Messaging	Military	Sports/Recreation/Hobbies
Intimate Apparel/Swimsuit	Computers/Internet	News/Media	P2P/MP3/Streaming Media
Nudity	Cult/Occult	Newsgroups	Travel
Pornography	Cultural Institutions	Pay to Surf	Vehicles
Sex Education	Education	Personals/Dating	Web Advertisements
Violence/Hate/Racism	Email	Political/Activist Groups	Web Communications
Weapons	Financial Services	Real Estate	Web Hosting
	For Kids	Reference	
	Games	Religion	

Cerberian Unique Advantages:

- **Real-time site rating technology ensures the most accurate filtering solution available**
  Unlike other filtering solutions, Cerberian realizes that a URL database alone is not enough to catch new and uncategorized Web content, which is constantly being added to the Web. As a result, Cerberian Web Manager analyzes all requested Web pages in real-time to ensure the highest level of protection while building the most relevant ratings database available.

- **Managed service platform eliminates set up cost and ongoing management hassle**
  As a managed service, Cerberian eliminates the added cost and burden that traditional locally hosted, server-based filtering solutions place on an organization's IT staff.

- **Platform diversity allows freedom of deployment**
  Cerberian Web Manager is available as an integrated, value-added service on a variety of leading network appliances, service solutions, and security software applications, allowing organizations to choose how they prefer to deploy and manage Internet security. See a list of premier partners below.

- **Easy to setup and manage**
  As a hosted service, Cerberian Web Manager is the easiest corporate filtering solution to get up and running. Its Web-based interface is simple and painless, enabling the access of policies and reports from virtually any Internet-enabled PC.

Benefits of Using Cerberian Web Manager:

- **Manage employee Internet access**
- **Mitigate employee computing risks**
- **Keep porn and inappropriate web content out**
- **Control risk of security breaches**
- **Enhance employee productivity**
- **Conserve capital and IT resources**

Cerberian Web Manager Service Architecture:
When a user of a Cerberian Web Manager enabled device (firewall, proxy, service provider, software application, handheld) sends a request for a URL (1) the agent device intercepts the request from the local network and sends a request to the designated Cerberian Service Point (2). The service point provides a category rating for the requested URL and at the same time a request is sent to the target Web server requesting the page for download (3). The requested site is then either allowed or blocked based on the users Internet access policy.

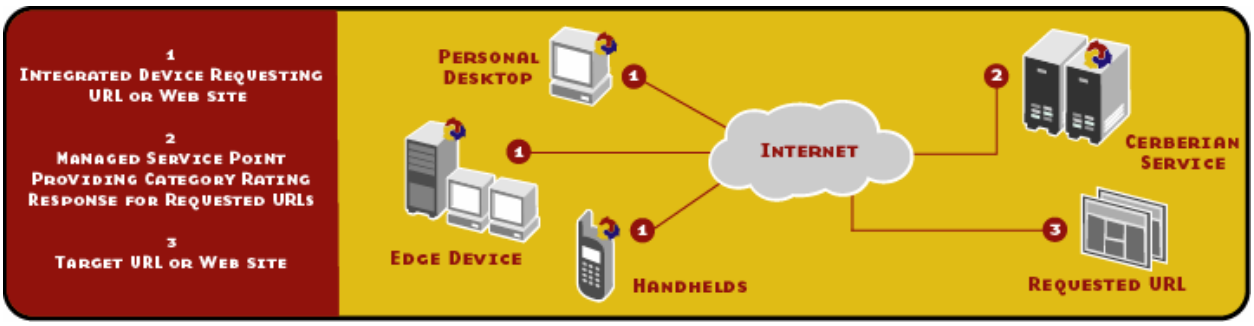

Figure 1. Cerberian Web Manager Service Architecture

Cerberian Product Solutions:
Cerberian Web Manager is available as an integrated component on the following devices, service solutions, and security software applications and can be purchased by contacting Cerberian or the appropriate partner vendor.

- **Firewall Appliances** – Barbedwire, Buffalo, Check Point, CyberGuard/SnapGear, Fortinet, LogiSense, MARA Systems, Microsoft ISA Server, MIS Technologies, SonicWALL, Squid, ZyXEL
- **PC Security Software Applications** – Zone Labs, LogiSense, Linspire
- **Cache / Proxy Products** – iMimic, LogiSense, Mara Systems, Microsoft ISA Server
- **Router / Switch Products** – Belkin, Buffalo, ZyXEL
- **Managed Service Providers** – MIS Technologies
- **Internet Service Providers** – IIJ, Mstar

Securing the Internet within your Organization
An inside look at how Cerberian Web Manager helps organizations secure Internet access and reduce the risks of Internet computing.

Security Breaches
Cerberian Web Manager provides the technology for companies to protect their networks by managing employee Internet access, and blocking access to potentially unscrupulous Web sites and offensive material that can open the door for security intrusions. Cerberian Web Manager allows administrators to limit what sites employees can access based on the organizations access policy. By blocking access to pornography, peer-to-peer, and gaming sites along with other potential carriers of similar content, organizations prevent employees from unknowingly downloading harmful adware, spyware and potentially malicious code.

Legal Liability
Cerberian Web Manager empowers administrators to limit or completely block access to Web sites that contain P2P applications, MP3s and software downloads, pornography and other inappropriate Web sites, and therefore protects the organization from potentially liable and objectionable content. While some people may feel that filtering impedes their individual freedoms, Cerberian protects the organization and its employees. Companies have the flexibility to monitor Internet access as tightly or as loosely as they choose while giving employees the freedom to surf the Web without worrying about seeing inappropriate and offensive material.

Lost Productivity
As the Web continues to create easier access to shopping, games, peer-to-peer activities, pornography and other non-work-related content, organizations may find that they are paying their employees to be unproductive. Cerberian Web Manager encourages employees to use the Web for work-related activities while ensuring employers their employees are not spending corporate time making vacation plans, padding their stock portfolios or placing online auction bids. Cerberian Web Manager's centrally managed system allows administrators to create a

customized access policy that is appropriate for their organization, ensuring the right level of control and balancing employee personal privacy and corporate governance. Whether organizations want to only monitor employee Internet activities, filter by category or time of day, or monitor, filter and provide some time for recreational surfing, Cerberian Web Manager offers them the flexibility to do so.

Bandwidth Consumption

It's obvious why many patrons of streaming media sites, peer-to-peer file sharing applications, and online movies wait until they get to work to participate in these activities. Recent studies show that only 42 percent of homes in the United States subscribe to broadband Internet services while more than 77 percent of at-work Internet users have broadband access[9]. Cerberian Web Manager allows organizations to proactively limit access to Web sites that transmit streaming media, encourage P2P file sharing or require significant bandwidth to download images, games, or other software. While Cerberian Web Manager helps maintain network bandwidth for core business applications, it also helps to eliminate large personal caches of downloaded files on network servers.

Conclusion

The Web is a dangerous place, constantly raising the inherent risks of Internet computing. As organizations continue to give employees new ways of accessing the Web, employees are regularly leaving backdoors open to attacks and the potential theft of proprietary and confidential information; the heart of many organizations. Unfortunately, traditional filtering companies are adding cost and burden to the organization, and bringing to market solutions that do not adequately cover the dynamic and ever-changing Internet.

Technology has finally caught up with the web filtering industry. While many filtering solutions continue to use archaic methods of maintaining their databases and filtering Internet content, technology has made it possible to help stifle security breaches, reduce legal liability, increase employee productivity, and better manage and conserve network bandwidth.

When compared to other Internet management solutions, Cerberian Web Manager leads the industry in innovation and technology, incorporating quality content, intelligent rating, multiple deployment options, global coverage, and comprehensive reporting and analysis. With Cerberian's breakthrough solution, organizations can add superior protection and efficiencies of Web management to their businesses with minimal infrastructure and management costs.

About Cerberian

Cerberian has revolutionized Internet management by delivering the most intelligent, hassle-free Web filtering solution available. This unique technology allows organizations to effectively manage and filter objectionable and unproductive Web content while reducing risk of security breaches, limiting legal liability, conserving IT resources, and boosting employee productivity. Offered as a managed service, Cerberian minimizes initial investment and ongoing management burden by maintaining the technology and data management responsibility at Cerberian's global data centers. Cerberian realizes that a URL database alone is not enough to stop new and uncategorized Web content. Consequently, unlike other filtering solutions, Cerberian's Dynamic Real-Time Rating (DRTR) technology analyzes all requested Web pages in real-time to ensure the highest level of protection while constantly feeding new ratings to Cerberian's massive ratings database. Cerberian Web Manager is available as an integrated, value-added service on leading network appliances, service solutions, and security software applications, allowing organizations to choose how they prefer to deploy and manage Internet security.

For more information or to download a FREE product demo visit **www.cerberian.com** or contact Cerberian at **801.999.2900**, send email to **info@cerberian.com**

[9] Associated Press, "Study: 2 in 5 Web users now have broadband at home", April 21, 2004