WebMarshal™ 2006 & Marshal Filtering List

WebMarshal 2006 is a flexible solution for managing employee Internet access. Marshal Filtering List is a categorized database of more than 60 million websites sorted into 55 categories of related content. Together, WebMarshal and Marshal Filtering List form a comprehensive, accurate and effective solution for securing Internet use. The end solution provides real-time anti-virus and anti-spyware security at the perimeter, control of file downloads/uploads and policy-based access management of Web content.

The Business Issues

Workplace Internet access is common in today's business environment. However, the Internet introduces many threats to business security and profitability. Unsecured Internet access can expose organizations to viruses, spyware, inappropriate or malicious content and excessive non-business use.

"87 percent of all corporate PCs are infected with spyware".

- CNET Article, 2005

In addition to the security challenges, the Internet can be a source of highly offensive content that employees can be exposed to unwittingly. Unmanaged, the Internet can threaten an organization's ability to provide a safe and productive working environment.

"30 percent of all time spent by employees on the Internet is not work-related".

- Angus Reid survey, 2003

There has been increasing public exposure and embarrassment as news stories proliferate about companies who have not protected their businesses from workplace pornography and "cyber-slacking". Misuse of workplace Internet access is not only a risk to security and a threat to business productivity, it also undermines the reputation of an organization when standards and policies are not upheld:

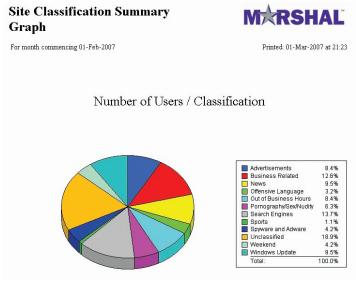
• The Canadian Department of Fisheries and Oceans discovered that each of their 10,000 employees visited seven sex sites per day on average. The most commonly accessed websites were shopping, sports/news and game sites.

• British Telecom, one of the largest telecommunications providers in the UK, fired 200 staff between 2002 and 2003 for regularly accessing inappropriate websites.

• A 2006 survey of 544 Human Resource managers by K Legal and Personnel Magazine (UK) revealed that Internet abuse was the #1 reason for workplace discipline in the UK. This was ahead of all disciplinary actions for dishonesty, violence and health and safety breaches put together. One in four UK companies had sacked employees for Internet misuse.

These are but a handful of examples. In many cases, the companies involved had written Acceptable Use Policies to inform staff of their obligations for work-related Internet access. But, by themselves, these policies often fail to curb non-business Internet use as they are effectively laws without a police force.

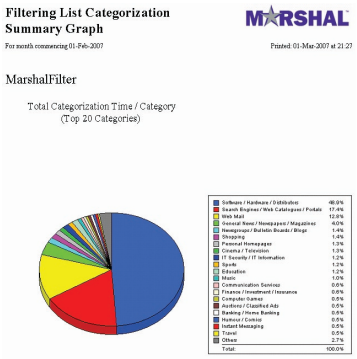
Workplace Internet misuse often ends in the dismissal of long-serving staff that are normally responsible and highly-valued. Dismissing staff costs companies valuable time, legal costs, replacement recruitment and training costs, productivity downtime, and sometimes negatively affects the organization's reputation if revelations become public.



Site Classification Summary Graph

A Total, Multi-layered Security Solution

Many companies appreciate the need to block certain types of websites like pornography and gambling. However, few companies have been able to easily enforce their Acceptable Use Policies, address web virus security and control what files employees are permitted to download from or upload to the Internet. Before now, there has not been a single, integrated solution that can provide all of these capabilities.



Filtering List Categorization Summary Graph

WebMarshal's Internet management together with Marshal Filtering List provides a total solution, integrating a range of Web security and management features into a single, policy-based framework:

• **Real-time Categorization**
– WebMarshal is able to analyze and categorize new websites on-the-fly which is important with the multitude of new websites being launched

MARSHAL™
Secure. Protect. Comply.

every day. WebMarshal uses a powerful lexical (keyword) engine to identify new websites in real-time, before users can view the site. This intelligent categorization engine is easily integrated with the depth of customization that 55 categories and the speed that the Marshal Filtering list provides, along with the guaranteed accuracy that human analysis and review provides. WebMarshal's real-time categorization also addresses anonymizers, or websites that allow users to hide what websites they are actually browsing to.

• Website Database – The Marshal Filtering List is a database of over 60 million websites, three times larger than other popular filter lists, sorted into 55 categories. It is automatically updated every day with approximately 250,000 revised database entries. When combined with WebMarshal's powerful policies, the filtering list allows you to manage user access to a range of websites and types of content appropriate to Acceptable Use Policy.

• Anti-Virus and Anti-Spyware – simply blocking access to pornography and other undesired websites does not protect users from inadvertently clicking on viruses or exposing themselves to spyware. WebMarshal easily integrates with a range of premium 3rd party anti-virus and anti-spyware scanners, as single or multiple layers of security, such as McAfee, Sophos, PestPatrol, Norman and CounterSpy. Once enabled, these scanners scan web traffic for viruses and spyware in real-time as users browse the Internet.

• File Downloads – Once users are allowed access to an approved website and there are no viruses or spyware present, what can they do there? WebMarshal allows you to set restrictions on the type of files and the size of files users can download. This allows you to prevent users downloading unknown executable file types, such as large movie files, MP3s, games and any other file type you care to set restrictions on. Additionally, you can combine file type and file size polices with other policies, such as who the user is and what website they are trying to download from. For example, you can set a policy in WebMarshal that says "no executable file downloads for unauthorized users except when it is from microsoft.com".

• File Uploads – WebMarshal allows you to control what files users can upload, to prevent data leakage. This means that you can set restrictions on uploaded file size, control who can upload sensitive or confidential files and specify which websites users are allowed to upload files to. You can prevent users from emailing sensitive documents or databases to webmail accounts, securing confidential information and preventing loss of restricted, confidential company, employee and customer information.

• Policy & User Management – WebMarshal is a powerful, policy-based solution. WebMarshal can manage users by individual, group or globally across the entire organization. Account information can be easily maintained through Active Directory or Novell Directory Services. WebMarshal also allows flexible usage policies with features like browsing time quotas, bandwidth usage quotas, time-dependant website access (e.g. lunch hours), on-request quota extensions and "click-to-confirm" access to websites for business purposes. With WebMarshal you can accommodate essentially any policy or exception you want, effectively enforcing your companies Acceptable Use Policy.

• Reporting – WebMarshal also provides comprehensive and meaningful reporting which will be invaluable for network administrators and executive managers alike.

- Which websites do we spend the most bandwidth on?
- Who does the most web-browsing by time?
- What types of files do we download or upload the most?
- What types of websites do our users access the most?
- How many viruses did WebMarshal block last month?

WebMarshal reports answer all of these questions and many others with clear and detailed information.

Requirements

The Marshal Filtering List requires WebMarshal 2006 (version 3.7.5.x or higher) and Internet access for regular updates.

Free Evaluation

No other solution provides the depth of security layers or richness of functionality found in WebMarshal and the Marshal Filtering List. You can try WebMarshal and the Marshal Filtering List; free for 30 days. Simply visit www.marshal.com and click on the Evaluation Center.

MARSHAL™

Marshal's Worldwide and EMEA HQ
Marshal Limited,
Renaissance 2200,
Basing View,
Basingstoke,
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

Email: emea.sales@marshal.com

Americas
Marshal, Inc.
5909 Peachtree-Dunwoody Rd
Suite 770
Atlanta
GA 30328
USA

Phone: +1 404 564 5800
Fax: +1 404 564 5801

Email: americas.sales@marshal.com

Asia-Pacific
Marshal Software (NZ) Ltd
Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Greenlane, Auckland
New Zealand

Phone: +64 9 984 5700
Fax: +64 9 984 5720

Email: apac.sales@marshal.com

info@marshal.com | www.marshal.com