



CLEARSWIFT™
The MIMESweeper™ Company

Clearswift White Paper

Policing Web Usage ***Securing the back door***

Table of Contents

Introduction	3
The web widens	3
The 'back door' is wide open	3
URL Blocking is not enough	4
Securing the back door: a three-step approach	5
MIMESweeper™ for Web	6
Just say no	7
About Clearswift	8

Introduction

It was all over the papers. Over 200 civil servants in a single department had been caught downloading porn. They had downloaded more than two million pages during an eight month period, including eighteen thousand images of child pornography. Sixteen people were fired, one was prosecuted and the department's reputation was badly damaged.

In another case, a software organization had to cease its development program because a contractor had stolen its source code – using webmail from inside the corporate network.

In yet another, a major brand was 'named and shamed' because its employees had been downloading vast amounts of illegal MP3 and DVD files.

All these cases, and many more like them, share a common theme: organizations suffering serious damage to their reputation or financial well being due to their employee's misuse of the web.

The web widens

The days when web use was only for select knowledge workers are long gone. Today, the web is a core business tool for most employees and nearly all office workers. The recent Clearswift Internet Survey of 2500 organizations shows how deeply web use is woven into business life:

- 71% of companies provide web access to all employees and another 28% provide access to some staff.
- 65% of companies allow the use of web-based email. Of these, over three quarters allow its use for personal email.

Add to this the use of chat rooms, forums, instant messaging, peer-to-peer and web applications and it becomes clear just how much traffic passes through the HTTP gateway– and right through corporate firewalls.

The 'back door' is wide open

While many companies have some level of email security in place, far fewer pay the same attention to web use. But the threats are very similar. As with email, the hazards can be divided into two main groups: network threats and business threats.

Network Threats

Every organization's IT infrastructure is in danger from malicious code such as viruses, Trojan horses and spyware – all of which are just as readily downloaded or transmitted via webmail and other web applications as they are by traditional email. Once infected, the consequences can range from benign to disruptive to catastrophic.

Spam also poses threats for webmail in the same way as it does for traditional email. Bandwidth is wasted, so is employee productivity, while risk of virus infections is high and will divert IT staff resources.

Business Threats

Poorly managed web use also carries a range of direct threats to business success, including:

- **Loss of productivity** – Non-business web surfing, chat rooms and downloads can make a real impact on productivity. If employees spend an average of 30 minutes per day on recreational surfing (at the low end of most estimates), an organization with a thousand employees will waste over £1.6 million per year.
- **Legal liability** – Employers have a duty to protect staff from 'hatemail' and sexual or racial harassment. Failure to do so can result in liability. Companies can also be prosecuted for illegal downloads of pornography, unlicensed software and music and video files.
- **Reputation damage** – The improper uses of webmail and web applications can lead to serious damage to the organization's reputation and brands, not uncommonly resulting in adverse media coverage.
- **Compliance issues** – The new wave of regulations regarding email archiving and traceability apply equally to webmail, instant messaging and peer-to-peer applications. It's not enough to have a compliance solution that only covers email and the SMTP gateway as employees can just as easily disclose confidential information via webmail, chat rooms and forums.
- **Loss of confidential information** – As email security becomes more common, Webmail is increasingly used to by-pass security at the SMTP gateway in order to send confidential information out of the organization. Without web content security in place, important financial information, strategic plans and new product designs can be lost.

All of these threats can have a very significant financial impact that will inevitably be paid by any organization that fails to secure its web traffic.

URL Blocking is not enough.

Most organizations still have little or no security in place to cover web traffic. Many incorrectly assume that their firewall will handle web-based threats; but web traffic passes through firewalls by design.

Others have put in place more or less rigorous URL filters, which block access to websites known to be contrary to corporate policy.

While this URL blocking is an important part of any web defense, it is only a partial solution:

- **No URL filter can ever be completely up-to-date** – even with millions of URLs categorized and daily updates, no filter can keep ahead of the sheer volume of new websites that may contravene corporate policy. Over 30,000 new pornography sites are born every day – not to mention the more legitimate but still time-wasting sites for gaming, gambling, shopping and chat.

- **URL filters can't guaranty to stop webmail** – so they can't stop staff from sending out confidential, illegal or abusive material by web.

Clearly, a strong URL filter is a first line of defense against web-borne threats. But is far from a complete solution.

Securing the back door: a three-step approach

As costly and common as web-based threats are, they can be stopped. Clearswift recommends a three-step approach to web security that brings the web gateways in line with the highest levels of email security.

1. Develop a web security policy

Web security is a policy issue. Each organization has to decide how it wants its employees to use the web, which activities are allowed by whom and which are forbidden.

No two organizations will have the same policy because no two organizations do business in the same way. A web use policy will reflect both the nature of the business and the organization's culture:

- Some organizations prohibit all non-business surfing while others allow it at lunchtime and after 5:00pm.
- Some block webmail, others allow it and still others only let certain departments use it.
- Some organizations block the sending out of spreadsheets, others block CAD designs.

Whatever decisions are made, no security technology can do its job unless it's referencing a clear set of policies.

2. Communicate the policy

The point of web content security is not to catch as many rule-breakers as possible. It is to educate all employees, to remove temptation and deter breaches of policy.

The best web security policy can only be effective if all staff are aware of it.

Once a policy is in place (along with the technology to police it), it's essential to make sure that all staff are clear about the policy and understand how it is being monitored and managed.

This should include a module in new employee induction programs that explains the policy and shows how it is being implemented.

3. Implement multi-layer content security

Once a policy is in place, it must be enforced and monitored using multi-layer content security. Firewalls, user authentication and intrusion detection are core infrastructure security tools, but they can't address web-based threats without three more essential pieces:

- **URL Filtering** – An important first line of defense. An effective URL filter must cover a huge range of URLs in many categories and languages. It should be automatically updated and allow granular policy support so that rules can be set for individual, department, time of day and type of traffic.
- **Real-time Content Analysis** – There will always be websites that are not yet blocked by even the best filters. There will also be outbound web traffic that may contain confidential or illegal content.

For these cases, real-time content filtering is essential. An effective filter must evaluate all content traveling in both directions – including message content and all attachments. It must apply recursive analysis to unwrap and read content such as spreadsheets embedded in zipped Word documents.

Finally, a content analysis tool must include full reporting and alerting to allow for effective management and tracking.

- **Anti-virus Integration** – The URL filter and Content Analysis engine must both be easily integrated with an organization's chosen anti-virus tools. The anti-virus performance will be significantly improved as it is acting on content already broken down into its component parts – even a virus in an embedded, compressed file will be scanned.

Just as URL filters are vulnerable between updates, anti-virus tools are vulnerable before patches can be written and distributed. This 'Zero-Day' vulnerability can be closed off with effective content analysis that can block entire file types and classes of attachment before virus patches are deployed.

This multi-layer approach to web content security is the only way to block every kind of threat to the network and the business, whether incoming or outgoing. Organizations serious about protecting themselves from web-based threats should settle for nothing less.

MIMESweeper™ for Web

MIMESweeper for Web from Clearswift offers the only integrated, multi-layer content security solution for all web-based threats. It combines a best-of-breed URL Filter with the world-leading MIMESweeper content analysis engine and complete integration of any chosen anti-virus tool.

The URL Filter

MIMESweeper for Web offers a best-in-class URL Filtering module that draws on a database of over 6.3 million URLs in forty categories. This covers over 1 billion pages in 65 languages – with thousands of sites and pages added every day. The URL Filter is automatically updated once a day, with no need for administrator intervention.

The Content Analysis engine

Clearswift invented content analysis and is still the worldwide market leader. The MIMESweeper for Web engine delivers complete recursive analysis of all content and attachments.

Because it recognizes more types of data, policies can be set with optimum granularity – improving performance and supporting the way each organization works.

The MIMESweeper engine also delivers comprehensive reporting and alerting to ensure compliance to the same rigorous standards as any email compliance solution.

The Anti-virus integration

MIMESweeper integrates easily with the leading anti-virus applications, singly or as multiples. And the MIMESweeper content analysis engine gives the AV tool access to the most deeply embedded file types so they can do their jobs better.

Before the anti-virus tool can issue patches for new threats, MIMESweeper lets administrators block any suspicious file types, helping to close the Zero-Day window.

Taken together the three layers add up to the most complete protection against all web-based threats, with the most granular policy support on the market.

Just say no

Unsecured web traffic poses a serious threat to every organisation and looking the other way is no longer an option.

The organizations who rely on simple URL filtering – and those who do nothing at all – are acting irresponsibly and are vulnerable to a variety of very real threats.

Organizations that implement a three-stage approach to web content security by developing a security policy, communicating it to staff and enforcing it with a multi-layer solution can move forward towards their goals with confidence.

Anything less is asking for trouble.

Contact Clearswift

United States

303 Twin Dolphin Drive, 6th Floor,
Redwood City, CA 94065
Tel: +1 800 982 6109 | Fax: +1 650 632 4601

United Kingdom

1310 Waterside, Arlington Business Park, Theale,
Reading, Berkshire, RG7 4SA
Tel: +44 (0) 11 8903 8903 | Fax: +44 (0) 11 8903 9000

Germany

Amsinckstrasse 67, 20097 Hamburg
Tel: +49 40 23 999 0 | Fax: +49 40 23 999 100

Sweden

Frösundaviks allé 15, 4tr, SE-169 70 Solna
Tel : +46 8 50 90 40 78 | Fax : +46 8 655 26 10

Australia

Ground Floor, 165 Walker Street, North Sydney,
New South Wales, 2060
Tel : +61 2 9424 1200 | Fax : +61 2 9424 1201

Japan

Eisho Takanawadai Bldg 6F, 2-11-8, Minato-ku Shiroganedai
Tokyo-to, 108-0071
Tel : +81 (3) 5423 8171 | Fax : +81 (3) 5423 1274

© 2004 Clearswift Ltd. All rights reserved. The Clearswift Logo and Clearswift product names including MIMESweeper™, MAILsweeper™, e-Sweeper™, IMAGEmanager™, REMOTEmanager™, SECRETSweeper™, ENTERPRISEsuite™, ClearPoint™, ClearSecure™, ClearEdge™, ClearBase™, ClearSurf™, DeepSecure™, Bastion™ II, X.400 Filter™, FlashPoint™, ClearDetect™, ClearSupport™, ClearLearning™ are trademarks of Clearswift Ltd. All other trademarks are the property of their respective owners. Clearswift Ltd. (registered number 3367495) is registered in Britain with registered offices at 1310, Waterside, Arlington Business Park, Theale, Reading, Berkshire RG7 4SA, England.