10 Essential Steps to Web Security

A Clearswift Best-Practice Guide

CLEARSWIFT™
Simplifying content security

Introduction

Web 2.0 brings Threat 2.0.

The web is changing fast from a one-way medium for ‘brochure-ware’ to a highly interactive, sophisticated and increasingly mission-critical platform.

The new, ‘Web 2.0’ applications – from social networking to tagging, blogging and presence-aware services like IM – reflect the new web-enabled relationships forming between individuals and enterprises.

But each new development of the web brings with it a new species of parasite. Spyware, adware, keyloggers, blogspam and IM viruses seem to sprout up within days of any new trend.

Clearly, it’s never been more important to protect your enterprise from the hazards of uninhibited browsing.

This short guide summarizes ten steps to web security. Do them all, and you’ll be better protected than 98% of enterprises out there. But the target never stands still. More than the steps listed here, it’s important to focus on the principles behind the steps, including: policy, vigilance, simplification, automation and transparency.

Putting these principles into action starts with the steps listed here. But it can never end there. At Clearswift, we invest massive resources into staying on top of every emerging Internet-borne threat. Keep in touch and we’ll keep you up to date.

Step 1

Policy, policy and policy.

All web security **must** start with policy.

- **Policy focuses your attention –** on the things you need to stop and the things you're happy to allow

- **Policy drives up compliance –** when everyone understands what's unacceptable, responsible web use becomes the norm

- **Policy enforces fairness –** by making the rules clear to all

- **Policy facilitates prosecution –** of the guilty and defense against regulations demanding due diligence

It's not difficult: create a sensible policy; make sure everyone understands and agrees with it; and enforce it with technology at every gateway.

MIMEsweeper web security products enforce your web security policy by filtering all web traffic in both directions. Any traffic that breaches policy is automatically blocked and a report or alert is generated.

Step 2

Now fine tune the policy.

When it comes to policy, one size does not fit all. Your policy should reflect the way you do business. A music company may allow all MP3 files while an engineering department may need to upload and download CAD files.

For most companies, these basic web rules are fairly fundamental:

- Block viruses
- Prevent and log Spyware call home activity
- Disable executables
- Only allow ActiveX from trusted sites
- Forbid intolerant content (e.g. racial, sexual or religious discrimination)
- Prevent access to inappropriate sites (e.g. porn and gambling sites)
- Inhibit loss of confidential or sensitive data

After this kind of thing, policy becomes highly tailored. You may want to allow certain departments or individuals specific privileges while denying them to the rest of the organization.

Or you may want to set times of day when certain activities are allowed (e.g. web shopping during lunch breaks). Or identify specific files that must never be uploaded or sent out through webmail.

The point is this: your policy should dictate your technology, not the other way around. If your filtering tools don’t let you do what you want to do, find better tools.

MIMEsweeper offers the most granular policy management in the industry. We pioneered policy-based content security and still lead the way.

Step 3

Attack spyware from multiple angles.

Spyware is one of the more insidious (and annoying) web hazards. Fight it from three directions:

- **Stop it at the gateway –** with automated filtering and spyware profiling
- **Stop it at the desktop –** by scanning regularly to eradicated embedded spyware
- **Stop it 'calling home' –** so newly installed spyware can't get back to base for instructions

The MIMEsweeper Web Appliance uses Aluria spyware profiles to stop spyware at the gateway. Spyware downloads and call-homes are blocked by the MIMEsweeper Web Appliance using Aluria's anti-spyware and the award-winning MIMEsweeper content filtering technology.

Step 4

Block undesirable URLs.

Millions of dubious websites spring up daily. You can't keep track of them all. But we can.

Use a comprehensive URL filter to block whichever kind of sites your policy demands – including gambling, pornography, remote proxies, hate site, or webmail.

You can supplement the filter with a blacklist of your own, or be able to make exemptions with a whitelist.

MIMEsweeper web security solutions include one of the world's most comprehensive URL Filters, cataloguing over 18 million URLs and 2 billion web pages into 40 distinct categories. You decide what to allow and prohibit. We keep the database up-to-date.

Step 5

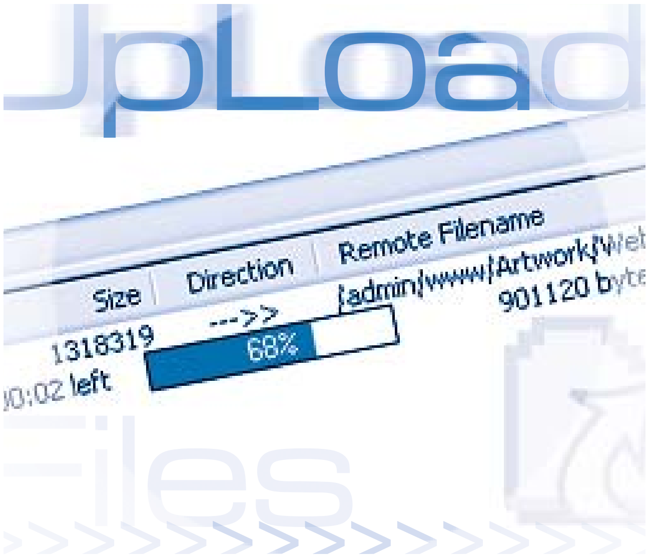
Smash 'container' file types to bits.

An innocent-looking spreadsheet can carry a virus. A presentation can carry spyware. A zip file can contain any number of files that might infect your network. A Word doc can contain 'fuzzing' software to crash the application and exploit the wreckage.

Your web security must be able to decompose all container file types to scan for deeply embedded malware. Superficial scanning may have worked five years ago. Not any more.

MIMEsweeper technology uses deep, recursive analysis to break down all container files into their constituent parts, then analyze, clean (if necessary), and apply policy to each one independently.

Step 6



Watch your uploads.

Companies that defend against hazardous web downloads are often completely vulnerable to threats going in the reverse direction.

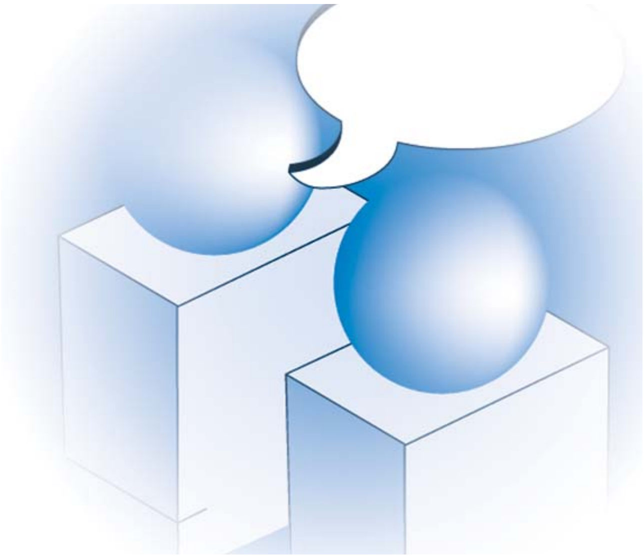
Web uploads can include webmail with customer data attached; stolen MP3 and movie files that not only sap network resources, but could also make your company liable for illegal use of copyrighted material; or IM (Instant Messaging) which is also a major source of data leakages.

Uploaded material has led to dozens of infamous prosecutions and embarrassments. Make sure your defenses are two-way.

MIMEsweeper offers comprehensive, bi-directional web security, applying anti-virus, anti-spyware, URL blocking and content filtering to all outbound traffic as well as inbound.

Step 7

Protect (or block) your IM traffic.



Instant Messaging has become a common traffic type through the HTTP gateway.

Your policy will determine if that's allowed or prohibited. Either way, your defense strategy needs to include IM traffic in both directions.

Clearswift solutions let you block all IM traffic, allow it during certain times or for specified people, or filter it thoroughly for all policy breaches – just like web or email traffic.

Step 8

Monitor all web activity.

That which gets measured gets managed. Your web security should include comprehensive monitoring, reporting and analysis.

Break down your analysis by user, site, activity, bandwidth, or threat , starting with big-picture snapshots including web activity, number of requests and data volumes.

For more real-time defense, alert triggers can flag serious breaches before they get out of hand.

Good monitoring and reporting will let you spot suspicious activity early, revise your policy when needed and improve your resource allocation.

MIMEsweeper web security solutions are famous for their rich, interactive, graphical web-based monitoring, reporting and alerting.

Step 9

Simplify policy enforcement.

Web security can eat up entire IT departments unless you simplify, automate and streamline.

Deploying, updating, managing and monitoring processes need to be designed with the real world in mind. Because over-complicated or poorly integrated web security not only wastes time and resources, it weakens your defenses.

Clearswift simplifies web security with software and appliances that are easy to install, maintain, update and manage.

Our web security appliances pre-integrate all of the key web defenses – anti-virus, anti-spyware, URL blocking and content filtering – in a single solution. And our software integrates easily with your own chosen solutions to create a single system.

Updates are automated and multi-box support makes central policy management and reporting easy.

Step 10

Keep an eye on emerging web activities.

Blogs, forums, social networking, P2P file-sharing… it’s all exciting stuff. But it all opens up new windows of opportunity for the people and organizations that make money from exploiting loopholes.

As new web services emerge, make sure to reflect your view of them in your policy. Consult with key stakeholders, establish the rules and issue updates to all staff. Then update your gateway defenses to reflect your new policy.

Rule of thumb: if it moves, it can be scanned, filtered and protected.

MIMEsweeper technology embraces new web developments as they emerge. We’re active participants in the global security initiatives and maintain excellent relationships with the very best minds in web security (some of whom work for us!). We’ll help you keep your defenses up-to-date.

Next steps.

Some of the steps listed here may seem obvious. But it never ceases to amaze us how many organizations miss so many of them.

Start with your own policy. Does it reflect all of the issues identified above? Has everyone in the organization read it and does everyone know where to find it? Is it continually updated to reflect new threats and activities? And, finally, do you have the right technologies in place to enforce your policy at all gateways in both directions?

If the answer is no, we can help. If it's yes, we're probably already helping.

Clearswift was a pioneer in web security back when 56kbps seemed fast. Since then, we've seen every kind of attack in every kind of environment, from small businesses to the largest multinationals.

All of our solutions reflect our experience in real deployments. We think this makes us the ideal partner for your own web security strategy. And we'd welcome the chance to earn that partnership.

Talk to us about simplifying your web security without compromising.
Or visit www.clearswift.com to see an introduction to our web security products.

About Clearswift

Clearswift simplifies content security.

Our products help organizations enforce best-practice email and web use, ensuring all traffic complies with internal policy and external regulations.

Our range of content filtering solutions makes it easy to deploy, manage and maintain no-compromise email and web security for both inbound and outbound traffic.

Clearswift is the only vendor to offer comprehensive, policy-based content security in all three deployment methods: as software, as an appliance and as a managed service.

All three platforms are designed to take the hassle out of securing internet traffic, with a clear, intuitive management interface; automatic, ‘zero-touch’ updates; powerful reporting and common-sense policy management.

Twenty years of experience across 17,000 organizations has helped us raise security standards while simplifying security management at the same time.

We’ve helped many of the world’s most successful organizations use the internet with confidence and are committed to staying ahead of the market and helping our customers defend against all emerging threats.

Contact Clearswift

United States
100 Marine Parkway, Suite 550
Redwood City, CA 94065
Tel: +1 800 982 6109 | Fax: +1 888-888-6884

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

Spain
Cerro de los Gamos 1, Edif. 1
28224 Pozuelo de Alarcón, Madrid
Tel: +34 91 7901219 / +34 91 7901220 | Fax: +34 91 7901112

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

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

Japan
Hanai Bldg. 7F, 1-2-9, Shiba Kouen Minato-ku
Tokyo 105-0011
Tel : +81 (3) 5777 2248 | Fax : +81 (3) 5777 2249