10

Essential Steps to Email Security

A Clearswift Best-Practice Guide

CLEARSWIFT™
Simplifying content security

Introduction

It's a jungle out there.

If email came with a health warning it would have to say something like:

CAUTION:
EMAIL CAN BRING DOWN YOUR NETWORK, CRASH YOUR APPLICATIONS, STEAL YOUR CONFIDENTIAL DATA, GET YOU THROWN IN JAIL AND DESTROY YOUR COMPANY'S REPUTATION.

When you think about the risks, it's amazing we let email into our enterprises at all. Then again, just try switching it off…

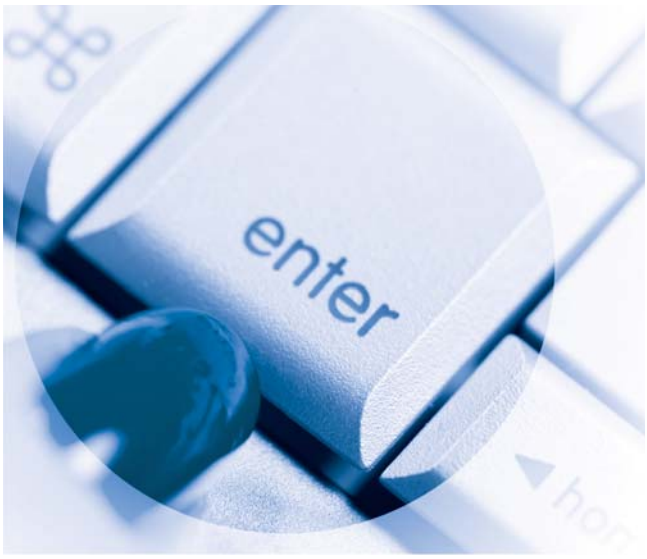
Every enterprise has to find a balance between security and the ability to carry on conducting business freely. This short guide is about finding that balance.

By following some basic principles, there's no reason you can't let legitimate business email move into, out of and within your enterprise while stopping the things that cause damage: viruses, spam, spyware, trojans, phishing, Denial of Service attacks, the loss of sensitive data and the collection of illegal, immoral and just plain offensive material.

There's no escaping it: the people behind these threats are getting increasingly sophisticated and well-funded. The only real defense is the vigilant application of policy, technology and processes designed to keep email safe and secure.

Step 1

Establish and promote a robust email policy.



Servers don't send email, people do. That's why it's so important that everyone in your organization understands exactly what is acceptable when using email.

In our experience, there's an inverse correlation between how much time a company spends developing and promoting its email policy and how much money they spend chasing the problems that poorly managed email creates.

A good policy looks like this:

- **Clear –** easy to understand, with minimal room for interpretation.
- **Realistic –** based on the involvement of all parts of the business to reflect the way you work.
- **Granular –** recognizing that different users, departments and locations use email differently (while sharing common ground).
- **Flexible –** the ability to change as your business changes.
- **Up-to-date –** covering all new threats and reflecting continuous feedback from the business.
- **In-your-face –** an effective policy is seen on induction, on bulletin boards, in cafeterias, newsletters, e-updates…

Don't just tell all staff about the policy, tell them how you're enforcing it using filtering technology. The deterrent effect alone will prevent breaches before they occur (and give you a stronger case if prosecution is necessary).

We feel so strongly about policy, we've decided to share our own. To see Clearswift's email policy, contact info@clearswift.com.

Clearswift's email security solutions are all policy-driven. The entire MIMEsweeper range is designed so that you can support your policy with our technology. You set the rules, let MIMEsweeper police them.

Step 2

Be clear about what you're defending against.

If your email security strategy doesn't cover every one of these threats, you're inviting attack:

- Viruses, trojans and bots
- Spam and phishing attacks
- Spyware
- Denial of Service Attacks
- Confidential data leaks
- Hatemail and pornography
- Illegal material and stolen files
- Regulatory breaches

A security solution that leaves any of these undefended is no solution at all. When your CEO calls you into his office and slams a newspaper on the desk with the headline, CHILD PORN RING OPERATES FROM Xco OFFICES, your great spam detection rates are not going to be of much help.

MIMEsweeper products cover every email threat, letting your policy dictate the response to each. And as new threats emerge, MIMEsweeper integrates them quickly and easily. No loopholes.

Step 3

Make sure your defenses are sustainable.

An email security strategy that over-burdens the IT department and email administrators will ultimately fail – not to mention wasting talent that can be better employed elsewhere.

A sustainable approach is:

- **Technology-enabled –** supported by robust traffic filtering and analysis tools.
- **Integrated –** handling all threats in one solution from a single management console.
- **Web-managed –** giving authorized administrators access from any browser anywhere.
- **Shared sensibly –** with users managing their own quarantine lists and authorized departments helping with relevant policy breaches.
- **Automatically updated –** minimizing manual patches and updates to profiles, software and operating systems.
- **Easy to deploy, monitor & manage –** with comprehensive reporting to keep things on track.

Take a look at your current defenses. If any of the above are not true, you're probably making life difficult and compromising security.

MIMEsweeper technology integrates best-of-breed defenses into a single, web-managed platform with centralized policies, roles-based management and auto-updates. No solution is easier to own.

CLEARSWIFT™
Simplifying content security

Step 4

Make sure all traffic is protected.

It's no good deploying great security for inbound emails if the outbound and internal traffic is unsecured.

- **Outbound** traffic can carry viruses or confidential data.
- **Internal** messages can carry hatemail, abuse or illegal files.
- **Webmail** – can include any or all threats founding normal email.

Are you as rigorous about your outbound, internal and webmail traffic as you are about inbound?

MIMEsweeper covers all traffic in all directions, inbound, outbound and internal. And webmail is covered as part of the MIMEsweeper web solutions.

Step 5

Choose the right deployment option.

Email security solutions are available in three form factors, each with its own pros and cons:

Software
Great for subtle policy control and complex, distributed environments but can have higher management overheads.

Appliances
Great for ease of use but you may prefer your own servers to make the most of your in-house skills. Beware though; some vendors make wild claims, and many appliances on the market have limited functionality and are not as “plug ‘n’ play” as they ought to be.

Managed service
Keeps unwanted traffic completely off the corporate network but some enterprises are uncomfortable with third-party handling of such sensitive traffic.

Only you can decide which deployment method – or which combination – is best for your enterprise.

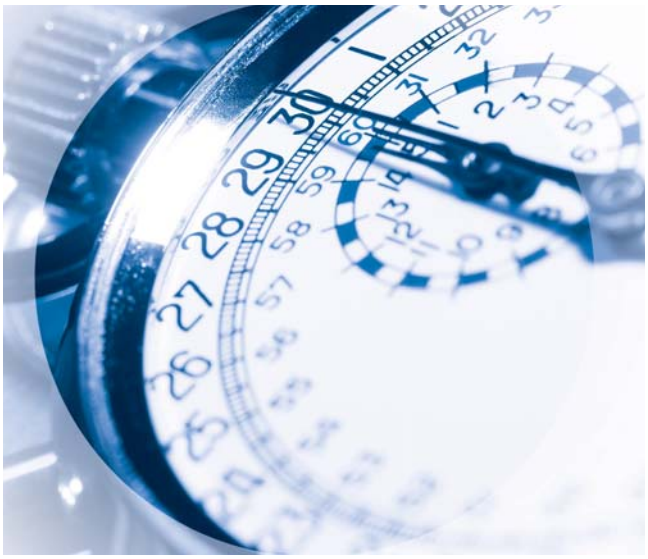
For smaller organizations, a managed service or appliance is often effective and efficient.

Larger enterprises often choose a layered model, with appliances at the gateway and software deployments behind the firewall.

MIMEsweeper email security solutions are available in all three form factors so you can choose the deployment that is best for you. All share the same management interface, policy management and integrated functionality so you make no compromises.

Step 6

Close the Zero-day window.



Anti-virus and anti-spyware solutions are great for defending against known dangers. But what stops a brand new virus from entering your network before it can be profiled and patches can be distributed and installed?

This Zero-day window is one of the most glaring vulnerabilities in many organizations email strategy. And there's only one way to defend against it: content filtering with intelligent rules.

Content filtering lets you stop messages that exhibit the characteristics of unwanted traffic even if they're not recognized malware. Your policy can decide what to do with this suspicious traffic –block it, park it, delay it, delete it, report it or do any combination. Just don't let it through untouched.

MIMEsweeper technology is built around the world's most robust content filtering engine. Every message is broken down to its smallest parts, analysed against relevant policy and acted on if at all suspicious.

Step 7

Future-proof your defenses.

The threats targeting your enterprise are always changing. You don't want to invest in technologies that will be out of date when the next piece of bad news comes around the corner.

The most important part of any email security solution is the filtering and policy engine. To be effective and efficient it needs to allow you to easily add new rules, profiles and processes to block emerging threats.

Clearswift pioneered policy-based security and content filtering and our MIMEsweeper engines still lead the industry – in technology and deployments. As new threats emerge, MIMEsweeper adapts to respond.

Step 8

Monitor traffic behavior and performance.

You can't secure what you can't see. Use reports to flag all email behavior and performance issues so you can take swift action.

Behavioral reports show you the biggest senders and recipients and the file types and sizes they use, so you can spot an employee running an unauthorized business.

Performance reports include mail volumes and data types by location, department, server or gateway.

Both kinds of reports help you refresh your policy and re-allocate resources to meet legitimate demand (while putting a stop to resource-draining illegitimate use).

All MIMEsweeper solutions come with comprehensive web-based reporting and analysis tools to help you monitor all traffic, generate reports and flag problems before they get out of hand. There's no better way to stay on top of your email traffic.

Blocking attachments over a given size can also protect your storage and bandwidth resources. Set your policy to either strip out the massive files – or park them for delivery at night. Either way, an audit trail of all breaches will help you manage any issues.

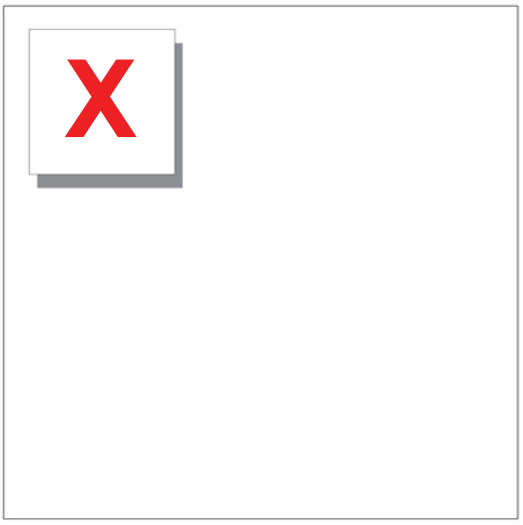
Step 9

Don't forget images.

Not all unwanted messages are verbal. Indecent, illegal and unpleasant images can upset staff, incur legal action and frighten the horses.

Confidential company material can also come in the form of images – including product designs, ad campaigns and package changes.

MIMEsweeper image scanning identifies and quarantines likely pornography, noting the sender and recipient. And you can add images such as confidential designs so they're stopped before leaving the network.



Step 10

Invest in compliance.

New financial reporting and data protection regulations can add a significant burden to the IT department.

The email gateway is the ideal place to start automating many of the procedures that regulations demand, including:

- **Encryption –** to protect sensitive traffic form unauthorized access
- **Archiving –** to store, search and retrieve all messages in all directions
- **Reporting –** to audit traffic and keep a record of all activities relating to message release

With an integrated security solution already filtering, and reporting on, all traffic, it's easy to add encryption or archiving functionality.

MIMEsweeper lets you choose your own encryption and archiving tools and integrate them easily into your security strategy. And world-class reporting tools are already built in to support robust compliance.

Summary

Automating Enterprise Content Governance

These steps summarize a simple approach to best-practice email security – a cornerstone of Enterprise Content Governance.

While the technologies to defend against emerging threats may change, the basics haven't:

- Promote a clear email policy
- Enforce it with the right technology
- Keep it simple

At Clearswift, we've been involved in content security for over 20 years. We've developed robust defenses against every kind of attack and helped a wide range of enterprises secure their email and web traffic.

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