

10

Essential Steps to Email Security

A Clearswift Best Practice Guide



Introduction

Email - so simple, so important

Modern business is reliant on email. All organisations using email need to answer the following questions:

How do we control spam volumes without the risk of trapping a business email?

How do we prevent infections from email-borne viruses?

How do we stop leakage of confidential information?

Can we detect and stop exploitation from phishing attacks?

How do we control brand damage from occurring due to employee misuse?

How do we prevent inappropriate content from being circulated?

Considering just these risks, it is amazing that organisations allow email at all. Then again, just try switching it off...

Every company has to have security with the ability to carry on conducting business freely. This short guide will help you find the right balance.

By following some basic principles, email can be allowed to move freely into, out of and around your enterprise while stopping the things that cause damage: viruses, spam, spyware, trojans, phishing, denial-of-service (DoS) attacks, the loss of sensitive data and the exchange of illegal, immoral or offensive material.

Those responsible for these threats are getting increasingly sophisticated and well-funded. The only real defence is the vigilant application of policy, technology and processes designed to keep email safe and secure.



1

Establish and promote a robust email policy

Servers don't send email, people do. That's why it is important that everyone in your organisation 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 created by poorly managed email.

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** - recognising 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
- **Visible** - an effective policy is seen on induction, on bulletin boards, in cafeterias, company newsletters...

Don't just tell all staff about the policy: tell them that it is enforced using filtering technology. The deterrent effect alone will prevent breaches from occurring.

CLEARSWIFT SECURE Email Gateway is powered by MIMESweeper, our renowned content-inspection and filtering technology. You set the rules - let MIMESweeper police them.

2

Be clear about the dangers

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

- Viruses
- Trojans and bots
- Spam and phishing attacks
- Spyware
- Denial-of-service (DoS) 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. Clearswift products protect against all email threats, letting your policy dictate the response. And as new threats emerge, Clearswift integrates them quickly and easily. No loopholes.

3

Make sure defences 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 interface
- **Web-managed** - giving administrators access from any browser, anywhere
- **Shared sensibly** - with users managing their own quarantine lists and authorised departments helping with relevant policy breaches
- **Automatically updated** - minimising manual patches and updates to profiles, software and operating systems.
- **Easy to deploy, monitor and manage** - with comprehensive reporting to keep things on track

Take a look at your current defences. If any one of the above is not true, both efficiency and security could be compromised.

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

4

Protect all traffic

It's no good deploying great security for inbound and outbound emails if use of webmail is overlooked and unsecured.

By combining Clearswift SECURE Web Gateway with CLEARSWIFT SECURE Email Gateway organisations can secure all messaging traffic. Policies can be created that permit the same rules and privileges to be applied for both normal mail and webmail from the same policy console. This saves time and provides consistency across your platforms.



5

Choose the right deployment option

Clearswift SECURE Email Gateway offers a variety of deployment options:

Packaged Dell hardware

Clearswift uses the latest server platforms from Dell to offer comprehensive and robust devices that protect your network. Backing from a world-leading vendor offers complete peace of mind.

Own hardware

Clearswift understands that organisations may wish to use hardware from a preferred vendor. To help, Clearswift has created a Hardware Compatibility List (HCL) by testing its solutions on a variety of hardware platforms, from vendors such as HP and IBM. Clearswift's HCL provides customers with the freedom to build systems to meet specific needs.

VMware / Hyper-V

Clearswift's unified information-security solutions can be deployed in virtual environments to achieve more with less, saving on hardware costs, storage space and power consumption. With Clearswift solutions, customers are free to mix and match physical and virtual deployments to provide the best of both worlds.

Of course, only you can decide which deployment method - or combination of methods - is best for your enterprise. Smaller organisations, for instance, may prefer a packaged solution; or the option to use existing owned hardware. Larger companies often choose a mix of physical and virtual servers to better balance performance and resilience.

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 security holes have been identified?

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

In addition to tried-and-trusted anti-virus and outbreak filters that can detect new malware, Clearswift SECURE Email Gateway content-filtering technology analyses message attachments and identifies the characteristics of malicious content. Your policy can decide what to do with this suspicious traffic: block it, park it, delay it, delete it, report it - or any combination. Just don't let it through untouched.

CLEARSWIFT SECURE Email Gateway 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 dealt with accordingly.

7

Future-proof your defences

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 crops up. That's why timely and easy upgrade paths are essential.

As well, 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 SECURE Email Gateway dynamically updates its anti-virus and spam configuration; and patches can be applied at a time to suits the administrator. Moreover, Clearswift pioneered policy-based security and content filtering. Our content engines still lead the industry - in technology and deployments. As new threats emerge, Clearswift adapts to respond.

8

Monitor traffic behaviour and performance

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

Behavioural reports will highlight the biggest senders and receivers of email, along with the file types and sizes used.

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

This information can prove invaluable in indentifying problem areas, allowing you to shape policy and reallocate resources accordingly.

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

All Clearswift solutions come with comprehensive web-based reporting and analysis. These monitor all traffic, generate reports and flag problems before they get out of hand. Reports can be scheduled for automatic delivery into your inbox. There's no better way to stay on top of your email traffic.



9

Secure your data

With companies collaborating more so increases the risk of sensitive data being read by unauthorised people. It is therefore essential to employ email encryption, allowing users to send messages securely to external organisations. The trouble is, many encryption solutions use proprietary methods that are both complex and expensive.

Clearswift SECURE Email Gateway breaks the mould, delivering easy-to-use, standards-based encryption at an affordable price. By using industry standard protocols of S/MIME, TLS and PGP - not to mention an ad-hoc method that requires no set-up at the recipient's end - Clearswift SECURE Email Gateway ensures that messages are encrypted strongly, reliably and according to policy.

10

Adhere to the rules

Many organisations need to adhere both to industrial standards and local regulations.

Some breaches might result in a figurative slap on the wrist but it is important to understand that some government agencies have powers to inflict heavy fines. In other words, breaking the rules could break your company.

Using Clearswift SECURE Email Gateway to define and enforce the rules will mitigate both regulatory and reputational risks.

Contact Clearswift

UK - International HQ
Clearswift Limited
1310 Waterside
Arlington Business Park
Theale
Reading
Berkshire
RG7 4SA
UK
Tel : +44 (0) 118 903 8903
Fax : +44 (0) 118 903 9000
Sales: +44 (0) 118 903 8700
Technical Support: +44 (0) 118 903 8200
Email: info@clearswift.com

Australia
Clearswift
5th Floor
165 Walker Street
North Sydney
New South Wales, 2060
AUSTRALIA
Tel : +61 2 9424 1200
Fax : +61 2 9424 1201
Email: info@clearswift.com.au

Germany
Clearswift GmbH
Amsinckstrasse 67
20097
Hamburg
GERMANY
Tel : +49 40 23 999-0
Fax : +49 40 23 999-100
Email: info@clearswift.de

Japan
Clearswift K.K
7F Hanai Bldg.
1-2-9 Shibakouen,
Minato-ku, Tokyo
105-0011
JAPAN
Tel : +81 (3)5777 2248
Fax : +81 (3)5777 2249
Email: info.jp@clearswift.co.jp

Spain
Clearswift España S.L.
Cerro de los Gamos 1, Edif. 1
28224 Pozuelo de Alarcón
Madrid
SPAIN
Tel : +34 91 7901219 / +34 91 7901220
Fax : +34 91 7901112
Email: info.es@clearswift.com

United States
Clearswift Corporation
161 Gaither Drive
Centerpointe
Suite 101
Mt. Laurel, NJ 08054
UNITED STATES
Tel : +1 856-359-2360
Fax : +1 856-359-2361
Email: info@us.clearswift.com

Summary

Automating Enterprise Content Governance

These steps summarise a simple approach to best practice in 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

Clearswift has been involved in content security for over 20 years. Our company has developed robust defences against every kind of attack and helped a wide range of enterprises secure their email and web traffic.

Talk to us about simplifying your information security without compromising. Or visit www.clearswift.com for an introduction to our unified information security products.

About Clearswift

Clearswift simplifies content security

Clearswift is a trusted information-security company with a history of innovation. We understand content and the way people work and communicate. Clearswift's content-aware, policy-based solutions benefit 17,000 organisations globally, enabling them to manage and maintain no-compromise data, email and web security across all gateways and in all directions.

Clearswift's track record in innovation includes developing many of the features the security industry now considers standard, such as image scanning, policy-based encryption and user-level message tracking. Clearswift continues to lead the IT security industry with the deployment of production-ready virtual appliances on the VMware ESX and ESXi platforms. These are built on powerful, effective and tested content-aware policies that protect our customers and their employees.

We believe that the IT security industry should evolve to help organisations interact and collaborate better in the connected world, rather than restricting communications. Clearswift's content-aware solutions reflect the mature approach that business demands, enabling safe and effective communication for unfettered productivity.

Simply, Clearswift's unified web and email security solutions dispense with fear and negativity, enabling businesses to get on with business without compromising security.