

Coppferfasten **User-Controlled Email** **Solutions**

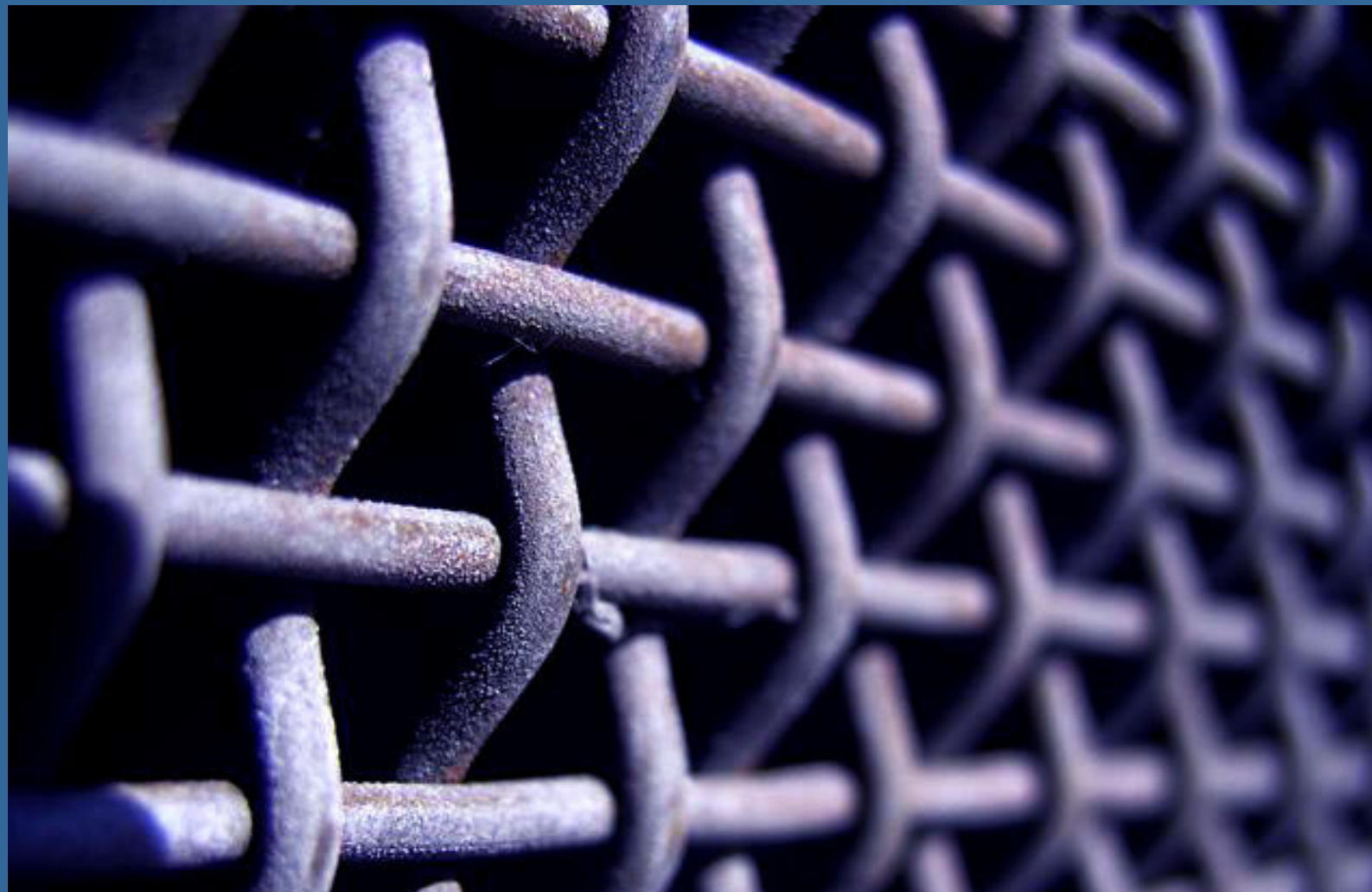


Table of Contents

Executive Summary	3
Current Landscape	4
IT Managers Set The Agenda	5
Facing Spam, Viruses and Threats	5
Setting Priorities	6
Shifting the Balance to the User	6
MFA — Self-Service Email Management	7
How It Works	7
User Management	8
Administrative Management	8
Business and Technical Benefits	9
Silver Bullets	10
The Bottom Line	12

Executive Summary

In less than ten years, the Internet has emerged from an obscure research project to the undisputed driving force behind today's digital economy. Central to this has been the role played by email, which has rapidly become one of the core—if not the most essential—service for companies who have embraced web-facing technologies. Few would argue that email has revolutionized how we communicate and promises to set the pace for the foreseeable future.

But progress comes with a price. For IT Managers the widespread adoption of email creates many new headaches. Examples of these include reducing disruptions to business operations, protecting the shareholders and staff from potential legal issues, and blocking obscene images, threats, and hate-mail.

As spam and virus outbreaks escalate, the demand for secure email management products continues to grow. To counter these measures, IT Managers require advanced technologies that protect internal users, partners, and customers from virus attacks, trojan horses, and malicious executables files.

Pressure from consumer groups and industry watchdogs has ensured that the remit of email security systems has increased, as it is no longer acceptable for systems to concentrate solely on virus protection. IT Managers are now responsible for tracking violations of corporate policies, such as sexual harassment, while monitoring the protection of digital assets and intellectual property rights.

In response to this spectrum of business and technical issues, Copperfasten has developed the Mail Firewall Appliance (MFA) a proven antivirus, spam and content security tool designed to protect Government bodies, Academic institutions, and Commercial organizations from Internet-borne email viruses, while restricting the transmission of spam and other non-business related contents.

This white paper discusses how the MFA helps IT Managers achieve their objectives, in particular by encouraging users to self-administer their own email accounts, reducing the workload on IT Department resources, and improving the performance of network and communications systems.

Current Landscape

In many mid-sized companies, e-mail systems rely on a random assortment of security services with poorly centralized management and administration polices. Many of systems were implemented on modest budgets using shareware programs, bespoke applications, and rapidly out-dated security products.

This piecemeal approach has meant that many IT Managers are constantly involved in ‘fire-fighting’ activities — providing technical assistance during virus outbreaks, manually installing patches, scheduling upgrades, educating new recruits, deleting expired account passwords, resetting access privileges, and co-ordinating other time-consuming activities.

To compound this problem, the very nature of the Internet’s working model—ungoverned, open systems, lack of accountability—means that web-based email and messaging applications are vulnerable to individuals with malevolent intentions. Email systems that were once shielded by layers of security are now only as strong as the most recent virus definition update.

In the past twelve months, spam attacks and virus infections have compromised Fortune 100s causing lost productivity, inaccessible content, and system downtime. Working in this environment means that potential risks, security vulnerabilities, privacy issues, lack of policy enforcement, and the possibility of lawsuits all need to be monitored.

For ‘time-poor’ IT Managers, this places even more pressure on their team’s resources, budget management, and service level agreements.

When developing the Mail Firewall Appliance, Copperfasten designed the application so that it reduces this workload by shifting the administration of spam and email management from the IT Department to the User.

Case studies have shown that by empowering employees to manage their own whitelists, blacklists, and quarantines, the MFA solution enhances security, reduces outbreaks, and by minimizing technical assistance IT Managers can focus their efforts beyond fire-fighting and towards more strategic planning and company-wide initiatives.

IT Managers Set The Agenda

As email usage continues on its upward trajectory, the ability of systems to defend themselves from fraudulent, infected, and unsolicited emails continues to falter.

- Failure to meet security standards leave organizations open to financial penalties and possible imprisonment.
- Adult and pornographic emails may lead to lawsuits from employees.
- Email systems may be hijacked by hackers, causing legitimate servers to be blacklisted.

Facing Spam, Viruses and Threats

Spam, viruses, and other forms of malware are constant threats for every Internet enabled organization. These see no distinction between Fortune 100s, large governmental departments and small business owners. All are targets.

Since 2000, Copperfasten has installed secure email products for clients including Creative Labs, Royal Collage of Surgeons, Bank of Scotland Ireland, Glasgow College of Commerce, Irish Revenue, and TG4. All of these have faced similar challenges when combating these unwanted emails.

For example: prior to implementing the MFA, the IT Department of a large educational institute had to wrestle with levels of spam that frequently exceeded 70% of all email received. With a user-base close to 11,000 students, this affected operations on a number of levels.

- Management was sensitive to potential legal issues and threats to privacy, including phishing and hijacking of accounts.
- Student and Admin staff inboxes were regularly flooded. Valuable time was lost sorting authentic email from spam, while under-mining the role of email as a business tool.
- System Administrators came under intense pressure to block spam addresses, create blacklist, analyse reports, while forced to relegate critical tasks to a later date.

- Mail Servers creaked under the large amounts of spam backed up on their drives. Spam and valid emails could not be distinguished.

Setting Priorities

After a brief evaluation program, Copperfasten developed a strategic roadmap to move the institute from its current situation to a more secure and controlled working environment.

During this consultation process, the IT Dept defined MFA key goals as follows:

- Reduce the reliance on the IT Service helpdesk.
- Empower the User to self-manage their own email within the constraints of the Institute's email policy.
- Avoid disrupting ongoing email services during installation.
- Integrate with current email infrastructure, including web-mail solution.
- Easy-to-use setup, no client changes, and minimal user training.
- Fixed-price cost as opposed to expensive 'per seat' licenses.

Shifting the Balance to the User

After a successful trial period, the MFA was rolled-out to all users. Installation and configuration was completed in less than two hours.

The IT Department emailed the MFA Quick Start Guide to users, which guide provided clear instructions on how to manage their own email account and use the quarantine functionality.

The results were immediate.

- Spam levels were reduced by up to 98%.
- Spam-related calls to the Helpdesk plummeted.
- Users quickly learned to analyse their own blocked emails and to release, whitelist, and blacklist email by themselves.
- The role of the IT Department was recognised with continuous positive feedback from Senior Management, Admin functions, and students.


In its first year of operation, the MFA had already paid for itself.

With this in mind, let's take a brief look at some of its key features and see how the MFA contributes to an organisation's success in controlling unwarranted emails.

MFA — Self-Service Email Management

The Mail Firewall Appliance provides a secure messaging infrastructure with coordinated defences against viruses, worms, and spam.

One of the central tenants of the system is that it shifts personal email management from the IT Department to the User. In simple terms, this means that Users become the System Administrator for their own email.


Spam Quarantine Report

This email contains a list of all messages which have been quarantined as potential spam and/or virus infected messages before they reached your Inbox.

- Click on the [Deliver](#) link to have a message delivered to your inbox. Messages that contain viruses will be stripped of any attachments before being delivered to avoid any damage to your system.
- Click on the [Whitelist](#) link to have a message delivered to your inbox and whitelist the sender so that subsequent messages from that sender will no longer be quarantined.
- Click the [Delete](#) link to have the message deleted from your quarantine.
- To delete all of the messages, click the [Delete All Messages](#) link at the bottom of the Spam Quarantine Report.
- Messages will automatically be deleted from the quarantine after 5 day(s).

If you have questions regarding this report, please contact sean@copperfasten.com.

Spam Messages (11)

Score	From	Subject	Date	Actions
8.2	bounces@phoenixemail.com	IC Logic Device Benchmark Study	Thu 14/10 10:51	[Deliver] [Whitelist] [Delete]
9.7	Sandy@info-goals.com	Complimentary Mortgage Calculator!	Thu 14/10 21:38	[Deliver] [Whitelist] [Delete]
9.8	webmaster@grindvolumen.net	Generate Six Figures lake	Fri 15/10 4:01	[Deliver] [Whitelist] [Delete]
10.5	Martin@info-goals.com	Financial Dead End? Look into e...	Thu 14/10 22:24	[Deliver] [Whitelist] [Delete]
12.7	3356@mail.com	How one can become a terrorist?	Thu 14/10 15:21	[Deliver] [Whitelist] [Delete]
13	odjarvbenfo@yahoo.com	Why go to the doctor when you ca...	Thu 14/10 12:37	[Deliver] [Whitelist] [Delete]
15.1	Annette.Holley@myway.com	RE: account # 996409C	Thu 14/10 10:44	[Deliver] [Whitelist] [Delete]
24.1	qszwn45229@olivepress.com	Please Confirm everything. - Oct...	Thu 14/10 16:32	[Deliver] [Whitelist] [Delete]
25.6	Rebecca@Fastmail.ca	Unfaithful wives	Thu 14/10 20:46	[Deliver] [Whitelist] [Delete]
27.2	lpjit.yVGXbP2@oliveramberg.com	Approved: Your Mtg application -...	Thu 14/10 22:45	[Deliver] [Whitelist] [Delete]
27.3	HerbertEllisonjo@highstream.com	It's me, Sunshine LG0609565 fro...	Fri 15/10 1:31	[Deliver] [Whitelist] [Delete]

[\[Delete All Messages \]](#)

Deliver this report every: [day](#) | [weekday](#) | [Friday](#) | [month](#) | [never](#)

Include the following items in the report: [All quarantined items](#) | [New items since last report only](#)

To view your entire quarantine inbox or manage your preferences, [Click Here](#)

End user Quarantine Report

How It Works

The MFA removes viruses and spam, while eliminating incidences of false positives by using a multi-layered approach to identify, analyze, and separate valid from invalid incoming email prior to delivery to users.

Each email is controlled along the following lines:

- Verified by recipient address lookup.
- Scanned for viruses
- Passed through content filters. .
- Passed through whitelist and blacklist databases.
- Real time checks for emerging Spam email including RBL's, URLRBL's, Checksum tests and Repudiation systems.
- Analyzed based on keywords in headers and body text.
- Scanned using customized and Bayesian rule sets.
- Assigned a "score" whereupon it is quarantined, flagged as spam, or delivered if an authentic email.

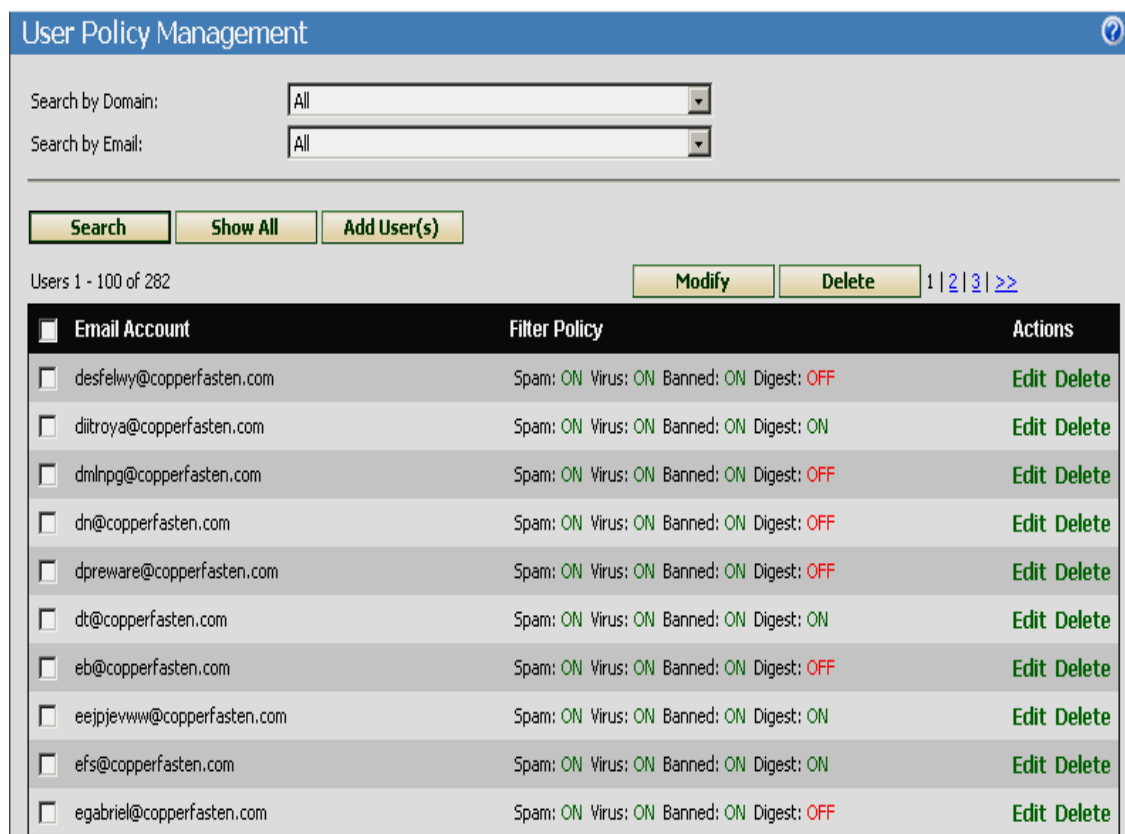
In this way, User can retrieve all quarantined email and ensure that no communications are ever lost.

User Management

The MFA enables Users to manage their own email control settings and ensure that email hygiene is maintained. Users have the ability to:

- View and release email blocked on their behalf
- Manage Blacklists and Whitelists
- Review Quarantine reports which are generated automatically on a daily or weekly basis
- Determine the frequency of Quarantine reports

Administrative Management



The screenshot shows the 'User Policy Management' interface. It includes search filters for 'Search by Domain' and 'Search by Email', both set to 'All'. Below the filters are buttons for 'Search', 'Show All', and 'Add User(s)'. A status bar indicates 'Users 1 - 100 of 282' and includes 'Modify' and 'Delete' buttons along with pagination controls (1 | 2 | 3 | >>).

<input type="checkbox"/>	Email Account	Filter Policy	Actions
<input type="checkbox"/>	desfelwy@copperfasten.com	Spam: ON Virus: ON Banned: ON Digest: OFF	Edit Delete
<input type="checkbox"/>	diltroya@copperfasten.com	Spam: ON Virus: ON Banned: ON Digest: ON	Edit Delete
<input type="checkbox"/>	dmlnpg@copperfasten.com	Spam: ON Virus: ON Banned: ON Digest: OFF	Edit Delete
<input type="checkbox"/>	dn@copperfasten.com	Spam: ON Virus: ON Banned: ON Digest: OFF	Edit Delete
<input type="checkbox"/>	dpreware@copperfasten.com	Spam: ON Virus: ON Banned: ON Digest: OFF	Edit Delete
<input type="checkbox"/>	dt@copperfasten.com	Spam: ON Virus: ON Banned: ON Digest: ON	Edit Delete
<input type="checkbox"/>	eb@copperfasten.com	Spam: ON Virus: ON Banned: ON Digest: OFF	Edit Delete
<input type="checkbox"/>	eejpjevww@copperfasten.com	Spam: ON Virus: ON Banned: ON Digest: ON	Edit Delete
<input type="checkbox"/>	efs@copperfasten.com	Spam: ON Virus: ON Banned: ON Digest: ON	Edit Delete
<input type="checkbox"/>	egabriel@copperfasten.com	Spam: ON Virus: ON Banned: ON Digest: OFF	Edit Delete

User Policy Management

System Administrators can also fine-tune the configuration settings by using features such as:

- Policy management- allowing for different rules to be implemented and defined at the domain or user level
- Active email monitoring - providing administrators with visibility of email as it is processed by the appliance.
- Quarantine Management – allowing administrators view and manage all quarantined email stored on the appliance.
- Generate ad-hoc and scheduled reports on all email activity.
- Implement Global Whitelists or Blacklists

Business and Technical Benefits

As illustrated above, the Mail Firewall Appliance offers management and customization tools for spam protection, personalized user controls management, and content filtering tools.

The MFA solution allows companies to realise significant business and technical benefits in the following areas:

- Attractive pricing model based on email processing power provided in the MFA in contrast to more expensive 'per seat license-based' models
- Integration with the existing infrastructure enhances the performance of mail servers and network communications
- Requires no changes to current business operations, email process or technical services
- Implementation of different policies at both the domain and user level allows rules to be implemented for individual user's requirements
- Provides users with an effective range of tools for managing incoming emails and defending against spam, virus and potentially malicious emails
- Staff can separate valid business messages from spam, thereby avoiding the loss of any legitimate correspondences
- Platform neutral architecture ensures that companies are not tied to a particular technology or operating system

Silver Bullets

Over the last five years, Copperfasten has worked with IT Managers from Europe, Asia and the USA.

Each of these identified similar risks, issues, and ‘pain points’ that effect their department’s operations and performance.

To explore this, we’ve compiled a list of ‘silver bullets’ that highlight these areas and illustrate how the MFA addresses these.

MFA Silver Bullets	
Spam Removal	Removes upwards of 98% of spam prior to delivery of mail to the existing mail servers. Quarantined mail is stored on the MFA.
Lack of Interruption	Removes spam prior to delivery to the mail server. Existing mail services are not affected by spam.
Enhanced Server Performance	Email servers require less processing power, back-ups are of legitimate email only, and mail throughput increases dramatically.
Phishing	Attempted Phishing scams are eliminated by identifying and removing suspect email
User Centric	Pushes the management of spam to the user so most administration related issues are removed from the IT Department.
Self-managed Quarantines	Users can send all suspected spam mail to a Quarantine facility thus removing spam from their inbox.
Report Generation	Quarantine reports are generated automatically on a daily or weekly basis allowing users to check and retrieve suspect mail if they require without having log on to web pages.

MFA Silver Bullets	
Legitimate Email Unaffected	Time required to process legitimate mail from spam is almost totally eliminated.
Accuracy	98% accuracy in identifying spam.
Low False Positives	0.03% “false positive” rate.
Frees up IT Dept	Allows IT Dept to pass ongoing spam management to the User that aligns with company policies.
User Whitelists & Blacklists	User can create whitelists and blacklists, search quarantines, and control reports.
Multiple Domains	Accommodate multiple domains and relay email from multiple domains to multiple email servers.
Supports Web Mail	The Copperfasten Appliance integrates seamlessly with Webmail solutions.
Remote Users	SSL integration allows remote users retrieve mail from their quarantine without compromising existing Webmail security policy.
Low Pricing Model	Pricing reflects the email processing power provided in the MFA, which provides a very economical solution for a large number of users in contrast to more expensive ‘license-based’ models.
No change required to current operations	Necessitates no changes to the current email process or service; in addition the removal of spam and much of the anti-virus processing from the mail servers greatly reduces the load on these servers.
Increases Performance	Implementation enhances the performance ability of the existing infrastructure.

MFA Silver Bullets

Quick Setup

Requires no client or user setup.

The Bottom Line

The Mail Firewall Appliance offers organizations wide cost saving opportunities.

By minimizing the downtime associated with viruses, spam, and other threats, the Mail Firewall Appliance removes the burden on your technical staff, simplifies security management and operation efforts, which ultimately reduces administrative and support costs, as well as the total cost of ownership.

As an “all in one” appliance-based solution, the initial outlay costs are significantly less than those required to implement its equivalent, including costs of servers, licensing of operating systems, virus and anti-spam software, notwithstanding product training and configuration.

The Mail Firewall Appliance design ensures ongoing management overheads are minimal with all updates being automated. Furthermore, its ability to remove viruses and spam reduces management overheads and affords organization-wide increases in productivity and efficacy.

The Mail Firewall Appliance helps reduce the overall cost of ownership through its tight integration, reporting tools, and user management features, giving companies the confidence to pursue their business goals, knowing that their network is secure.

Copperfasten
Galway Business Park
Galway,
Ireland

Tel: +353 91 540054

Fax: +353 91 540055

Email: info@copperfasten.com

Web: www.copperfasten.com