



CLEARSWIFT™

Simplifying content security

Simplifying content security

Ensuring best-practice email and web use

Clearswift White Paper

Email security: beyond the hype and hyperbole

A common-sense guide to a pressing problem



Table of contents

Introduction	3
Internet and email threats	4
Defense: take a layered approach	6
Choice of solutions	7
Addressing each threat with the right technology	10
Our credentials	15

Introduction

Every business depends on email and the Internet. But reading the press, it's tempting to believe that the risks sometimes outweigh the benefits. Viruses, phishing, spyware, spam, trojans, worms, pornography, hate mail and the like are presented, particularly by the press, as some sort of remorseless digital plague sent down from on high to damage businesses everywhere.

While it's true that the scale and scope of the threat has increased dramatically in recent times, much more heat than light has been generated by the hype. This guide takes a common sense approach to the email security challenge, aiming to avoid hyperbole by highlighting the practical, common sense steps that can be taken to beat the hackers.

It provides an overview of the most common threats as well as a discussion of how a layered approach to security is the best route to effective countermeasures. It examines the product and technology choices available to business - focusing on the benefits of software, managed services and appliances and where these solutions might be used together.

At Clearswift, our mission is to simplify email security. While we believe it's a critical issue for business decision makers, we also believe that the battle can be won through some straightforward steps. That's why we've produced this document. We hope you find it useful.

Jon Lee,
CEO, Clearswift

CLEARSWIFT
Simplifying content security

The porous enterprise: Internet and email threats

Today, no organization could consider switching off its email or web access. The Internet is digital DNA, enabling instant communication, collaboration and access to information. But one unforeseen result of email and web use is a radical change in the ratio of structured to unstructured content within your business.

Unstructured data exploding

Even a few years ago, the majority of your enterprise content existed as structured data, living within the controlled security of corporate applications and databases. Today, 80 percent of it is unstructured - held as emails, text documents, pdfs, presentations and spreadsheets.

This unstructured content - the vast bulk of your vital enterprise knowledge - circulates freely into, within and outside the company. Security, access control and regulatory compliance are limited while the ability to damage the enterprise is unlimited.

While the advantages of the Internet are clear, its ubiquity and reach means that today's business is more porous than ever before. The result is a new generation of threat that many companies are only now beginning to recognize - threats that can wreak havoc with corporate reputations and brands. How your organization treats the information that flows in, out and around it has become a critical success factor of business today. Where IT departments were once obsessive about network downtime, now they have to concentrate on defending the business against the content that travel across its networks.

Four big threats

The threats fall into the following four areas.

1. Corporate threats

These relate principally to loss of IP and confidential information. Imagine these scenarios:

- an employee - knowingly or not - emails the designs for your next generation product to a competitor
- your communications department mistakenly announces your acquisition of a rival ahead of time or, worse, your financial results.
- your HR director accidentally emails the file containing the salary of every manager in the company to the entire employee address list.

In all three cases, you can imagine the consequences if the media learns of these leaks and runs stories that affect customer and investor confidence.

2. Legal threats

Two broad categories of threat exist here:

- Offensive messages - mainly sexual harassment and racial abuse - are often spread by email. One in four UK companies has prosecuted employees in recent times for this misdemeanor.

With the liability now falling on company directors personally, rather than the company corporately, it's not good enough to have a policy against it - you need to prove you're actively fighting it.

- Compliance - companies are now more accountable for how information is stored, used and distributed - so it is imperative that data is managed and controlled correctly.

In the US, new legislation around the privacy of health and medical information enshrined in HIPAA rules, the need for financial and accounting compliance to Sarbanes-Oxley and new SEC controls related to share dealing scandals have raised the cost to business of non-compliance. In Europe, the Data Protection Act, Basel II, FSA regulations and EU94/96 are acting in the same fashion.

All of this legislation forces companies to provide clear audit trails to ensure that email from their employees complies with financial disclosure and privacy regulations. Emails that mislead customers or manipulate markets must be stopped before they do any damage and businesses now have a legal requirement to stop their employees from breaching regulations.

3. Social threats

This encompasses frivolous web surfing and email abuse (e.g. racial abuse and hate mail) as well as downloading of pornographic material - especially child pornography - which has no place in your company. You might be blocking the URLs of known websites, but are you also analyzing all downloads? Thousands of new sites are born every day, so no URL blocker alone can keep up. Some of your employees may also be stealing in your name by using your company broadband network to download illegal music, DVDs and software.

4. Digital threats

Every organization's IT infrastructure is in danger from malicious code and other harmful inbound content. The principal threats are:

- Spam is unsolicited commercial mass email, often advertising fraudulent schemes or products of dubious quality.
- Worms are a special type of virus that can propel themselves around the internet, without the need to infect a host program or document to act as a carrier.
- Trojans are programs that appear to be benign but perform some covert, malicious action. The term is often used in a broader sense to include any non-viral program that is used to allow backdoor entry into or remote control over a computer system.
- Spyware is any software that allows remote monitoring of actions and data on a system, without the user's consent or knowledge.
- Proxies are programs that perform some action (e.g. relaying mail or caching of web pages) on behalf of a remote user.
- Phishing attacks use 'spoofed' emails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc.

- Denial of service attacks are where the corporate email server or web site are overwhelmed by email volumes forcing them to be shut down temporarily.

Defense: take a layered approach

Defending your enterprise against these Internet-borne threats has become increasingly difficult:

- Email volumes are exploding
- New regulation makes poor controls illegal
- Emerging 'hybrid' threats combine the worst aspects of spam, viruses and spyware
- Standalone security solutions don't work together, compromising manageability and consistency
- Irresponsible vendor claims give a false sense of security

As the previous section showed, the threat doesn't centre just on malicious code, it's about regulatory compliance, corporate responsibility, loss of confidential data, harassment - anything that can go in an email and hurt your company.

Basic defenses: too little, too late

When malicious content first came to prominence, most enterprises implemented basic security: firewalls and virus filters.

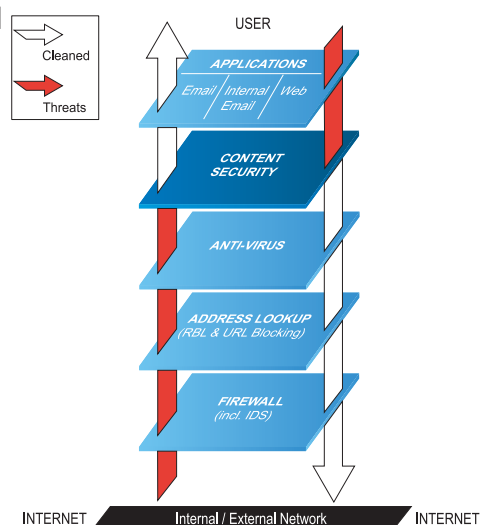
Unfortunately, these security staples don't address the majority of Internet-borne threats. Firewalls protect against network intrusion but are designed to allow email and web traffic through untouched. And virus filters catch most known viruses (those for which a profile has been created and distributed) while missing new viruses and those buried deep within apparently innocuous files.

And because even this basic layer of defence is deployed as an ad hoc collection of point solutions, the ability to enforce consistent policy is severely compromised.

The solution: simple layered defence

These threats should all be addressed with a single, simple comprehensive solution that fills every content security gap as part of a Layered Security approach.

As shown in the picture below, layered security supplements the basics of firewall, intrusion detection and anti-virus software (which most companies have in place) with critical Content Security functionality that closes the wide-open security gaps.



A choice of solutions

Dealing with the threats outlined above has become big business. According to industry analyst the Radicati Group, email security in 2005 will be an almost \$4 billion market serving an installed base of 756 million mailboxes.

More interesting than the sheer size of the market, however, is the range of choices now offered to enterprises. Companies of every size can now choose email security in three variants:

- as software,
- as a managed service or
- as an appliance.

Choice is undoubtedly a good thing for enterprises looking to squeeze more value out of hard pressed IT budgets. But what are the comparative advantages of the three alternatives. And are there circumstances when they can be used in tandem? Let's look at the three choices, starting with managed services.

Managed services: the advantages

There are some clear benefits of employing a managed service to handle your email security challenges:

- **No hardware** - managed services require no additional hardware, and can be typically implemented in a few minutes by simply redirecting message traffic to the service provider's email servers.
- **No updating** - as new threats emerge, it is the service provider's responsibility to update virus or spam signatures - this is a key benefit if you are a smaller company with limited IT resources.
- **Predictable costs** - most managed email services are billed on a per user, monthly basis allowing your business to treat them as a revenue (or P&L) item, not a capital (or balance sheet) item. This convenient pricing structure is attractive especially for smaller companies compared with the sometimes unpredictable cost of implementing and managing in-house security solutions.
- **Contract flexibility** - related to price predictability is the issue of contract flexibility where, if you are not satisfied with the service or there are advantages in switching to an in-house solution, the service contract can be terminated in short order.
- **Infrastructure/staff savings** - a comprehensive service obviates - or at least reduces - the need for in house infrastructure and professional technical support.
- **Disaster recovery on tap** - if an internal email server fails, a managed service can often act as a disaster recovery service reducing the need to invest in back-up internal systems.

Managed services: the downside

The concomitant downsides to deploying a managed service are:

- Outsourcing strategic assets - many companies are wary of having a third party scan their email traffic, particularly when much of it is of strategic importance or confidential.
- Expense past a tipping point - over time as email - legitimate and spam - volumes grow, per user monthly fees can become expensive, especially for larger organizations.
- Limited flexibility long term - most managed services offer basic security functionality (anti-virus and/or anti spam) and for inbound traffic only. Companies that wish more sophisticated deployments - covering SMTP, web and internal email traffic combined with implementation of flexible email policies - may find in house security solutions to be a better route.

The MIMEsweeper SMTP Appliance

Easier to install - a single sheet of paper comes in the box. It leads you through seven steps that take under an hour.

Easier to manage - the simplest, most intuitive management console on the market, with the richest reporting to boot.

Easier to release messages - with transparent, user-driven management of inbound and outbound quarantines.

Easier to maintain - auto-updates come every fifteen minutes (or every hour if you prefer). New rules are set in minutes.

Easier to support - Clearswift's global support is everywhere.

Easier to upgrade - with new revisions downloaded automatically and auto-rollback to revert to any state you like.

Easier to buy - thanks to the largest network of dealers in the security business.

Easier to justify - best-of-breed anti-spam, anti-virus, anti-spyware and content filtering on a single, plug 'n' play, Linux appliance made by Dell.

Appliances: the benefits

The advantages of appliances are:

- **Deployability** - appliances are easy to deploy, since they include pre-integrated hardware and software components. The boxes themselves are of standard sizes and have been designed for plug 'n' play installation.
- **Reliability and robustness** - appliances are generally very reliable and can handle large volumes of message traffic. Most run on a specialized, hardened version of Linux or UNIX that is designed for reliability and performance and designed to eliminate exploits. Most have a redundant hardware to protect against failure. In Clearswift's case, our secure Linux kernel was designed by experts who have years of experience delivering security solutions to the most demanding military customers.
- **Scalability** - most appliances can be easily scaled by adding additional boxes to an existing deployment.
- **Upgradability** - most appliances provide online, automatic updating for anti-virus and anti-spam capabilities as well as software versions.
- **Manageability** - the promise of appliances is that they are the easiest of our three security approaches to manage and maintain.

Appliances: the downside

Appliance weaknesses fall under one major heading: limited functionality.

Many vendors have traded functionality for ease of use and manageability. While most appliances include best-of-breed anti-virus and anti-spam functionality (although some only offer one of these), few, if any, can handle deep content filtering as well.

In addition, most appliances are deployed only at the network perimeter because they cannot filter internal email traffic passed between email servers. Filtering of internal email traffic is an important part of the regulatory compliance process for many businesses. Bi-directional content filtering - for both inbound and outbound email traffic - is a key requirement for most business, although few appliances offer this feature. After all, a leak of confidential data can hurt a company just as much as a virus can.

In addition, most appliances are dumb and are unable to offer enterprises the ability to apply rules by domain, geography, department, individual, file type and so on. Granular policy management that allow you to set policy by company, region, department or individual and by dozens of parameters such as sender, file type, file size and content will be key as organizations become larger or more complex.

Software solutions

The email security industry was founded on software solutions to the email security problem and it's no surprise that the most sophisticated email security deployments tend today to be based on established software solutions. The key strength of a software solution is its ability to be customized for specific requirements at a cost that an enterprise can afford.

The underlying choice for your business as it relates to software is how much they themselves want to get their hands dirty in managing the solution. The more they want to be involved, the more likely that software-only implementations (as opposed to appliances or managed services) are likely to be attractive.

One recent Clearswift customer illustrates this choice. It wanted a comprehensive email security solution - handling web mail as well as internal and external email - to cover the 36 countries in which it operated. It also wanted to set clear policies on profanity and other illegal content in all the languages in use across these geographies.

Key to the choice of a software solution for this enterprise was the issue of policy. This company was clear what was and what was not acceptable in use of email and the web. And it wanted to be able to control use of email and the web at a very granular level.

The goal was to find the balance between freedom and security that was most relevant for each discrete operational unit. And the company realized that a single, monolithic policy was unlikely to prove effective for all individuals at all levels in all departments in all regions. They wanted a policy that could combine the corporate email principles set at the center while reflecting the way each subsidiary and department did business. They could have accomplished this using appliances or a managed service, but wanted the granularity of control and absolute flexibility they knew was offered by software.

A mix of solutions

Most smaller companies - particularly those with limited in house IT resources - should probably opt for either a managed service or an appliance to handle email security challenges. Many larger companies, however, will use appliances or a managed service as part of a multi-layered defense against spam and viruses. In this type of deployment, appliances act as a first layer of defence at the network perimeter, while subsequent layers of email security software are deployed within the messaging infrastructure.

nPower mixes software and appliances

nPower was the first customer for Clearswift's new appliance, buying four of them to filter email for more than 13,500 corporate and retail users at the organisational gateway, to eradicate spam and scan for viruses, while using their existing MIMESweeper software solution for its more detailed content filtering and compliance needs. Since spam and other non-business mail accounted for over 50 per cent of the company's email, by eradicating spam and other malware at the gateway, they could reduce the numbers (and infrastructure cost) of email servers required to handle legitimate mail.

As Andy Broome, nPower's Infrastructure Manager says: "nPower has used Clearswift's software for some time now and we know it just works - they have a well-deserved reputation as the leader in content security. By taking a layered approach using Clearswift's MIMESweeper SMTP Appliances to filter out spam and viruses at the gateway, and MIMESweeper for SMTP 5.0 inside the gateway, it means we only perform deep content analysis on legitimate business email thus protecting the company from both inbound and outbound email threats."

A comprehensive solution

Whichever choice you make for your company, a comprehensive content security solution meets these criteria:

- **Easy to use** - with simple deployment, management and reporting that recognizes the importance of 'the human factor' in enterprise security.
- **Covers every gateway** - instead of a patchwork defense
- **Filters both email and web traffic** - simple solutions only cover email and basic URL filtering for web traffic.
- **Covers all directions** - including inbound, outbound and internal mail (many only filter incoming traffic).
- **Offers central, granular policy management** - instead of basic, local policy configuration.
- **Delivers enterprise-class performance** - for the highest volumes and most complex traffic.

Addressing each threat with the right technology

As this document has shown, the threats carried by email can hurt your company in many ways:

- **Downtime** - Viruses, trojans and malicious code can cause major crashes in mission-critical systems. The longer the downtime, the more expensive and damaging the consequence.
- **Lost productivity** - Spam-clogged mailboxes and employee email misuse waste thousands of hours of employee and IT staff time. Stop it and you can get back to work.
- **IT resource drain** - Bandwidth and storage cost money. Don't waste it on email that is malicious, uninvited or frivolous.
- **Legal liability** - The circulation of offensive content or copyrighted material leaves your company open to litigation and reputation damage.
- **Competitive disadvantage** - The loss of confidential information can seriously affect your ability to compete - and cause major corporate embarrassment.
- **Compliance breaches** - New regulations make your company accountable for how data is stored, used and distributed. Manage it or you're in breach.

To avoid these problems, email security comprises the following elements:

- Anti-virus
- Anti-spam
- Anti-phishing
- Anti-spyware
- DoS
- Content filtering

Let's look briefly at each of these in turn.

1. Anti-virus

Anti-virus solutions are one of the key tools in the defense against viruses. However, simply relying on an anti-virus tool alone does not provide organizations with complete protection against complex and hidden content threats.

Virus attacks via email are on the increase, but anti-virus solutions are only as good as their last update. And, according to the UK Department of Trade and Industry (DTI), only 59% of organizations automatically update their systems when a new virus signature is identified.

Addressing the 'Zero-Day' window

A key issue for anyone implementing an anti-virus solution must be to mitigate the 'Zero-Day' window - the vulnerability that exists before anti-virus companies issue patches and updates to deal with new threats. In the time it takes to create and deliver the patches used to meet the threat from new worms and Trojan horses, a serious amount of damage can be done.

Administrators need new ways to defend against rogue files. The answer lies in 'best-in-class' policy-based content analysis that can spot and quarantine any questionable content before it has a chance to compromise corporate networks.

2. Anti-spam

Spam causes a huge drain on system resources, employee productivity and business costs. In addition, spammers are now using viruses to spread emails and virus writers are using spam to spread viruses. With the emergence of "spam zombies", spammers are now using Trojans with embedded email engines to relay spam emails through infected computers.

And managing spam places an enormous burden on IT departments. IT staff waste time purely on checking whether blocked emails are spam, or releasing valid business emails which have been incorrectly categorized as spam. Organizations need to be able to pass on some of the burden of reviewing potential spam to end-users, which is also a key part of educating companies on how to deal with spam.

Any successful spam solution should offer the following features:

- **Bayesian Analysis** - a statistical inference in which probabilities are interpreted not as frequencies but as degrees of belief.
- **Heuristic Scanning** - basically analysis guided by rules. From the same Greek root as 'Eureka' which means 'I find'.
- **Auto-whitelisting** - the appliance watches your traffic, determines who are the good guys and lets them send you mail.
- **Real-time blacklisting** - this depends on accessing lists in real-time from the industry bodies that identify dangerous websites
- **Sender Policy Framework and Sender ID** - Two industry initiatives that put the burden of authenticity on the sender (spammers hate that).

3. Anti-phishing

Phishing is the act of sending an email to a user falsely claiming to be a legitimate enterprise in an attempt to scam the user into surrendering private information that can be used for identity theft. The email directs the user to visit a bogus web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has.

Anyone with an email address is at risk of being phished. Phishers send out literally millions of these scam emails in the hopes that even a few recipients will act on them and provide their personal and financial information.

4 Anti-spyware

Spyware is a broad category of malicious software intended to intercept or take partial control of a computer's operation without the user's consent. Spyware differs from viruses and worms in that it does not usually self-replicate. Typical tactics include delivery of unsolicited pop-up advertisements; theft of personal information (including financial information such as credit card details); monitoring of web-browsing activity for marketing purposes; or routing of HTTP requests to advertising sites.

5. Denial of Service (DoS) protection

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Usually it involves attempts to "flood" a network, preventing legitimate network traffic or an effort to disrupt connections between two machines, thereby preventing access to a service.

DoS attacks can disable your computer or your network. Depending on the nature of your enterprise, this can effectively disable your organization. DoS attacks have become a serious problem in recent times. Until recently, DoS attacks were essentially an amateur pastime - still serious, but uncoordinated and frequently unsophisticated. The main motivations were either 'because it's there' or simple-minded cyber-vandalism.

But there is now growing evidence that more and more sites are under DoS attack from organized crime. Attacks on gaming sites in the UK have led to stories that the 'cost' of avoiding a DoS attack was about \$50,000. It is certainly true that there are increasing numbers of 'hackers for hire' offering to hit sites for certain amounts of time. In addition, the number of computer zombies - compromised computers used for DOS attacks - is mounting.

6. Content filtering

Content filtering stops the things that aren't spam or viruses but can be even more dangerous, like confidential customer data being mailed to a competitor or illegal, immoral or just plain unpleasant material coming in or out.

Customers looking for best-in-breed content filtering should demand that their content engine has:

- **Breadth** - to stop spam, viruses, trojans, confidential leaks, hatemail, inappropriate content and malicious code - all from a single management console.
- **Depth** - content engines should have the ability to 'explode' all email content to detect deeply embedded problems and content. Many simple filters may capture common malware data types, but they'll miss the not-so-common, particularly when they're hidden in zipped up attachments.
- **Power** - the performance to handle millions of emails with ease.
- **Granularity** - Content security is all about creating and enforcing policy and the best results come from the most granular policy management capability. That also requires policy templates and wizards to make it easy to design, deploy and update.
- **Control** - Look for a solution that requires minimal management time and resource. You should be able to configure and manage all email gateways from a central console, for instance, as well as receive automatic updates and patches.

About Clearswift

Make it simple, but never compromise.

Clearswift's award-winning MIMESweeper™ technology is the world's leading content filtering and policy management engine.

MIMESweeper solutions help companies define their security policies, then easily enforce them, ensuring all traffic complies with internal policy and external regulations.

Email security, simplified

The MIMESweeper portfolio of email security products includes comprehensive solutions for inbound, outbound and internal email.

The solutions combine anti-virus and anti-spam with the award-winning MIMESweeper content filtering engine. Optional archiving and TLS encryption complete the unified security solution.

All MIMESweeper email solutions simplify the deployment, management and maintenance of the entire content security activity, with intuitive management and reporting consoles, automatic updates and personal message management.

Solutions for government, defense and financial sectors.

Clearswift provides a range of security solutions, accredited to EAL4 standard, for highly sensitive government, defense and financial institutions. Products, such as Bastion™ and DeepSecure™, address the security needs of the world's most mission-critical messaging applications for clients such as the UK Ministry of Defence and NATO.

Web security

MIMESweeper for Web does for web traffic what the email products do for SMTP: analyze every bit of traffic and remove every kind of content threat.

For the first time, one solution can defend against web-borne viruses, loss of confidential information, prohibited browsing, illegal downloads & uploads. The web solution combines the world-class content analysis technology of MIMESweeper with a powerful add-on URL Filter.

Three different deployment platforms.

Clearswift is the only vendor to offer complete content security solutions in all three delivery platforms: as software, on an appliance or as a managed service:

- The MIMESweeper software family includes comprehensive content security solutions for corporate email (inbound and outbound), internal email, web traffic and webmail.
- MIMESweeper appliances deliver complete content security in a plug & play appliance for rapid deployment and easy management.

- MIMESweeper managed services deliver full content security as hosted services, to stop email- and web-borne threats before they even reach corporate servers.

The Clearswift difference.

In a world of 'me too' security products, Clearswift presents a highly differentiated proposition to enterprises:

Simplicity without compromise.

Easy to deploy, manage and maintain with a clear, intuitive management interface; automatic, 'zero-touch' updates; powerful reporting and common-sense policy management.

Enterprise-class content security.

Comprehensive content security designed for the resilience, performance and manageability demands of large enterprises.

Granular policy management.

Built around the most powerful policy management engine on the market, applying rules enterprise-wide or by department, region or individual.

Super-intuitive management interface.

The most fully-featured, user-friendly interface on the market, with clear, simple, browser-based tools for provisioning, updating, monitoring and graphical reporting.

Deepest content inspection.

Unbundling and analyzing files deeply embedded within other files. We recognize more file types including compressed and password-protected files, so no message eludes our analysis.

Covering all traffic in all directions.

Covering all web and email traffic from a single platform, whether it's inbound, outbound or internal.

Three delivery platforms for customer choice - today and tomorrow.

The only vendor to offer full content security as software, on an appliance or as a managed service.

A trusted partner.

Clearswift pioneered the content security market over 10 years ago and continues to lead it today. Our products are licensed to over 15,000 businesses, covering over 20 million users all over the world. Because we handle more traffic in a greater variety of environments, we spot new trends and emerging threats faster.

Our ThreatLab™ analyzes email and web traffic 24x7x365 on a global basis, identifying and responding to new threats as they emerge. And our dedicated R&D department continues to keep the MIMESweeper family ahead of the market in functionality, performance and manageability.

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

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