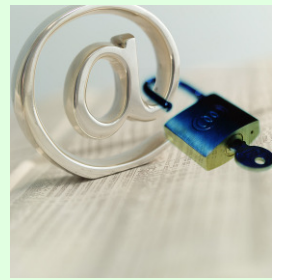


Intelligent Email Management Solutions



Using e-Solutions comprehensive and innovative approach to email management, businesses can improve operational efficiency, comply with regulatory requirements, ensure that valuable data and information is kept secure and confidential, and provide improved customer service and security.

Email is a pervasive method of communicating that is cheap, efficient and convenient. However, the sending of unencrypted emails over the internet represents a major threat to security and confidentiality. It's the electronic equivalent of sending a postcard – potentially, anybody can read it.

We offer fast and effective solutions to the risks associated with using email covering:

- ◆ Automated archiving and subsequent analysis and retrieval
- ◆ Email encryption
- ◆ Content examination of emails and attachments
- ◆ Virus and Spam curtailment
- ◆ Electronic invoicing

Our solutions are specifically designed for:

- ◆ Banks and building societies
- ◆ Insurance companies
- ◆ Telecommunications providers
- ◆ Accountants
- ◆ Lawyers
- ◆ Health industry

Email – The fastest growing communication medium

Over the past decade email has fundamentally changed the way most businesses operate and has even overtaken

the telephone as the preferred means of business communication.

Email is quick, simple, ubiquitous and appears to be free; but the volume and free-format nature of email raises numerous problems from the risk of receiving viruses and inundation with spam to the difficulty of finding stored emails should it prove necessary while ensuring that anything confidential is not accidentally disclosed.

As a result companies need to develop and implement a strategy for email to ensure that they are addressing the various risks. For some companies this is just a matter of good practice but for many others it is a requirement, albeit usually not explicit, of various pieces of UK and overseas legislation.

e-Solutions has used its experience, gained primarily within the financial services industry, to identify best-of-breed technology solutions to the various problems associated with email and have integrated these to provide a comprehensive solution. We recognise that different companies will have differing needs and we can tailor our solution to ensure that as your needs evolve it is easy to change the components.

Our email system is fine – Why should I be concerned?

Installing an email system is relatively simple. The challenges come later when you suddenly realise that you are dependent upon it but haven't placed the necessary infrastructure to protect your business should things go wrong.

Most companies appreciate the need to check email for viruses, and with the rapid growth in unsolicited emails (spam) there is an ever growing need for spam filtering. Such problems and solutions are obvious to the end user, but how do you:

- ◆ Ensure that you are not breaching compliance requirements?
- ◆ Monitor the acceptable use policy agreed with your staff?
- ◆ Ensure that any confidential information sent to customers and suppliers is suitably protected in transit from prying eyes?
- ◆ Find copies of email communications months or even years after they were sent when required to do so for legal reasons?

Can you afford not to protect yourself and your business? In the UK fines relating to the inability to find emails have been up to £450,000 and in the US these have exceeded \$10m.

Archiving and analysing email

Although it is good business practice to backup email systems, and most companies have processes in place, this is not the same as archiving email.

Backup files are generally designed to restore lost data after a major failure and as such are difficult to search for individual items. Depending on how the backup cycle operates it might also be possible for emails to be deleted by a user and that deleted email may not to be retrievable afterwards (which could breach many regulations).

Archiving is different in that it operates separately to the standard backup. Copies of email are taken and held independently from your current email server.



Detailed Analysis

Once email has been captured in an archive it is possible to undertake robust analysis to cover:

- ◆ Policy violation reporting
- ◆ Abuse management - suspicious or inappropriate email being sent
- ◆ Personal usage by staff against agreed guidelines
- ◆ Forensic investigation - permitting access by managers without recourse to IT
- ◆ Compliance - providing an audit trail for FSA, Sarbanes-Oxley, Data Protection and other legislation
- ◆ Volume analysis - understanding where emails are being sent to and received from

Flexible searching

All message content and attachments are captured for record retention or investigative need. An advanced search facility permits full body text and attachments from the email archive to be examined.

Searching can use wildcard, verb tense, fuzzy or proximity search technologies allowing in-depth evidentiary discovery on corporate email data. A full reporting package shows email usage and permits easy drill down for more detailed information.

Cost Savings

In an increasingly litigious age, it is essential that email can be searched quickly and effectively for evidence. Many companies when faced with court requests for emails have either been forced to spend very significant sums in searching back-up files, or have been fined for the inability to retrieve emails.

Supporting HR Issues

The flexible searching capability can provide HR managers with a simple means to address harassment or other sensitive situations without needing specific access to each users' email account.

A comprehensive email management solution

e-Solutions have integrated product solutions to provide an end-to-end service covering the challenges associated with email management.

At the heart of our solution is comprehensive email encryption and routing software developed by Aliroo who are experts in data security. Their system has been deployed worldwide and is used by banks, hospitals, health professionals and others who need to ensure that the messages they send are not disclosed to third parties.



We appreciate that all businesses are different and therefore our solution is modular enabling you to licence only those features that you actually need.

Based upon preset criteria it is possible to:

- ◆ Archive emails
- ◆ Make automated decisions based upon the content of the email on how it should be handled
- ◆ Check for viruses and spam
- ◆ Encrypt the message and any attachment



Identity Verification

e-Solutions, in partnership with Equifax, can provide an identity verification service which permits an individual's

identity to be confirmed at a distance and in real time, without the inconvenience of physically producing a passport, a driving licence etc. Once identity has been confirmed, then a digital certificate can be issued, which can be used to digitally sign emails and documents and for email encryption.



The certificates are tScheme accredited – Equifax is the first and only online provider in the UK of authenticated certificates.

Ensuring confidentiality of email

When a user sends an email it appears to go directly from the sender to the recipient. In reality it transfers via a number of different servers which due to the way the Internet works

can be anywhere. Therefore, whenever an email is sent, it is as if you have sent the message on a postcard. Anyone with the tools and desire could theoretically intercept and read or alter it. This means that standard email is an inappropriate medium to use when personal or confidential data needs to be communicated.

Compliance

The principles of protecting information are enshrined in Sarbanes-Oxley, the Data Protection Act, Basle II and other legislation covering the UK, the USA and Europe.

It is incumbent on organisations to take suitable care to protect confidential data and this means that emails should be encrypted between the parties.

Our encryption solution permits end-to-end encryption of an email and its attachments. The decision on whether to encrypt can be automated based on a number of criteria, such as recipient email address or message content so that staff need not be concerned and cannot accidentally forget to send a message encrypted.

Encrypted email can be sent to ANY email address and can use a number of different encryption methodologies.

At its simplest all a recipient needs to do is register his/her email address and a password and the encrypted message can be sent to them. There is no need for the recipient to download any software. They merely double-click on the message attachment and a box will appear asking for their password, and if correctly entered the message is decrypted.

An automated email is sent to first-time recipients advising them that an encrypted message awaits them and encouraging them to register.

There are further options for using digital certificates (PKI) or PGP keys for encrypting messages should a recipient already have such tools.

How does it work?

The exact configuration for each client is different and depends upon:

- ◆ The number of users
- ◆ The amount of email traffic expected
- ◆ Whether archiving is required
- ◆ Whether the client wants to have their own SES (Secure Email Service) centre or use ours for processing encrypted messages

For example, the typical configuration, shown right, would permit Company 1 to:

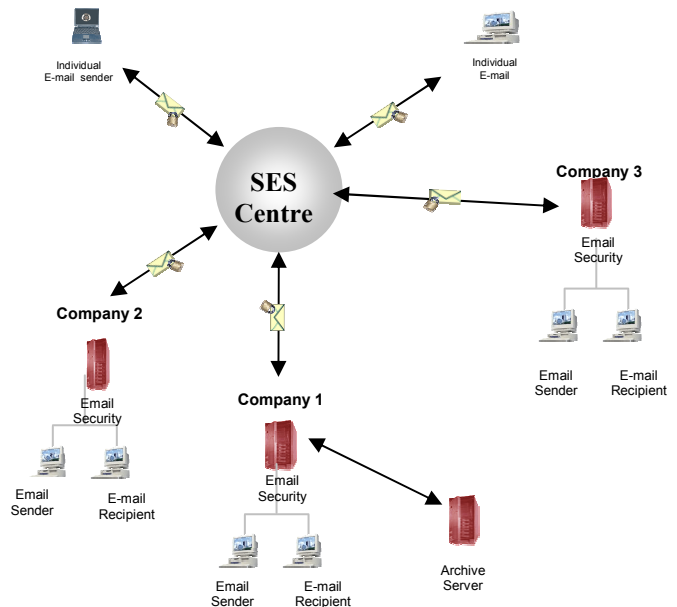
- ◆ Archive all mail sent and received to their own internal archive server.
- ◆ Examine all outbound mail and encrypt automatically based upon pre-agreed rules
- ◆ Receive encrypted emails from clients, customers and suppliers
- ◆ Examine all inbound emails and route as required to improve operational effectiveness

Improving operational effectiveness

The efficient use of email as a business tool can enable operations to be more effective from both cost and customer service perspectives.

Our solutions can permit:

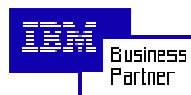
- ◆ Email to be deployed in situations where confidentiality concerns would have prevented safe use
- ◆ Confirmed delivery of email. There is sometimes some doubt whether an email has actually been received. It is now possible to use a certified return receipt. When decrypting the email a message is sent back to the user confirming that the recipient has not only received but has opened the email.
- ◆ Message Routing. Automated reading of emails so that they can be forwarded to the correct customer service team.



- ◆ Secure Response. There are occasions when you will want to have a secure response from a customer but don't want them to inconvenience them in any way. Secure Response permits a customer to reply to you directly with an encrypted message.

In-house or outsourced technical options

The recommended technical configuration will depend upon a customer's specific needs. Our email management solutions operate on standard servers using Microsoft Windows 2003 Server. Archiving and encryption key management require Microsoft SQL Server 2000.



We are able to offer a fully managed service provided by our partner IBM. As a result we can implement quickly and with a minimum impact on your current operations to provide you with the service that your business and customers require.

Further information Please contact us for more detailed information on our range of email management solutions and how they can be tailored to meet your specific business requirements.

e-Solutions and Services UK Ltd
Upper Linbrook Farm
Needwood
Burton-upon-Trent
Staffs DE13 9PF

Phone: 0870 855 0631
Fax: 0870 855 0639
Email: enquiries@e-solutions.uk.com