

Keep your email secrets secret with XM SecureMail

XM Technologies provides companies with messaging solutions to protect the efficiency, security, manageability and usability of their email systems. Our **SecureMail** encryption solution provides your firm with an open, IETF approved, automated secure email which protects your electronic communication from unwanted eyes.

Communication between your employees and your suppliers, customers and shareholders is the lifeblood of your firm. What if this confidential information leaked out?

Today, over 1/3rd (and increasing rapidly) of business documents are sent through the internet. Literally, tens of millions of documents travel through cyberspace daily and email has rapidly become the number one form of corporate communication. What most companies do not realize is that only the correspondence within a company network is secure because of its firewall – all communication with outside parties is completely open to eavesdropping on the Internet, *which is perfectly legal*.

Email is now the leading form of corporate communication – shouldn't it be fully secured?



While the Internet has become an incredibly efficient tool for communication, is open to sniffing. As a document travels from the sender to the receiver, there are many different paths it can take, depending on bandwidth and the amount of traffic at the time of sending. Your confidential communication and even corporate secrets are fair game for anyone who happens to be monitoring your network. It is just like sending a confidential letter via the post office – without the envelope.



Options - Client vs. Server-based Systems

Internal to a company's network, there are rarely any security problems as Domino, or Exchange Mail are typically protected by firewalls and are fairly secure on their own. However, when a firm connects with its remote stakeholders the need for additional security measures is required.

Client-Based

Client based systems such as Pretty Good Privacy (PGP) or S/MIME may require additional software to be purchased and installed on every user's desk and encryption keys must be shared over the Internet. Large scale deployment is extremely difficult. The number of keys required grows rapidly as each user (both internally and external) requires keys in the directory. Keys can get corrupted or lost – leading to administrative headaches. Extra training is generally required, which can be a nightmare for the IT support staff and often costs more than the application itself. Users are forced to be proactive in verifying the encryption process, thereby jeopardizing the integrity of the whole process. Finally your existing anti-virus solution generally will not work with encrypted messages encrypted.



Server-Based

A second method of setting up secure email with your suppliers, customers and shareholders is a server-to-server type connection. With a server-based encryption system, every client running off of that server uses the system automatically. There is no need to install software on each individual workstation. There is only one corporate encryption code to use as opposed to individual ones for each client. As well, there is no manual step involved. Each email is automatically encrypted in transit using a 128 Bit 3DES encryption key. When it is received at the other end it is automatically decrypted. This ensures all e-mails in both directions are protected.



The XM Solution

XM SecureMail minimizes the costs and hassles of setting up your secure email network. XM SecureMail seamlessly encrypts outgoing email using the 3DES algorithm. At the receiving side it is unencrypted automatically and scanned for viruses using your existing anti-virus solution. Therefore your email is more secure with little impact on your users and existing infrastructure. We help every step along the way getting your customers and suppliers up and running.

Benefits

Easy to Use

- ? No End User impact
- ? Automated
- ? The email is encrypted seamlessly in the background.
- ? Nothing is installed on the users desktop which means no training
- ? Always on

Easy to Implement

- ? Minimal IT support and maintenance.
- ? Corporate implementation package ensures easy and fast company-wide changeover.
- ? Outgoing and incoming email can be routed through company SMTP servers or the XM SecureMail relay
- ? No new ports to open on your firewalls – it runs on port 25
- ? Use your existing email infrastructure
- ? We free your administrators from doing the administrative hassle of contacting other companies.

Open

Your company does not lock itself into a proprietary system that is costly and often difficult to maintain and upgrade – XM complies with IETF RFC 2487

Minimal ongoing costs

XM SecureMail provides more value for less money - Other solutions require expensive yearly licensing fees

Technical Highlights

- ? XM uses TLS(SSLv3) 128 Bit 3DES encryption, like banks use
- ? IETF RFC 2458 compliance
- ? Can process more than 1 million messages per day per server. (10-50K average users)
- ? Only 5% additional network overhead
- ? Unlimited email size
- ? Remote Administration available if required
- ? Works with all corporate email systems such as MS Exchange, Lotus Domino and Unix based systems.
- ? Allows for Virus Scanning
- ? Can scan for UCE (Unsolicited Commercial Email)

Requirements

Domino-Server, Version 5.x or higher
Microsoft Exchange 5.5 or 2000
Sendmail, Postfix, Qmail, Exim

Operating Systems

AIX 4.3.1 or higher
Linux
Windows 2000 Server
Windows NT 4.0
AS/400, V4 R4 or higher
SUN Solaris 7 or higher
OS/390 V2 R6

Hardware

RAM: 64 MB in addition to e-mail system
CPU %5-8 increase

Company background

XM provides open IETF approved, automated secure email messaging solutions for leading North American companies to protect the efficiency, security, manageability and usability of their email systems.

Through the XM SecureMail encryption solution we help firms ensure that emails are secure via standard SSL encryption. The XM MailFilter solution pairs server-based filtering and around-the-clock support and analysis to prevent email-borne threats.

XM is based in Toronto, Canada and has over 12 years combined IT experience with companies such as Bank of Montreal, BCG, Celestica, IBM, accenture and many others.



Many solutions look great on paper, ours works.

Contact us at:

XM Technologies, Inc
7035 Fir Tree Drive, Unit 20
Mississauga, Ontario L5S 1V6

Tel: 905-676-8699
Fax: 905-676-8610

Email: darryl@XMinc.com