Email Privacy 101

A Brief Guide

Trend Micro, Incorporated

A brief guide to adding encryption as an extra layer of security to protect your company in today's high risk email environment.

A Trend Micro White Paper I **February 2009**

Email Privacy 101
A Brief Guide

A brief guide to adding encryption as an extra layer of security to protect your company in today's high risk email environment.

- **Why does an organization like yours need email encryption?**
- **When do you need email encryption?**
- **Where does electronic theft occur?**
- **How do you add the extra layer of email security necessary in today's environment?**
- **What makes Trend Micro Email Encryption different?**

WHY DOES AN ORGANIZATION LIKE YOURS NEED EMAIL ENCRYPTION?

You wouldn't think of running an IT network without basic security measures such as firewalls, content filters and anti-virus programs, yet every day security holes are created in your network when unprotected data travels in and out of your company via email.

Email is the primary method of business communication. More than 60 billion email messages traverse the globe via the Internet each day.

Curiously, we tend to believe that email is somehow inherently secure and that someone somewhere is making sure each message stays secure as it goes from one public server to another. The opposite is true. Email is inherently insecure.

There is an increasing amount of corporate governance legislation being passed requiring the collection and storage of commercially sensitive data in order to satisfy reporting obligations. Governments have introduced this legislation to protect confidential information precisely because email is so insecure.

We're not suggesting you stop using email. What we are suggesting is that you add the missing layer of email encryption to your existing security measures.

No matter what security you have in place, generally no one in your organization would even know that email security breaches had occurred until it was too late to do anything about them. Yet once an email message and its attachments are encrypted it doesn't matter if it falls into the wrong hands – no one but the intended recipient can open it.

Standard security tools like firewalls and anti-virus programs remain necessary, but they are not enough to protect private and sensitive data as it travels over the Internet in today's high-risk climate. The people paying most attention to your security gaps are those who want to exploit them. The only way to beat them is to pay more attention yourself. Email encryption does that for you.

10 OF THE MOST VULNERABLE DOCUMENTS

1. Financial spreadsheets
2. Sales pipelines
3. Customer details
4. Competitive analyses
5. Marketing plans
6. Development roadmaps
7. Patents
8. Contracts
9. Board meeting minutes
10. Employee details

WHEN DO YOU NEED EMAIL ENCRYPTION?

Most vulnerable data is sent between company employees and between employees and suppliers and customers. This includes anything that is confidential and sensitive (see box) which, if it fell into the wrong hands, could be used in ways that compromise your financial position and future.

Any email that contains vulnerable company data – either in the message or in the attachment/s – should be encrypted.

> “Unencrypted email is the one gap in your security infrastructure that electronic thieves really care about.”

WHERE DOES ELECTRONIC THEFT OCCUR?

Outside

Although your employees might be sitting comfortably in their offices, they are constantly sending data beyond your firewall where it is vulnerable to electronic theft. From the time an email is sent until the point at which it arrives at its destination, it travels along a massive web of public, unprotected and insecure networks, perpetually exposed to electronic eavesdropping, snooping and electronic theft, laying your company open to fraudulent misuse of information.

Inside

Networks protected by firewalls may be considered safe and secure from external vulnerabilities. However, insecure email within protected networks is still susceptible to malicious and determined insiders. On mail servers, tape backups, and many other devices that store email, unencrypted messages and attachments are at risk because they can be potentially access by someone other than the intended recipient.

HOW DO YOU ADD THE EXTRA LAYER OF EMAIL SECURITY NECESSARY IN TODAY’S ENVIRONMENT?

Trend Micro offers three versions of its email encryption technology: Trend Micro Email Encryption Client, Trend Micro Email Encryption Gateway and Email Encryption for InterScan Message Hosted Security.

Trend Micro Email Encryption Client has zero infrastructure cost, is implemented in less than a minute by an untrained user, and requires nothing more than a single click to use. Each time a user sends an email they decide whether to send it as an unencrypted postcard style email or whether to use email encryption to lock the message in the equivalent of a sealed envelope.

Email that is encrypted, however, cannot be read by anyone but the intended recipient, unless he or she chooses to allow access to it.

Trend Micro Email Encryption Client takes encryption to the end user, right to the point where confidential and sensitive corporate information resides in this wireless age of electronic communication and always-on mobile employees. This is also where corporate data is most at risk, however inadvertently. Trend Micro Email Encryption Client can be used independently or in conjunction with either Trend Micro Email Encryption Gateway and Email Encryption for InterScan Message Hosted Security, to provide client-to-client encryption of highly sensitive email.

Trend Micro Email Encryption Gateway puts encryption and decryption at the boundary of the corporate network and is supplied as turnkey software for installation onto hardware from your favorite vendor. It can be deployed adjacent to an existing compliance engine which decides on the messages to be passed to Trend Micro Email Encryption Gateway for encryption. Alternatively, it can be deployed in the SMTP mail path where the inbuilt rules engine makes encryption decisions.

Trend Micro Email Encryption can be rolled out across corporate infrastructures with ease. It can be installed centrally by the network administrator or, because it is so easy to use, it can be installed by individual users on demand. A web based control panel allows the administrator to set policy for both network and remote users.

IT departments can enforce and maintain control over individual usage of email encryption and it can be configured to meet specific requirements to conform to internal policies for management and governance of email content.

Email Encryption for Interscan Message Hosted Security provides policy-based encryption that integrates seamlessly with the content filtering capabilities of Trend Micro's hosted email security service, automatically encrypting email messages and attachments by using content filtering rules that identify types of content or email for particular groups. With policy-based encryption, organizations do not have to rely on end users to secure important content. Encryption is automatically applied, enabling organizations to enforce compliance requirements and help ensure confidential information is kept secure. Since it is a hosted solution, no additional hardware or software is needed. Encryption is offered as a rule action in InterScan Messaging Hosted Security—administrators simply check a box to apply encryption.

TREND MICRO EMAIL ENCRYPTION OVERCOMES THE LIMITATIONS OF PKI TECHNOLOGIES:

Trend Micro's Identity-Based Encryption technology has several important advantages over conventional PKI [public key infrastructure] technologies:

- Simpler for users to send and receive encrypted email.
- Far lower TCO [total cost of ownership], due mainly to its simplicity and ease of use.
- Easier for IT staff to install, operate, and manage.

These advantages are generally shared by competing identity-based solutions. However, Trend Micro Email Encryption has additional advantages over its competitors. These are:

- Higher performance.
- Simplified administration.
- Improved security.

WHAT MAKES TREND MICRO EMAIL ENCRYPTION DIFFERENT?

The most fundamental principle of encryption is the secure exchange of secret keys between sender and receiver. This has been a challenge since the earliest systems invented by Julius Caesar and even more recently developed systems have struggled to overcome it elegantly.

Our key exchange has cracked this challenge. It is based on a system we've developed using the latest highly advanced mathematical knowledge to create a unique key encapsulation mechanism which is coupled with a unique method of separating keys and data. We've then gone one step further and applied elliptic curve cryptography. In addition, we've based our technology on the Advanced Encryption Standard (AES) military-grade security which encrypts every email using 2^{256} possible keys.

It is easy to add an email encryption layer to existing security methods with Trend Micro Email Encryption. Encryption no longer means a big and unwieldy change to your IT infrastructure or to the way your people work. Trend Micro Email Encryption has modernized encryption to the point where it is painless to deploy, implement and use.

Our technology is unprecedented, allowing us to create the Trend Micro Email Encryption product line which provides strong, standards-based security, adds minimal infrastructure cost and integrates seamlessly into your existing systems and processes.

TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: +1 800.228.5651
phone: +1 408.257.1500
fax: +1 408.257.2003

www.trendmicro.com