SecureAge

Email Security for Enterprises & Governments

SecureAge SecureEmail Whitepaper

Email Security

Why is Email Security Necessary?

In today's business arena, email has become an indispensable, daily communication tool to all governments and large enterprises. Sensitive corporate information and documents are frequently transmitted via emails amongst employees and external parties. But they may overlook the fact that email is not a secure mode of communications. Standard emails are like postcards which can be read by anyone. They travel unprotected through the network and remain unprotected even when stored in the mail server. They can be easily eavesdropped and modified along the network link, accessed directly on the user machine, mail server and recovered from backup storage. Any attackers can easily copy and compromise these emails any time, as long as they have access to the user machines, server or network. Furthermore, confidential emails can be easily forwarded to unauthorized recipients causing unnecessary data leaks and embarrassment to the organization.

Evidently, email threats will pose serious implications and may even result in huge financial losses to organizations and government bodies if no security solution is in place to protect the email.

1) Threats of Advanced Malwares

Formidable email threats have raised undue concerns over malware protection, privacy and even the authenticity of the email reader. Widespread email attacks, ranging from the widely known email viruses and spamming to the more malicious risks like unwanted tampering or interceptions or espionage, have dangerously become routine recurrences. In fact, one of the most treacherous and stealthy attacks hounding both government and large enterprises is Advanced Persistent Threats (APT). The APT attackers will inject malicious malwares via social engineering ploy to gain legitimate access into the enterprise network infrastructure. The victims are, most of the time, oblivious to the attacks and the malwares can remain undetected by the enterprise security systems over a long period of time. The ultimate objective of such attacks is usually to steal sensitive information from user's documents or email communications.

One of the recent renowned attacks is at HBGary. A team of organized attackers gain access to the key enterprise servers by exploiting sensitive emails and using them to embarrass the company and their business partners.

APT is real and very formidable. It has given momentum to governments and enterprises to accelerate their initiatives in fortifying their enterprise email security infrastructure. They have realized that securing actual user's email ID and data is as crucial as the network perimeters. But given the diversity of the user base in large corporations, it is paramount that the email security system should also be easy to use and does not impede the usage of the email system.

2) Critical business information faced the danger of being compromised

Email is an instrumental tool to organizations for disseminating confidential business information like business strategies and intellectual property. However, without realizing the detrimental impact of such a practice may run the potential risk of highly sensitive information being stolen by competitors or insiders or hackers. Basically, anyone within your corporate networks or the administrator of any of the intermediate email servers may read, delete or even modify your email messages. There is no way the email recipients will know whether this email has been compromised.

3) Invasion of Privacy

Email protocols like SMTP, POP3 and IMAP relay unprotected email messages to designated servers in plain text. This gives any eavesdropper an opportunity to intercept or tamper with the email message at any point during its transmission. Email messages are also stored on email servers in plain text and backups of these messages can be easily made anytime. Even those deleted email messages may still be lying around unprotected in the server or client machine. As a result, any IT administrators or persons who have the access rights to the server or client machine can read any of the email messages any time.

4) Identity Theft, Email Impersonation and Repudiation

Email username and login password are submitted in plain text via SMTP, POP or IMAP connections. This becomes an easy avenue for imposters to steal their targeted username and password which they can then use to access all the confidential email messages and attachments, including those in the past. They may, even without the email sender's user ID and password, impersonate the sender's identity to foil any invaluable business transactions. There is no way to ascertain the sender's identity or to prove that the email received is genuinely from the sender. Any sender can also conveniently claim that they did not send that email even if they actually did. One more worrying fact is that the victimized users tend to use the same password for all the other applications. This means that the attackers, after stealing the username and password from one application, may potentially be able to access the user's emails from their email server.

5) Installing Anti-virus Software, Anti-spamming Software and Firewall is Not Enough

Anti-virus software, anti-spamming software and firewall address only part of the email risks and are not entirely foolproof. Anti-virus software only protects you against deadly viruses. Anti-spamming software only prevents unwanted email spamming and phishing. Firewalls only impede unauthorized access to your network. They do not protect proprietary information from being stolen or sabotaged by potential intruders or insiders. They also do not ensure that only the senders and the intended recipients are privy to the content of the email.

6) Sophisticated Email Security Technology is Not Good Enough

Email security technology has been around over the past 20 years. It is embedded in most commonly used free and commercial email clients today. However, their sophisticated security setup and usage pose a major challenge to non-technical savvy users. It is therefore crucial for companies to implement a robust but hassle-free email protection to address all their email security concerns over insider attacks and malwares. Any users, including those with only minimal computer knowledge, are able to use it blissfully without undergoing any training. Since email communication involves a large user base within the organization, it is best for the email security solution to support multiple email platforms that can be readily deployed into the current email system without having to change the email software or use a different email client.

Why SecureAge SecureEmail is the Best Solution?

The perfect solution to counteract imminent email threats is SecureAge SecureEmail. It ensures email's authenticity and privacy by signing and encrypting email automatically based on IETF S/MIME (RFC 3851) standard without any user's involvement. The S/MIME standard also allows SecureAge

SecureEmail's users to send signed and encrypted email to other non-users. Its ready platform makes integration and deployment into a company's existing infrastructure and processes with ease. Organizations are able to transmit email securely to any recipient without undergoing complicated upgrade or modification to the current email infrastructure.

- Easy to Use

SecureAge SecureEmail allows your users to send and receive secured emails transparently. All they need to do is to follow the usual way of sending or receiving emails without unduly worried about the security setups and configurations. It is so easy to use that even a non-technical savvy person will have little difficulty using the software.

- Improve Your Business Process and Productivity

SecureAge SecureEmail gives you the complete assurance that all your critical business information will be securely transmitted to your intended recipients. You no longer need to fear that such mission critical data will be stolen or compromised, causing you great financial losses or failure to regulatory compliance. Furthermore, the encrypting and digital signing capabilities of SecureAge SecureEmail also elevate your user's confidence over the level of privacy and integrity of confidential information being transmitted via email. Such renewed confidence in email saves them the hassles and costs of sending confidential documents like sales contracts by using expensive and ineffective media like fax and courier services. With SecureAge SecureEmail, you can now use email to your fullest advantage to accelerate your business transactions, strengthen relationships with your employees, customers and partners, and also reducing costs in your organization.

- Easy Installation and Implementation

SecureAge SecureEmail can be easily implemented without having to modify your existing email system. Its Graphical User Interface (GUI) and step-by-step instruction makes the installation process hassle free for your IT administrators.

- SecureAge SecureEmail's Advantages over Clientless Email Encryption Solution

For convenience, some organizations may opt for email encryption solutions that do not require any client installation. They simply encrypt and decrypt email messages on the desktop or laptop via some form of self-extracting executable. On the surface, they seem to provide organizations a simpler and secure way of encrypting emails without the hassles of installing email security software and corresponding PKI digital certificates. But think again. Nowadays many viruses and spywares are delivered as self-extracting executables. As a result, such clientless email encryption solution becomes extremely vulnerable to the danger of accepting treacherous emails that may potentially compromise the organization's desktops or laptops.

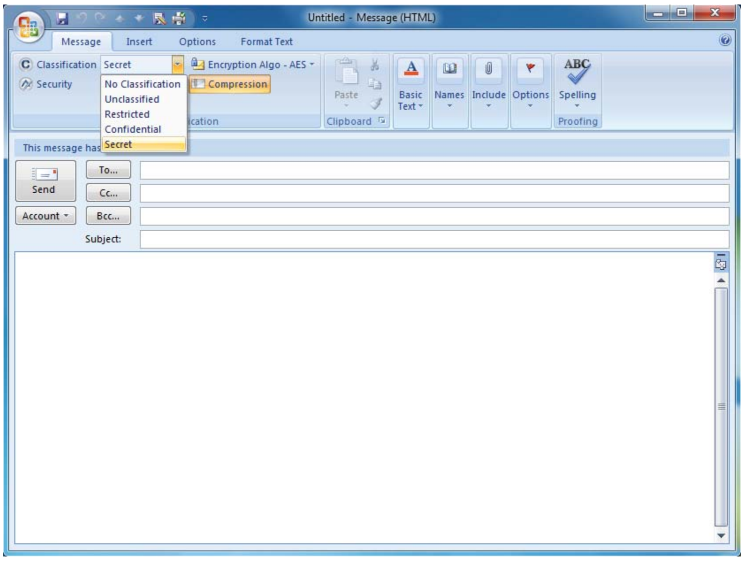
Another clientless solution is using secure email gateway to only protect emails that are sent to external parties. There is no protection for any email exchange internally and no protection against email lost, insider attacks and malware attacks. Sad to say, some organizations are using this clientless solution simply for the sake of regulatory compliance even if it does not provide a robust email protection.

On the contrary, end-to-end email security solution like SecureAge SecureEmail is the best way to fully secure email transmission for any organizations. It supports state-of-the-art encryption and digital signature technologies. Its end-to-end encryption capability enables email messages and attachments to remain encrypted during the entire transmission and even up to the point when they are stored on the desktop, laptop or server. Any unauthorized access of such encrypted email messages and attachments will only unveil scrambled content that does not make any sense. Only intended recipients have the authority to decrypt and read the email content.

How does SecureAge SecureEmail work?

1) Policy Based Security Control

SecureAge SecureEmail provides a powerful policy based security control that configures and integrates intuitive email labeling into standard email clients. The email labels are classified based on how companies traditionally labeled their sensitive paper documents with easy to understand classifications like "Confidential" and "Secret". Hence, users do not have to be trained on how to label their emails.



An enterprise IT administrator simply uses SecureAge SecureEmail's software configuration tool to define email classification labels (like "Confidential", "Secret" and "Protected") that are relevant and familiar to their employees within the organization. Each email can be classified under a label to signify its level of confidentiality. It helps users to effortlessly eliminate email security risks without having to understand the complexity of security technology. Such labels are highlighted in different colors and added to the email body in plain text, html text and rich text format. The different color codes make the labels more prominent when the emails are read on the computer monitor or printed out as hardcopies. These labels can also be added to the email subject line for convenient viewing in email list view. They can even be added to email MIME header so that email server or Mail Transfer Agent (MTA) could apply further policy control to these labeled emails. For example, a MTA may be configured to block emails that are labeled as "Secret" from being pushed to unprotected handheld devices.

However, most enterprise users are not technically savvy enough to decide correctly on which types of emails should be signed or encrypted. With SecureAge SecureEmail, this problem is resolved by integrating the digital signing and encryption operations with the policy governing labeled emails. The users only need to decide how they should label an email and leave the requirements on digital signing and encryption to the policy rule engine. The email labels selected by users are securely embedded into signed or encrypted emails so that they could not be tampered with. The policy rule engine also determines how each labeled email should be treated when transmitted, stored, forwarded and replied to. It also defines what recipients can and cannot do after receiving email with specific classification label.

Such comprehensive set of security policies can be easily created for all labeled emails via SecureAge SecureEmail's software configuration tool. The following security associations are some examples:

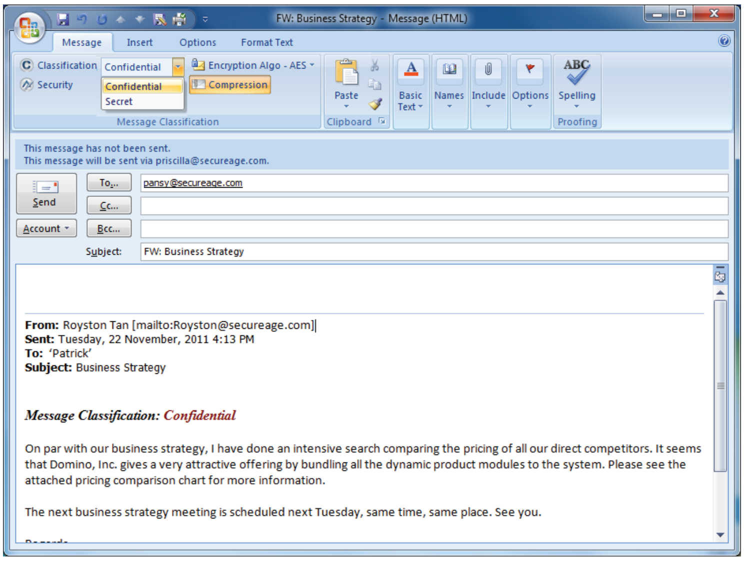
i) The email security of different labeled emails

The policy can mandate that a "Secret" email must always be signed and encrypted, but a "Confidential" email must be encrypted but with optional digital signature.

How Does SecureEmail Work?

ii) The policies related to replying or forwarding a labeled email

A “Confidential” email can be upgraded to “Secret” email when forwarding or replying, but it cannot be downgraded to “Unclassified” or normal email.



Classification: Confidential
Confidential
Secret

This message has not been sent.
This message will be sent via priscilla@secureage.com.

To... pansy@secureage.com

Subject: FW: Business Strategy

From: Royston Tan [mailto:Royston@secureage.com]
Sent: Tuesday, 22 November, 2011 4:13 PM
To: ‘Patrick’
Subject: Business Strategy

Message Classification: ***Confidential***

On par with our business strategy, I have done an intensive search comparing the pricing of all our direct competitors. It seems that Domino, Inc. gives a very attractive offering by bundling all the dynamic product modules to the system. Please see the attached pricing comparison chart for more information.

The next business strategy meeting is scheduled next Tuesday, same time, same place. See you.

iii) The encryption algorithms for different email labels

A “Confidential” email can make use of Triple-DES or AES, but a “Top Secret” email must make use of a proprietary algorithm privately developed.

iv) Protect email from leaking out

An email labeled as “Private” could be controlled by disabling it from being forwarded to a third party and/or disabling it from being printed to a printer.

2) Seamless Integration with Most Email Applications

SecureAge SecureEmail enables secure email exchange among all mainstream email software. It works seamlessly with most email platforms like Lotus Notes and Microsoft Outlook. Organizations can readily deploy SecureAge SecureEmail without having to change their current email software or use a different email client. They can even incorporate their own secure email business logics by adding email security features like email security classification and secure email policy rules to their email communication.

3) Automated SecureAge SecureEmail Sending Agent

SecureAge SecureEmail provides automated agent that can be used to send out classified and sensitive emails securely. Such agent is ideal for sending out routine but sensitive emails to large group of users without needing human intervention. An enterprise can gain substantial productivity improvement resulting from eliminating the need of using physical letters to send sensitive financial information or classified documents to their users.

4) Supports S/MIME V2, V3 and V3.1 Email

SecureAge SecureEmail uses S/MIME (Secure / Multipurpose Internet Mail Extensions) standards to provide a consistent way of sending and receiving email messages and attachments securely. It automatically encrypts and decrypts email without any human intervention, to ensure authentication, message integrity, non-repudiation and data confidentiality.

SecureAge SecureEmail also supports S/MIME v3.1 that comes with email compression capability (IETF RFC 3274). It significantly reduces the size of standard email messages and attachments (like word document, excel, worksheet and text file) by as much as 5 times. At the encryption stage, it also reduces the amount of data being processed and greatly accelerates the processing time.

5) Most Advanced Cryptographic Algorithm Support in the Market

SecureAge SecureEmail ensures robust protection for all transmitted email messages and attachments by using unlimited key length public key digital signature and encryption algorithms. These include RSA algorithms, Digital Signature Algorithm (DSA), Elliptic Curve Digital Signature Algorithm (ECDSA), 168-bit Triple-DES (Triple Data Encryption Standard) and 256-bit AES (Advanced Encryption Standard). Typical usage of 1024-bit RSA is no longer considered sufficient for high security emails. With SecureAge SecureEmail, one could migrate to higher strength RSA (e.g. 2048-bit) or the more efficient Elliptic Curve public key system. For data to be transmitted in a fully secured environment, it is important for the digital signature and encryption key length to be large enough to resist any possible brute force attack. Strong algorithms and larger keys will force an attacker to spend more computing resources and longer time to decipher the encrypted data.

In terms of hash functions used for digital signature operations, SecureAge SecureEmail supports the commonly used SHA-1 and MD5. But the users could choose the stronger SHA-256, SHA-384 and SHA-512 to mitigate against the increased vulnerability of MD5 and SHA-1.

For symmetric key algorithm, SecureAge SecureEmail makes use of the default 256-bit AES algorithm. It also provides support for weaker algorithms like Triple-DES and RC2 for backward compatibility purpose.

6) Smart Card and USB Token Support

By leveraging on SecureAge PKI middleware platform, SecureAge SecureEmail automatically supports key storage on a wide variety of smart cards and USB tokens from different chip vendors. It also supports the storage of user's key on on-board TPM chip that is now commonly available on business PC and laptop, as well as centralized Hardware Security Module (HSM).

Besides acting as a second factor authenticator, another unique security strength of smart card and USB token is their similarity to a bank ATM or debit card. The smart card / token will be locked permanently after an attacker has exceeded the restricted number of authentication attempts. Hence, users can have peace of mind even if their machine and smart card / token are both lost or stolen.

7) Flexible Key Management

Encryption keys are renewed every few years based on a standard PKI security practice. The problem is once the encryption keys are renewed, the user can no longer decrypt past emails with the new key. But this is no longer a problem with SecureAge SecureEmail as it ensures that all archive emails can still be decrypted with every future renewal of encryption keys. It allows access to unlimited key history and automatically selects the correct key for users to decrypt any past email of their choice.

SecureAge SecureEmail also supports both single-key and dual-key usages. The user may make use of a single private and public key pair for signing and encrypting their emails. For some organizations, different key-pairs are issued to each user; one for the signature operation and the other for the encryption operation. This is particularly useful when centralized key escrow process is put in place to ensure encryption key could be recovered when needed but signature key are not duplicated so as to ensure non-repudiation.

8) Migration Tool to Re-encrypt Old Emails with New Encryption Key

In every organization, employees may resign or re-allocated to different sub-organizations and new set of digital certificates are issued. Hence, there is a need to 'migrate' old secure emails to make them accessible by different users or different keys.

SecureAge SecureEmail's powerful migration tool enables organizations to easily re-encrypt old emails with new encryption keys in different email platforms. It allows IT administrator to use the old key for a one time migration. After the migration, the emails in the email server and the archive folders will be encrypted with the new keys and the old key can be immediately discarded. The same tool also allows the users to encrypt confidential emails that were received in plain so that one can be assured that all their emails are protected even when the email storage device is lost or compromised.

9) Supports Email Header Integrity Protection

SecureAge SecureEmail securely signs and encrypts both email content and email header to ensure email integrity. Email header, like email content, when sends in plain, will be exposed to unwanted tampering. Therefore, apart from email content, it is also equally important to protect email header that comprises of the email subject line and the names of the sender and recipients. SecureAge SecureEmail will first check and verify the integrity of the encrypted email header by matching it with the email headers located in the inbox mail folder view. It will then alert the recipient if any discrepancies are found.

10) Supports Proprietary Encryption Algorithms

SecureAge SecureEmail supports user defined proprietary encryption algorithms. To further boost the security strength of their corporate email system, government regulators, military or organizations can choose to incorporate their own developed proprietary encryption algorithms into SecureAge SecureEmail, with or without the standard encryption algorithms.

11) SecureAge SecureEmail Digital Rights Management (DRM)

SecureEmail DRM is an extension of SecureAge SecureEmail. It allows email senders to stipulate additional email permissions and impose certain restrictions on the recipients when accessing the email. It can stop the recipients from copying, printing, screen capturing the email content, and restrict the recipients list when replying and forwarding the email. Email senders can even define the email's expiry date to forbid the recipients from viewing the email contents once it expired and all the expired emails will be deleted permanently.

Key Features

- Automatic Retrieval of Recipients' Digital Certificate

Whenever you send an encrypted email to your designated recipients, SecureAge SecureEmail will automatically perform a directory lookup of your recipients' certificates using a LDAP (Lightweight Directory Access Protocol) repository or Active Directory (AD). After locating your recipients' certificates, it will automatically import these certificates to your personal certificate store for future use.

SecureAge SecureEmail also comes with the capability of automatically expanding your email groups. For example, you want to send an encrypted email to a few recipients listed in a group email address. SecureAge SecureEmail will automatically identify the encryption keys of each and every recipient. The email will then be encrypted using their respective keys to ensure that they are the only recipient privy to the email content.

- Supports Certificate Revocation Checking

By using SecureAge SecureEmail, your email security is guaranteed by its comprehensive Certificate Revocation List (CRL) checking and automatic updating capability. It will automatically check the validity of the digital certificates. The Certificate Revocation List (CRL) of each certificate is automatically updated to ensure their validity. If any of the certificates is found to be revoked, it will automatically retrieve the new certificate and replace the old one.

- Supports Online Certificate Status Protocol (OCSP)

SecureAge SecureEmail provides another advanced certificate revocation checking option via OCSP. OCSP enables online certificate validity checking. It is an ideal option for organizations that require timely revocation information. Digital certificates are considered as valid only after OCSP responder provides a positive response to the status request issued by SecureAge client.

- Supports SecureAge Management Server

SecureAge SecureEmail supports SecureAge Management Server which allows enterprises to centrally control all SecureAge software deployment. It provides central policy control, audit log and key management for SecureAge SecureEmail.

- Helps Achieve Regulatory Compliance

SecureAge SecureEmail is able to help your organization to fulfill regulatory compliances like 201 CMR 17 (Massachusetts Privacy Law), Senate Bill 227 (Nevada Electronic Encryption Law), California Security Breach Information Act (Senate Bill 1386), Sarbanes-Oxley Act of 2002 (SOX), Health Information Portability and Accountability Act of 1996 (HIPAA) and the Gramm-Leach-Bliley Act of 1999 (GLBA).

SecureAge SecureEmail fulfills the Massachusetts Privacy Law - 201 CMR 17 compliance by signing and encrypting confidential emails to prevent data loss, frauds and identity thefts. It fulfills the requirement under Nevada SB 227, HIPAA and GLBA by encrypting email messages and attachments to protect the confidentiality of information, whether during transmission over the Internet or stored in the desktop / laptop / email server. It also helps your organization to comply to the legislation of SOX with its authentication and encryption capabilities.

Technical Specifications

- Support PKCS #1, #5, #7, #8, #9, #10, #11, #12 standards.
- Support MD5, SHA-1 and SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512) hash functions.
- Provide full support for X.509 v3 and PKIX compliance extensions digital certificate format.
- Support external PKI / CA for certificate based authentication and certificate validity checking.
- Support key and certificate import / export via PKCS #12, DER and PEM formats.
- Support smart card and USB token via PKCS #11.
- Support .pem, .der, .cer, .crt, .p12, .pfx, .p7m, .p7s and .p7z file formats.
- Support SecureAge CA and many other public and enterprise CAs.
- Interoperable with other commercial S/MIME compliance solutions.
- Support user account and certificate mapping.
- User-friendly GUI customization via email templates.
- COM APIs and DLL to provide integrated PKI support for external applications.

Need More Information?

Sales Enquiry: biz@secureage.com
Public Relations / Marketing: pr@secureage.com

General Enquiry: contactus@secureage.com
Technical Support: support@secureage.com

www.secureage.com
www.lockcube.com

Asia Pacific
SecureAge Technology Pte Ltd
3, Fusionopolis Way
#05-21, Symbiosis
Singapore 138633

Japan
SecureAge K.K.
Barbizon 18, 7F
5-18-18 Shirokanedai
Minato-ku, Tokyo 108-0071
Japan

North America
SecureAge Technology Inc
3 Twin Dolphin Drive Suite 150
Redwood City CA 94065
U.S.A.