



Email Encryption

Overcoming the Two Big Obstacles to Deploying Email Encryption: Cost and Complexity

White Paper

WatchGuard® Technologies, Inc.

Published: March 2011

Introduction

Email was the original “killer app” of the online age; it was the tool so desirable that people were willing to buy into the Internet boom just to have it. And in spite of all the communication methods that have rolled out since, including text messaging, instant messaging, and social networking, email remains king.

Checking email is the first and last task of the day for most workers. According to a survey by Osterman Research, email is so vital that 82 percent of employees working in large companies regularly check email from home on weekdays, 78 percent log in on weekends, and 61 percent while on vacation. [Source: Osterman Research, 2010]

Electronic mail is more than just text typed into the body of a message. Email is the single most-used medium for sending files within an organization and transmitting them outside the network boundaries. The Osterman study found that 29 percent of emails sent through corporate email systems include attachments. In terms of content volume, those attachments account for close to 96 percent of all content sent via email. As businesses look to secure their email, attachments are a critical component.

LOOK AT THE NUMBERS

How much do we rely on electronic mail in our daily lives?

- **1.88 billion** – The number of email users worldwide
- **2.9 billion** – The number of email accounts worldwide
- **25 percent** – Share of email accounts that are corporate
- **294 billion** – Average number of email messages sent daily¹
- **2.5 billion** – projected number of email users worldwide by 2014²

Why Is Email So Vulnerable to Exposure?

Email makes communication simple. Regular, unencrypted email messages are sent in clear text or some other easily readable format regardless of the email program used. Whether using Microsoft Outlook, Gmail, Eudora, or one of a host of other programs, any recipient with a standard email client can open and read the message.

This interoperability is what makes email vulnerable. Email, as it travels through routers and mail servers on public and private networks to its destination, can be intercepted and read – and even altered – at any point by a third party if it is sent unencrypted. Mail servers on the Internet regularly backup the email that passes through, and if what is backed up is not encrypted it leaves open the possibility of future exposure. A copy of that highly confidential contract you sent unencrypted two months ago may still exist, sitting on a server somewhere just waiting to be discovered. Without encryption, every email you send is an open book – including all your attachments.

Didn't anyone realize the privacy problems that clear text email would cause back when email technology was first developed? Actually, it wasn't an issue, according to Michael Cobb, Web Security Advisor for searchsecurity.com.³ In the earliest days of the emerging Internet world, the original mail

¹ 2010: the year in internet stats, Venture Beat, January 2011, <http://venturebeat.com/2011/01/12/2010-the-year-in-internet-stats/>

² Radicati Group http://email.about.com/od/emailtrivia/f/how_many_email.htm

³

http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1521432,00.html?asrc=SS_CLA_306977&psrc=CLT_14 http://searchsecurity.techtarget.com/expert/KnowledgebaseBio/0,289623,sid14_cid945941,00.html

protocol (still known as Simple Mail Transfer Protocol or SMTP) was developed for government access (the DARPA network) and the security of the connections was a given. The idea of protecting SMTP mail from being hijacked as communications bounced around a global network of mail servers came later – as did HTTP and the interception problems that that technology introduced.

Data Loss over Email

With all the unencrypted email moving around, email is the number one source of data loss risk in large enterprises. One study revealed that more than 35 percent of companies surveyed had investigated a leak of confidential or proprietary information via email over a 12-month period. On average, respondents estimated that as many as one in five outbound email messages contains content that poses a legal, financial, or regulatory risk.⁴ And it isn't necessarily because of malfeasance. Unintentional data leaks are more common than you may think. It's all too easy to accidentally select the wrong recipient name from a drop-down list in your mail client, or to send a file with the intention to share one kind of data, only to realize after the fact that confidential data was included. In 2010, a University of Hawaii faculty member did just that, releasing a spreadsheet with the intention of sharing student research data, not realizing that the file included birthdays and social security numbers of 40,000 UH alumni.⁵

What Data Needs to Be Encrypted?

Most of what is sent in business email does NOT need encryption. The repercussions from the average memo or meeting reminder being intercepted are hardly serious. Communications that do need protection are the ones that carry your business' most precious and revealing data and intellectual property including proposals, contracts, bids, customer credit card numbers, personnel records, patient or client personal identification information, purchase orders, discussions among executives, business plans, product roadmaps, and trade secrets. When these fall into the wrong hands your organization can face adverse, even disastrous, consequences.

Many kinds of data have stringent confidentiality requirements dictated by industry and government. (See page 4.) Other kinds of data may be partially or completely unregulated, but could put a company in legal jeopardy, cause public embarrassment, or diminish market value if their unencrypted files were intercepted. *Table 1: Potential Scenarios and Consequences* in Appendix A lists many common examples.

Talk About Encryption: a Glossary for Business Decision Makers

As a business decision maker, you don't have to dive deep into encryption algorithms and transport protocols to consider options and opportunities for improving your email privacy. Familiarity with the terminology can keep you plugged into project plans and discussions about encryption. *Table 2: Glossary*

⁴ "Email still the top source of data loss," Help Net Security, August 31, 2010, <http://www.net-security.org/secworld.php?id=9806>

⁵ "Security Breach of Personal Information on 40,000 University of Hawaii Alumni Could Have Been Prevented, Expert Say," Hawaii Reporter, November 2, 2010, <http://www.hawaiireporter.com/security-breach-of-personal-information-on-40000-university-of-hawaii-alumni-could-have-been-prevented-expert-say>

of *Encryption Terms* in Appendix 1 provides a short list of encryption terms to help you navigate the email encryption landscape.

Need for Email Encryption Is at Its Peak

Based upon the growing volumes of sensitive information traversing networks daily, regulatory bodies and business executives have turned their concerns to ensure messages are protected from unauthorized viewing. Regulations such as PCI DSS, HIPAA, GLBA, and others have been introduced to mandate that email messages containing confidential data are handled securely.

Email Encryption Laws and Regulations

According to the Ponemon Institute, non-compliance costs are 2.65 times higher for organizations than compliance costs.⁶ That means that companies with ongoing investments in compliance-related activities save money compared with organizations that fail to comply with government and industry mandates. It pays to be compliant.

Email encryption is an essential component of regulations that are designed to protect the privacy and reliability of business and personal information. The following list includes just some of the requirements that are driving encryption adoption in the United States and around the world.

- **HIPAA and HITECH** Encryption is now a primary aspect of HIPAA (Health Insurance Portability and Accountability Act) since the passing of HITECH (Health Information Technology for Economic and Clinical Health Act) regulations in 2009. HITECH requires healthcare providers to notify individuals when their protected health information (PHI) is breached.

For example, if a hacker hijacks unencrypted PHI in transit from a physician's office, the physician practice would have to inform the patients and the Department of Health and Human Services of the breach. However, if the electronic PHI is transmitted in encrypted form, notification is not necessary even if there is a security breach. Encryption grants safe harbor because it can be assumed that the transmitted data is unreadable by unauthorized individuals.

- **PCI DSS** (Payment Card Industry Data Security Standards) is very clear. Requirement 4 mandates the encrypted transmission of cardholder data across open, public networks.⁷ This is a requirement for any organization worldwide that accepts credit card payments from American Express, JCB International, Discover Financial Services, Visa Inc. or MasterCard Worldwide.
- **EU Data Protection Directive** (also known as Directive 95/46/EC) was designed to protect the privacy of all personal data collected for or about citizens of the EU. According to the Information Law Group, encryption is becoming a mandatory checklist item to establish "reasonable" security for sensitive categories of data for the EU, and "... it would be difficult to

⁶"Ponemon Study Shows Cost of a Data Breach", 2010, <http://www.ponemon.org/news-2/23>

⁷ PCI Security Standards Council, Documents Library, https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0

defend an organization's security measures for sensitive data as 'reasonable' without reference to such [encryption] standards or industry practices."⁸

- **SOX** (Sarbanes-Oxley Act) governs the integrity of financial operations of publicly traded companies with the primary goal of protecting "investors by improving the accuracy and reliability of corporate disclosures made pursuant to securities laws." Although encryption is not explicitly mandated as part of the internal controls, SOX implies the need for encryption to protect the integrity and confidentiality of financial information.
- **GLBA** (Gramm-Leach-Bliley Act) requires that all financial institutions maintain safeguards to protect customer information. Although GLBA does not expressly require email encryption, it does require that financial institutions implement the necessary technological controls to protect the privacy and security of customer financial information. The Federal Financial Institutions Examination Council (FFIEC) recommends that institutions employ encryption to mitigate the risk of disclosure or alteration of sensitive information in storage and transit. If a financial institution does not deploy encryption to the degree expected by the FFIEC, then the institution must demonstrate that it considered the use of encryption and justify why it chose not to deploy it. Financial institutions, therefore, must carefully evaluate the need to encrypt emails to protect against unauthorized access to sensitive information.
- **California Security Breach Notification Act (SB 1386)** requires a business, regardless of its location, that owns or licenses personal information about a California resident to implement and maintain reasonable security procedures and practices to protect the personal information from unauthorized disclosure. If protected information is acquired by an unauthorized person, then the business must promptly give notice, *but only if the data was not properly encrypted*.
- **Nevada Statute**, passed in 2008, made Nevada the first among a growing number of states to specifically require encryption of email that contains personal customer information. The statute states that, "A business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission."

The consequences of violating these and other government and industry encryption requirements can include fines (for example, the HITECH Act allows for penalties of up to \$1.5 million), incarceration, public embarrassment, loss of business privileges and customer/client/ patient/stakeholder trust.

The Solution: Seamless Email Encryption from WatchGuard®

WatchGuard XCS SecureMail Email Encryption technology provides easy-to-use, business-class encryption to enable organizations to securely transmit and receive private and sensitive data. This

⁸ "Code or Clear? Encryption Requirements," Information Law Group, <http://www.infolawgroup.com/tags/eu-data-protection-directive/>

encryption solution, available as an add-on subscription for all WatchGuard XCS appliances, provides transparent, policy-driven email encryption, supporting the encryption of large messages up to 100 MB.

Every WatchGuard XCS solution has a powerful data loss prevention engine that identifies outgoing messages that meet pre-defined policies for confidentiality. When an XCS SecureMail subscription is deployed on the XCS appliance, these messages are automatically encrypted, with no special action required by the sender. Encrypted messages are sent as HTML attachments to ordinary email messages and are directly delivered to the recipient. The email recipient does not need special software or applications to open an encrypted email. Encrypted messages can be opened with any browser running on any operating system or mobile device. The process is simple: a recipient opens an HTML email attachment, he authenticates his identity, and he can view the message.

XCS SECUREMAIL ENABLES BUSINESSES TO:

- **Secure Confidential Information**

Outgoing messages containing sensitive information are transparently encrypted, delivered to any mailbox, and are easy for recipients to decrypt and view.

- **Adhere to Privacy and Compliance Regulations**

Sensitive messages are handled in compliance with industry regulations including HIPAA, PCI, SOX, GLBA and others, without any effort on the part of the sender.

How XCS SecureMail Encryption Works

1. **A sender triggers an email** from within the organization. (See Figure 1.)
2. **The email is processed** within the organization's email environment and the email is routed to the WatchGuard XCS appliance for scanning.
3. **The email passes through the XCS data loss prevention engine's pattern and content filters**, which scan the data and match it against pre-defined company and regulatory policies. Each message is checked to determine if it needs to be encrypted, quarantined, bounced, or handled in other ways as established by the policies created by the administrator.
4. **If the message meets the requirements of a specific encryption policy**, the XCS SecureMail engine communicates with the Voltage SecureMail Cloud to generate encryption keys and creates the notification message. XCS SecureMail uses Identity-Based Encryption technology, which generates encryption keys based on the sender and recipient email addresses. The message is signed with the sender's public key and is securely pushed by the XCS appliance to the intended recipient.
5. **The recipient opens the attachment**, and, if it is his first time receiving an encrypted email via XCS SecureMail, he completes a one-time registration and his email address is authenticated.
6. **Once the recipient has authenticated with the service**, the private session key is issued based on the recipient's identity. The entire email, including attachments, is decrypted. Recipient views the message securely.

XCS SecureMail Email Encryption Architecture

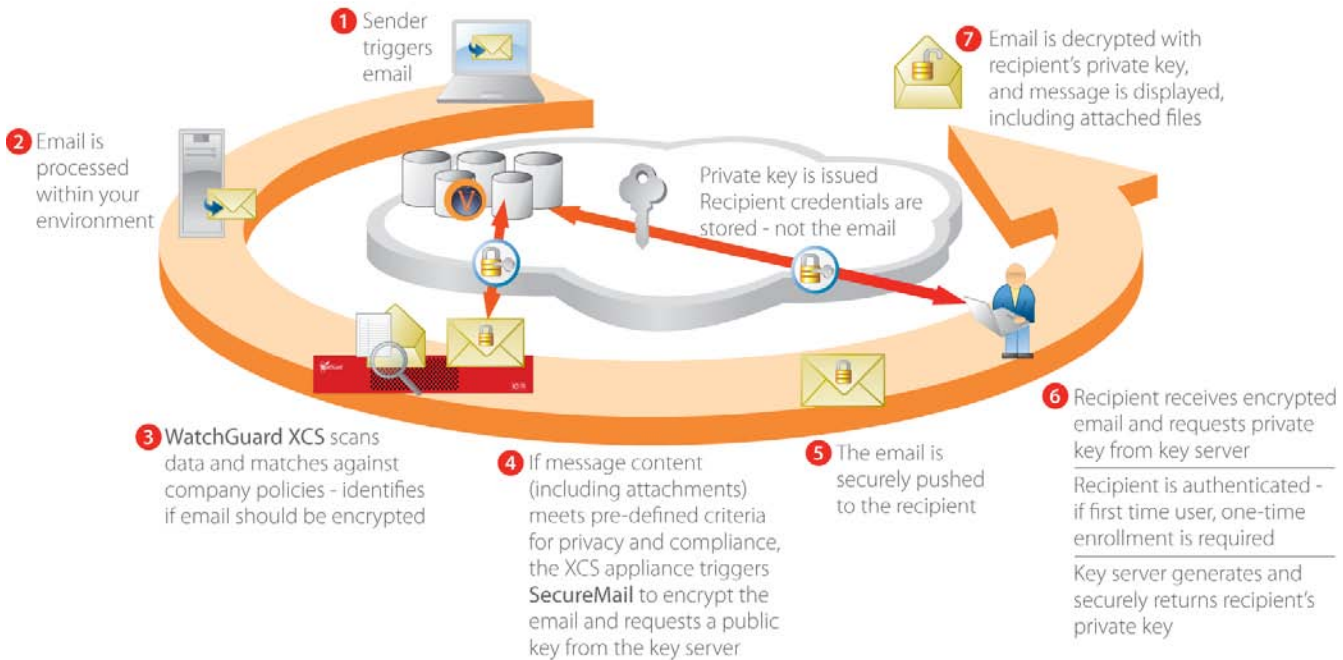


Figure 1. Instant-On Email Encryption

Next-Generation Identity-Based Encryption

XCS SecureMail Email Encryption is based on **Identity-Based Encryption (IBE)** technology, a unique approach that uses a simple identity (an email address) as the public key in a public/private key pair.

IBE came about because of the shortcomings of legacy encryption methods. One of the main problems with other email encryption technologies is that senders and recipients must exchange certificates or keys before any communication can take place. This can be a burden for users.

Other email encryption technologies assume static relationships and authentication policies that do not reflect the dynamics of contemporary business processes. Administrators are forced to deal with cumbersome management responsibilities. Keys need to be tracked, stored, backed up, recoverable, and highly available at all times. Certificates need to be managed, must be renewable and revocable if users are no longer with the organization.

Simply put, these legacy technologies lack usability; they do not scale to support many users; and they are costly to manage. This is how IBE overcomes these issues:

DOWNTIME AND ADMIN BURDENS CAUSED BY LEGACY ENCRYPTION

Results of a 2010 survey of 150-plus participants from the world's largest companies found that:

- **78 percent of organizations have experienced system downtime** due to encryption failures in the past 12 months
- **85 percent of organizations manage encryption certificates and private keys manually** via spreadsheet and reminder notes

Source: Help Net Security, November 8, 2010

- **With IBE, senders can encrypt a message simply by knowing the recipient’s email address.** Keys to encrypt and decrypt are generated dynamically when needed. This means the organization doesn’t need a key database or escrow system to store and archive keys.
- **IBE can use any arbitrary string as a public key,** enabling data to be protected without requiring certificates. A key server controls the mapping of identities to decryption keys. IBE radically simplifies key management because the sender does not need to contact the key server to get an encryption key. Instead, the encryption key is mathematically derived from the receiver’s identity.
- **The receiver must only contact the key server once to authenticate** and get the required decryption key. The key server is able to construct the receiver’s decryption key mathematically, eliminating the need to maintain a database at the key server, making key recovery extremely straightforward.
- **Because keys are generated on-the-fly and never stored, IBE provides greater ease of implementation** and management over traditional public key cryptography technologies, eliminating the complexity of certificates, Certificate Revocation Lists, or other infrastructure requirements.

Benefits of XCS SecureMail Email Encryption

The technical innovations of the IBE technology translate into many tangible benefits for organizations seeking to secure their most critical business communications. When compared to other email encryption technologies such as Symmetric Key Management and Public Key Infrastructure (PKI), XCS SecureMail offers a significantly better feature set at a lower total cost of ownership. The table below highlights key differences in these technologies.

REQUIREMENT	SYMMETRIC KEY MANAGEMENT	PKI	WATCHGUARD XCS SECUREMAIL (IBE)
ENCRYPT	Yes, but online connection required	Often no, when no recipient certificate is available	Yes, to anyone including groups
DECRYPT	Yes	Yes	Yes
INTEGRATION WITH INFRASTRUCTURE	Yes, but requires a per-decryption lookup	Not without complex key escrow and sharing	Yes, no per message lookup or key escrow required
KEY RECOVERY	Must maintain a key database	Must maintain a key database	Yes, no database required
SCALABILITY	Limited by per-transaction key server operations	Limited by operational complexity	Yes, messages and keys are never stored, and keys are generated on-demand

Filters and Lexicons Support Compliance and Policy Management

XCS SecureMail draws on the capabilities of the WatchGuard XCS integrated compliance and policy dictionaries, customized dictionaries created by the administrator, and policies that search the subject headers and body text of email messages and attachments. Pre-defined compliance and privacy lexicons include terms, phrases, and alpha-numeric listings related to financial, health, and other private information, and help enterprises maintain compliance with industry and government regulations.

Centralized, Granular Control of Encryption Policies

Because the XCS SecureMail technology is tightly integrated into the WatchGuard XCS appliances, content control and secure messaging policies are managed and enforced centrally from a single location, without the need for a dedicated, costly management appliance.

Message encryption policies can be highly granular. Once defined, encryption policies are applied automatically at the gateway, ensuring encryption and email privacy are handled consistently. This eliminates the risk of user error – doing away with the need for senders to continually decide whether or not to secure an email's content.

When encryption is enabled, you can use XCS policy and content filtering features to scan for specific patterns in email messages that indicate the message must be encrypted, including:

- **Pattern Filters**
- **Objectionable Content Filters**
- **Content Scanning**
- **Content Rules**
- **Document Fingerprinting**

Policies can be set to encrypt messages based on many attributes of an email message, including:

- **Keywords in Header or Subject Line**
- **Sender or Recipient:** Encryption based on destination (e.g. auditors, Board of Directors, a specific business partner or supplier) or sender.
- **User, Group, or Domain:** For example, all emails from the HR department can be set to be automatically encrypted.
- **Email Body:** Encryption based on full text search of message body.
- **Private Data and Objectionable Content:** Relies on a pre-defined dictionary to identify messages that should be encrypted. For example, any outgoing message that contains credit card information would automatically be encrypted.
- **Keywords and Regular Expressions:** Keywords and regular expressions found in the subject line or content of messages as defined within WatchGuard XCS content control policies.
- **Attachment Type:** For example, encryption can be triggered for all .xls or .csv documents.

- **Attachment Content:** WatchGuard XCS can scan content of over 150 file types for keywords, phrases, or patterns. Detection of policy-based content can then trigger the email for encryption without user intervention.

The SEAMLESS User Experience

WatchGuard XCS SecureMail Email Encryption has been specifically designed for ease of use so that employees, customers, and other business partners can immediately realize the benefits of encrypted email communications.

Sending Encrypted Email: Transparent Encryption

XCS SecureMail is “transparent” to employees. This means that when sending an encrypted email, the user simply composes and sends the email as he would at any other time. As shown in Figure 2 below, the content of the outgoing email is then automatically scanned and, if deemed to contain sensitive material as pre- defined by your organization’s policies, it is then automatically encrypted without any further action by the sender.

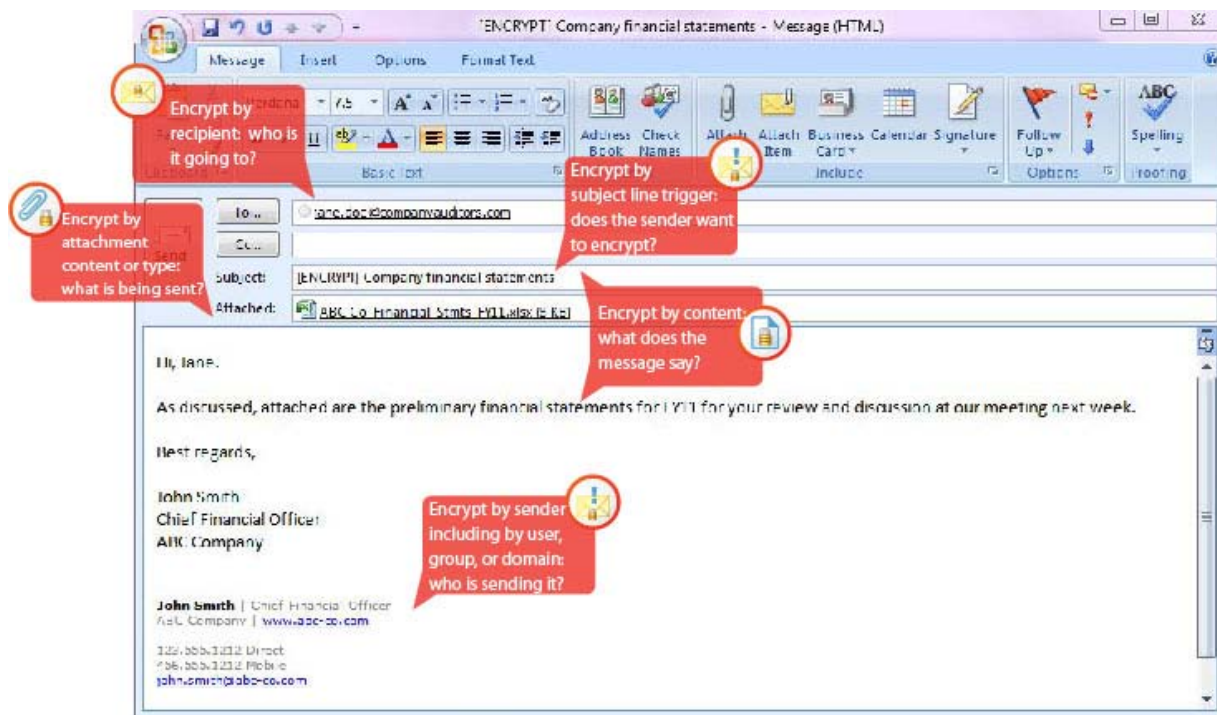


Figure 2. Transparent Encryption Based on Pre-Defined Organizational Policies

Sending Encrypted Email: Manual Encryption

XCS SecureMail also allows a sender to clearly flag a message for encryption by adding a “trigger.” For example, by inserting [ENCRYPT] or [SEND SECURE] in the subject line. This automatically initiates encryption.

Receiving Encrypted Email

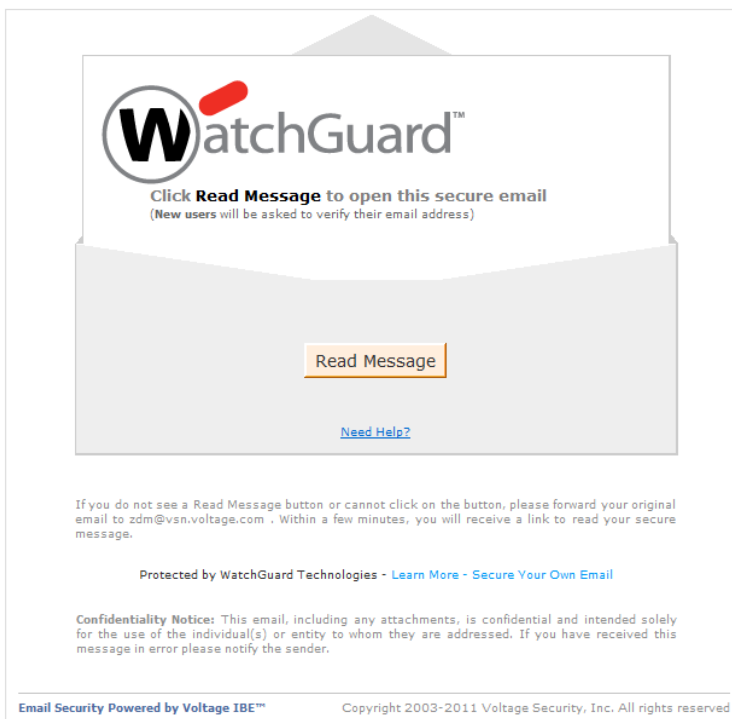
As mentioned previously, no special software is required to receive XCS SecureMail encrypted messages. Recipients can open encrypted messages with any desktop email program or web browser running on any operating system.

1. **Recipient receives a notification message** in her email inbox and clicks to view the message.

Note: The notification envelope can be fully customized with the sending organization's logo and branding with the purchase of an XCS SecureMail Branding subscription.



2. **Recipient clicks on the Read Message button.**



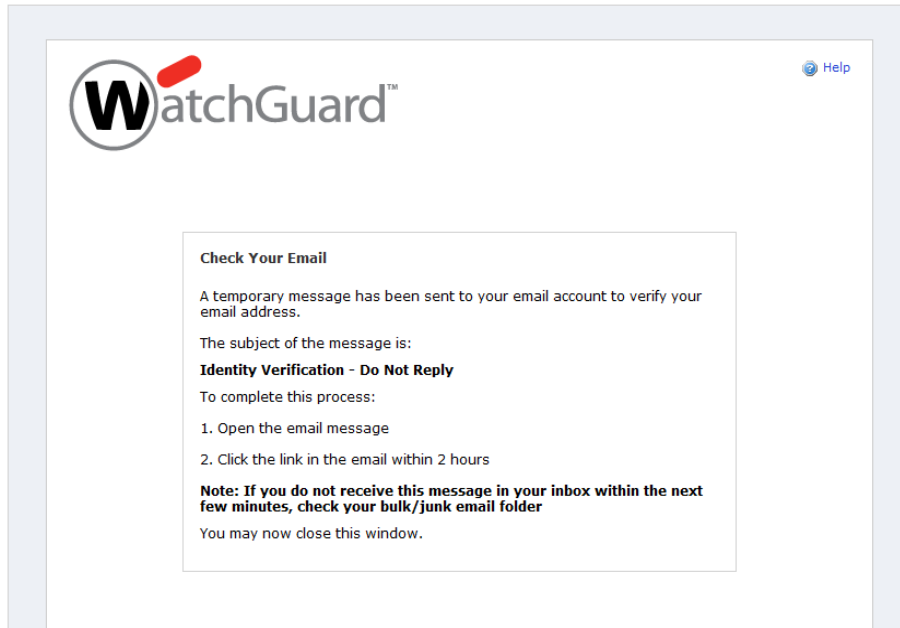
3. **If the recipient has already registered with XCS SecureMail**, she would simply enter her password in the Identity Verification dialog box and click Sign In.

The screenshot shows the WatchGuard Identity Verification dialog box. At the top left is the WatchGuard logo, and at the top right is a 'Help' link. The main content area is titled 'Identity Verification' and contains the following elements: 'Email Address: recipient@example.com' with a text input field; 'Password:' with a password input field; a link for 'Forgot your password? Click here to reset your password.'; and a 'Sign In' button. At the bottom of the dialog box, it says 'Protected by WatchGuard Technologies' and 'Email Security Powered by Voltage IBE™'. The footer of the page contains 'Copyright 2003-2011 Voltage Security, Inc. All rights reserved'.

If the user is a first-time recipient of a SecureMail encrypted message, she creates and enters a password and clicks Sign In.

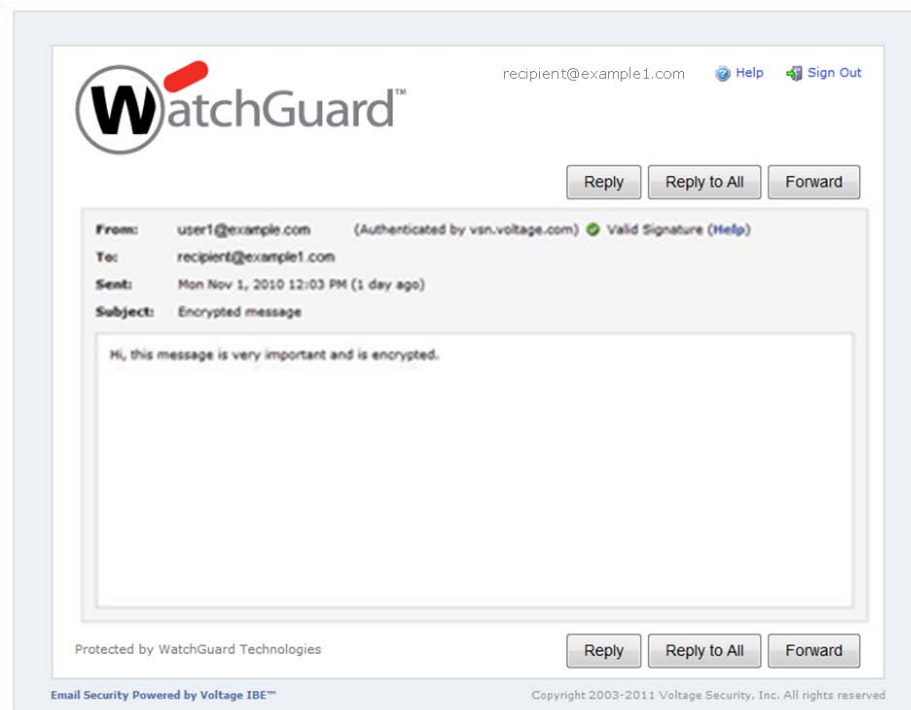
The screenshot shows the WatchGuard 'Create a password to continue' dialog box. At the top left is the WatchGuard logo, and at the top right is a 'Help' link. The main content area is titled 'Create a password to continue:' and contains the following elements: 'Full Name:' with a text input field; 'Email Address:' with a text input field; 'Choose a Password: (6 letters/numbers or more recommended)' with a password input field; 'Retype Password:' with a password input field; and a 'Continue' button. Below the input fields is a grey box containing the text: 'You will be asked for this password periodically for security purposes. We will not share your information or sell it to a third party. We value your right to privacy. By clicking 'Continue' we use this information only with your consent.' At the bottom of the dialog box, it says 'Protected by WatchGuard Technologies' and 'Email Security Powered by Voltage IBE™'. The footer of the page contains 'Copyright 2003-2011 Voltage Security, Inc. All rights reserved'.

A verification message is then delivered to the recipient's inbox. Responding to the verification message is the final step in this one-time registration process.

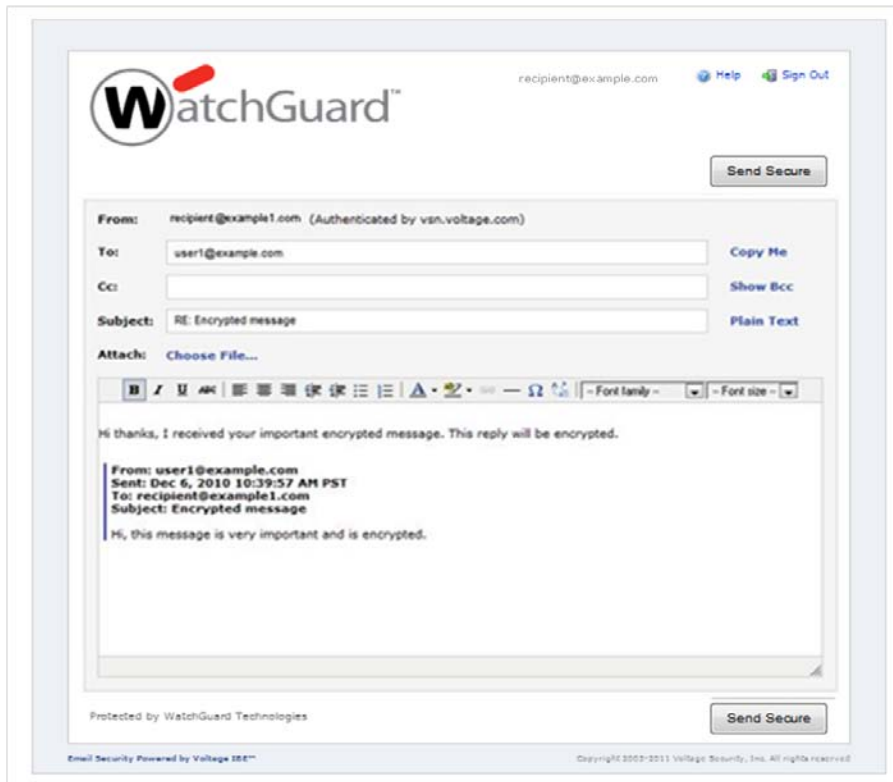


Note: Once a recipient has set up an account, secure messages can be received from any number of senders using SecureMail email encryption, using the same login credentials.

Once the authentication process or initial registration is complete, the recipient can view the decrypted message, which is automatically displayed in the browser window.



4. **Recipient has the ability to securely Reply, Reply All, and Forward the email**, still encrypted, for ongoing secure communication as it moves to its new destination.



The Message Decoding Process

Messages are encrypted using 1024-bit RSA-equivalent (highly secure) industry standards. The HTML attachment in the notification:

- Eliminates the need to install special software
- Ensures the highest delivery rate
- Enables the solution to have universal reach with high usability

Compare this to the many cloud-based services that rely on JavaScript, which is not always available and is often stripped out at the receiving gateway or disabled in the recipient's browser. This results in higher delivery failure rates, user frustration, and higher help desk costs.

Conclusion

No other solution on the market provides greater flexibility and ease of use. With its transparent application and universal reach, WatchGuard XCS SecureMail Email Encryption can send encrypted messages to any email inbox without cumbersome and costly administration, infrastructure requirements, or special client software. Thus, confidential communication is simplified and scalable.

XCS SecureMail provides maximum security to organizations with its transparent encryption capabilities using custom or pre-defined policies, data loss prevention, and compliance dictionaries. Because

messages are never stored on the same server as their keys, XCS SecureMail ensures that only those with permission to view the encrypted message have access to its content.

WatchGuard XCS SecureMail provides the necessary infrastructure so that all you have to do is enable it on the WatchGuard XCS, set data loss prevention policies and compliance rules, and your outgoing emails and data will be protected from unintended viewers.

Next Steps

For more information on the powerful WatchGuard XCS family of extensible content security products with next-generation email encryption capabilities, visit www.watchguard.com/xcs.

Appendix 1

Table 1: Potential Scenarios and Consequences

GROUP OR DEPARTMENT	POTENTIAL SCENARIOS AND CONSEQUENCES
ENTIRE ORGANIZATION	<ul style="list-style-type: none"> • Disparaging Remarks Communications that may cast other parties in an unfavorable light falling into the wrong hands may lead to lawsuits against the company and public embarrassment. • Non-Disclosure Agreements Unauthorized disclosure of information to be kept confidential under a non-disclosure agreement can lead to legal action. • Potential Misinterpretations Communications that may be misinterpreted could fall into the wrong hands and lead to lawsuits against the company by employees or whistleblowers. • Unauthorized Disclosure of trade secrets can lead to loss in the value of intellectual property, loss of business competitive advantage, lost revenue or business, and inability to obtain legal relief under trade secret law.
EXECUTIVE MANAGEMENT	<ul style="list-style-type: none"> • Strategic Plans Important to protect in any kind of business. For publically traded companies, management must prevent unauthorized disclosure of strategic plans or important favorable/unfavorable news that is material nonpublic information in order to prevent insider trading.
BUSINESS DEVELOPMENT / STRATEGIC PLANNING	<ul style="list-style-type: none"> • Merger and Acquisition (M&A) Information An organization must prevent advance knowledge of mergers and acquisitions in order to prevent insider trading or premature disclosure of M&A activity. The right approach to information security can improve business agility. • Strategic Plans Business plans for acquisitions and strategic planning can be trade secrets of the company.
ENGINEERING / R&D	<ul style="list-style-type: none"> • Trade Secrets Research, technology, know-how, and code developed by engineering and R&D are trade secrets of a company. Preserving the value of this intellectual property is dependent on preventing unauthorized disclosure.
ACCOUNTING / FINANCE	<ul style="list-style-type: none"> • Financial Records Compromised confidentiality and integrity of financial records that will be used for the basis of reporting to the SEC indirectly (private company subsidiaries of public companies or possible acquisition targets)

	<ul style="list-style-type: none"> • Other Kinds of Financial Data Exposure of sales or other financial information classified as confidential can result in lost business, loss of competitive advantage, and lost revenue.
HUMAN RESOURCES	<ul style="list-style-type: none"> • Basic Employee Information Employers have an obligation to keep certain kinds of information about employees and job candidates confidential, including social security number, birth date, home address, etc. • Other Kinds of Employee Information Employers may have an obligation to keep info confidential, including background check results, health test results, images (including fingerprints and photos), legal records, driving records, etc. • Review/Performance Information Employers will want to protect employment review and performance information from unauthorized disclosure to prevent potential lawsuits.
LEGAL DEPARTMENT	<ul style="list-style-type: none"> • Client Confidentiality Attorneys have an ethical obligation to preserve the confidences of their client/company they work for. • Corporate Conduct Information concerning the company's failings and wrongful conducted, when placed in the wrong hands, can be used against the company in legal proceedings. Note, however, that when lawfully requested, the company may have an obligation to disclose adverse information to opposing parties.
INFORMATION TECHNOLOGY / SECURITY	<ul style="list-style-type: none"> • Security Posture Communications concerning security assessments, network topography and configuration, and vulnerabilities is sensitive information, if compromised, may lead to attacks exploiting security vulnerabilities.
PUBLIC RELATIONS & CRISIS COMMUNICATIONS	<ul style="list-style-type: none"> • PR Discussions In the event of a corporate PR crisis, or a disaster, it is essential that the crisis response team be able to communicate confidentially to ensure a single voice speaks for the company and prevent unauthorized disclosure of internal non-public communications • Corporate Statements Communications from company officials may be used against the company in legal proceedings. Thus, companies should strive to keep communications confidential to limit disclosure to authorized recipients.
SALES & MARKETING	<ul style="list-style-type: none"> • Internal Data Sales forecasts, customer lists, sales and marketing plans, marketing requirements documents, and other planning documents should be treated as trade secrets of the company.

	<ul style="list-style-type: none"> • Images Transmitting native images for marketing materials may lead to unauthorized disclosure and copying. If copying takes place, the company may need to take expensive legal action to stop it.
CONSULTING SERVICES	<ul style="list-style-type: none"> • Client Data Unauthorized disclosure of confidential information of clients could lead to legal action or lost business.
CUSTOMER SERVICE	<ul style="list-style-type: none"> • Unauthorized disclosure of customer records following a security breach may lead to lawsuits or enforcement actions against the company. Regulatory enforcement actions can come from the Department of Health and Human Services (health records), a banking or insurance regulator (financial services customer records), the Federal Trade Commission (violation of privacy policies, non-banking financial services providers), and the State Attorney General (unfair and deceptive trade practices). <p>Also, private plaintiff lawsuits can stem from customers whose records were compromised.</p>
FINANCIAL SERVICES OPERATIONS	<ul style="list-style-type: none"> • Agreements, Records of Transactions Operations will want to ensure email confirmation of financial transactions, user agreements, and customer lists remain confidential when transmitted via email.
INSURANCE / RISK MANAGEMENT	<ul style="list-style-type: none"> • Actuarial Information gathered at considerable expense to the company can be company trade secrets. The company will want to prevent unauthorized disclosure of such information. • Risk Management A compromise of risk management information concerning security vulnerabilities may lead to security breaches. • Company Reputation Risk management information concerning the company's failings and wrongful conduct, when placed into the wrong hands can be used against the company in legal proceedings and result in negative publicity.

Table 2: Glossary of Encryption Terms

Encryption Term	What It Means
EMAIL ENCRYPTION	<p>Email encryption encompasses various technologies that scramble data in electronic communications so it is unreadable until decrypted by the authorized recipient. To read an encrypted file, you must have access to a secret key or password that enables you to see it in its decrypted form.</p> <p>Unencrypted data is called plain text or clear text; encrypted data is often referred to as cipher text.</p>
KEY	<p>A key is simply a special piece of data used for encryption and/or decryption. Keys are not human readable and typically look like alphanumeric gibberish.</p>
CERTIFICATE	<p>A certificate is a piece of data, typically a public key, that is digitally signed by some signing authority (certificate authority or CA). A signing authority works like a notary public; a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate. CAs are characteristic of many public key infrastructure (PKI) schemes.</p>
SYMMETRIC vs. ASYMMETRIC ENCRYPTION	<p>When encryption is referred to as symmetric, only one key is used to both encrypt and decrypt the message. If encryption is asymmetric, there are two keys – the sender has one for encrypting, the recipient has one for decrypting. Asymmetric encryption is also called public key encryption and was considered a breakthrough in encryption technology when it was developed in the 1970s.</p>
PUBLIC KEY ENCRYPTION	<p>With Public Key Encryption (see above), the key is broken into two parts – a Secret Key that is kept on your computer, and a Public Key that is given out to each email recipient.</p>
PUBLIC KEY INFRASTRUCTURE (PKI)	<p>If the encryption discussion turns to PKI, you're looking at "the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke Public Key Certificates based on public key cryptography." [Source: IETF PKIX working group]</p>
DIGITAL SIGNATURE	<p>A digital signature is a mathematical way to guarantee that a given message was sent by a specific confidant. Be aware that a digital signature does NOT encrypt the document or message; its function is to ensure the authenticity of the sender's identity.</p>

ELECTRONIC ENVELOPE	When an encryption method is referred to as electronic envelope technology, it means that a message is encrypted into a data packet, using a secure encryption standard such as OpenPGP or S/MIME .
TLS (TRANSPORT LAYER SECURITY)	TLS is an IETF standard that provides encryption of message transmission over TCP/IP connections. If both the sender's and recipient's email environment supports TLS, all transmissions traveling to and from both parties' email programs and mail servers are automatically encrypted. If a recipient's email environment does not support TLS, the transmission is sent anyway, but unencrypted.
IDENTITY-BASED ENCRYPTION (IBE)	Identity-Based Encryption technology is a unique approach to encryption that uses a simple identity – an email address – as the public key in a public/private key pair. (See page 7 for a closer look at the benefits of IBE.)

ADDRESS:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:

www.watchguard.com

NORTH AMERICA SALES:

+1.800.734.9905

INTERNATIONAL SALES:

+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. WatchGuard's award-winning extensible threat management (XTM) network security solutions combine firewall, VPN, and security services. The extensible content security (XCS) appliances offer content security across email and web, as well as data loss prevention. Both product lines help you meet regulatory compliance requirements including PCI DSS, HIPAA, SOX and GLBA. More than 15,000 partners represent WatchGuard in 120 countries. WatchGuard is headquartered in Seattle, Washington, with offices in North America, Latin America, Europe, and Asia Pacific. For more information, please visit www.watchguard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis. ©2011 WatchGuard Technologies, Inc. All rights reserved. WatchGuard and the WatchGuard Logo are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part.No. WGCE66732_030311