



## When Pressing the Send Button Results In Compliance Violations

October 2009

### Introduction: The Importance of Compliance

In today's electronic age, organizations are relying not only on traditional communication vehicles such as email, but also real-time web-based communications tools to share information internally, as well as with external parties. As electronic communications tools have become the most prevalent tool for communication and collaboration by businesses and government alike, it has never been more vital to protect the flow of confidential private and company information transmitted via this medium. In the millions of messages sent weekly via corporate email and popmail (such as Hotmail, Gmail, etc.), content (including attachments) inevitably contains data that is private. In every organization, HR, finance, legal, executives, and other critical functions send email that is confidential at a minimum.

As quickly as businesses are increasingly relying on electronic communications vehicles for every facet of business, the techniques of hackers and other malware are evolving at an even faster rate. Hacking has become a lucrative business. The days of teenagers defacing websites are over – now the objective is to steal private financial information and remain undetected. To accomplish this, cybercriminals are increasingly using multi-protocol and multi-application attacks to lure unsuspecting victims to web-based threats that can take control of their computers and compromise confidential information within the network, to be used for financial gain in the underground market. What has emerged is really an arms race between the bad guys and the good guys, with fraud and the privacy of personal information hanging in the balance.

Based on the growing volumes of confidential and sensitive information traversing networks on a daily basis and the reliance on both email and web for critical and private business communications, regulatory bodies and business executives have turned their concerns to ensuring messaging is protected from unauthorized viewing. Regulations such as Sarbanes-Oxley, HIPAA, GLBA and others have been introduced to mandate electronic communications containing sensitive or confidential data are handled securely.

Since the announcement of HIPAA in 1996, increasingly onerous regulations and the requisite process, technology, and reporting improvements have forced organizations to take a hard look at how private information is managed and stored, ensuring that only the proper individuals or systems have access to private information. As such, compliance is an issue that can no longer be ignored. Regardless of a company's size or industry, the impact of regulations in North America and abroad is being felt by IT professionals in every corner of the world.

As within any network, there exist many entry and exit points for sensitive information in a typical organization, and, as such, sending confidential and/or private information and possibly violating compliance regulations is now as easy as pressing the "send" button.

The good news is that many companies have already embraced a messaging security solution to help eliminate incoming security threats such as spam, viruses, infrastructure attacks, etc. A messaging security solution installed at the perimeter can also act as the most effective line of defense for a company, inspecting and applying complicated compliance-oriented policies to outgoing messages. This can make the difference between what is and what is not a violation. Once sensitive content travels outside of the boundaries of an organization, it becomes a violation. A comprehensive secure content and threat prevention solution that spans both email and web traffic using a single policy can stop violations before they occur and help to control an organization's liability.

Despite all the efforts to come up with a simple and complete answer to solving the compliance "problem", it is important to note:

1. **There is no panacea.** Compliance is both broad and complicated, so no one product provides an all-encompassing solution. A combination of processes, policies, and technology is required to get there.
2. **No one really knows what is "good enough."** There have been very few enforcement acts for any of the high profile regulations (SOX, HIPAA, GLBA). We are largely dealing with speculation as to what is good enough to meet the spirit of the regulation. While it may seem obvious that things like access control and encryption are key parts of any compliance solution, without the legal precedent to truly prove this fact, at this point true lasting requirements are not clear.

The WatchGuard Security Platform™ is an easy-to-use, all-inclusive email and web secure content and threat prevention appliance that provides security and privacy of inbound and outbound traffic. With data loss prevention integrated into the solution for inspection, discovery, and remediation of outbound content and messaging, the WatchGuard Security Platform addresses key aspects of compliance requirements across email and web. This whitepaper provides an overview of the key regulations and how WatchGuard enables organizations to enforce and demonstrate compliance.

## Sarbanes-Oxley Act of 2002 (SOX)

### What is SOX?

SOX was initiated as a result of the significant and severe corporate and accounting scandals of organizations like Enron, Adelphia, and WorldCom. These scandals cost investors billions of dollars when the share prices of affected companies collapsed and shook public confidence in the nation's securities markets.

SOX AT A GLANCE	
WHAT	Ensure financial statements are valid through tight internal control
WHO	All U.S. publicly traded companies
HOW	Authentication, anti-virus, encryption
PENALTIES	Jail time for executives, significant fines

The SOX legislation set standards for all U.S. public company boards, management, and public accounting firms as a means of deterring and preventing fraudulent offenses and set significant financial and criminal penalties for corporate officers that commit fraud. The spirit of the regulation is to ensure the validity of financial statements by insuring that proper financial controls are in place.

### **Who is impacted by SOX?**

Every public company that trades in the U.S. is subject to SOX compliance. The regulation does not apply to private companies. Large companies were required to be compliant for their fiscal year ending after November 2004, and smaller companies (with market caps < \$75 million) had until April 2005 to become compliant. To date, over 5000 companies have filed their SOX statements with the SEC.

### **SOX IT Security Requirements**

Since SOX was passed in 2002, it has been on the radar screen of network and security administrators because some of its provisions cross over and become regulatory concern for IT. Some computer security vendors advertise their products, software, or services as “100% Sarbanes-Oxley Compliant.” The reality is, however, that no single technology can make an organization Sarbanes-Oxley compliant.

As with all the other regulations, the legislation does not dictate specific technologies or practices – rather, it states the required outcome. Yet the SEC (the main enforcement entity for SOX) has stated that a standard list of internal controls assembled in 1992 by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) “satisfies their criteria” for SOX compliance. Since COSO, however, has very little to say on IT issues, organizations wishing to be SOX-compliant have been relying on the set of “Control Objectives for Information and Related Technology” published by ISACA otherwise known as COBIT. From an information security standpoint, COBIT requires organizations to:

- **Safeguard information** from unauthorized use, disclosure, modification, damage or loss
- **Assure that electronic transactions** are authorized and authentic
- **Have strong processes** to issue and manage user credentials
- **Prevent an exposure of data** due to malicious software
- **Ensure systems meet performance** and availability requirements

While SOX is primarily focused on the accuracy of financial reporting data, IT security is an important element under SOX in that it enhances the reliability and integrity of the reporting and can prevent data leakage of confidential data or documents that are transmitted electronically via email or web. Again, the legislation does not dictate specific technologies or practices – it states the required outcome. However, Section 302, which assigns responsibility for financial reports, and Section 404, which describes required internal controls, are the two most relevant sections within the regulation that pertain to electronic data loss. Specifically, these sections outline key conditions that relate to email policies and practices for the purposes of financial data leakage, including:

- **Identification and handling** of information that must be kept confidential
- **Identification** of individual message senders
- **Confidential transmission** of email
- **Hardening email** and other servers that store confidential information
- **Tracking and logging** message traffic
- **Auditing** capabilities
- **Message indexing**, archiving, and retention

## Penalties Associated with Non-Compliance to SOX Regulations

The ramifications of not complying with SOX are severe, ranging from heavy fines to jail time for corporate executives. As a result, every public company (and those contemplating going public) must take SOX very seriously and it is important to understand how messaging security can assist their compliance efforts.

## Health Insurance Portability and Accountability Act of 1996 (HIPAA)

### What is HIPAA?

HIPAA mandates the privacy and security of protected health information (PHI). The HIPAA security rule was published in May 2003 and subject to enforcement for all covered entities starting in April 2005. Given the productivity gains for healthcare professionals to communicate with patients and other doctors and health professionals via email, healthcare organizations need to leverage real-time electronic communications, but do so securely.

HIPAA AT A GLANCE	
WHAT	Protect confidential healthcare and patient information
WHO	Healthcare providers, health plans, healthcare clearinghouses
HOW	Access control, authentication, message encryption
PENALTIES	Fines up to \$250,000 (per violation) and/or 10 years of jail time

HIPAA places a number of requirements on the health care industry's information handling practices, and has direct impact on the operation of messaging systems.

### Who is impacted by HIPAA?

Covered entities consist of healthcare providers, health plans (insurance, etc.) and healthcare clearinghouses (claims and transaction processors). Service personnel (accountants, lawyers, etc.) working on behalf of the covered entities are also subject to HIPAA requirements.

### HIPAA IT Security Requirements

HIPAA dictates that organizations must ensure that:

- **Email messages** containing protected health information are secured, even when transmitted via unencrypted links
- **Senders and recipients** are properly verified via person or entity authentication
- **Email servers** and the messages they contain are protected

NIST (National Institute of Science and Technology) has published an information security guide that many believe will meet the requirements of HIPAA. This guide (**An Introduction to Computer Security: The NIST Handbook**) provides the specifics an organization needs to understand the scope of their compliance efforts. <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>

To better understand at a high level the outcomes that HIPAA requires, covered entities must:

- **Have a documented process** to protect PHI and detect/correct security violations
- **Allow only authorized personnel** have access to PHI
- **Develop a process** to respond in the event of a security breach

- **Periodically evaluate** the organization's ability to protect PHI

From a technology standpoint, strong cases can be made for organizations to implement:

- **Access controls:** to ensure the wrong people do not get access to information
- **Detailed auditing of mail traffic:** to track who is accessing data (and more importantly, prove it to the examiners)
- **Encryption:** to authenticate sender and recipient, provide protection of the message contents and ensure a message hasn't been tampered with

While HIPAA does not specify particular technologies that should be used to implement these rules, the regulation can be seen as an attempt to mandate best practices for information security, and, for the purposes of this paper, messaging security.

### Penalties Associated With Non-Compliance to HIPAA

The general penalty for failure to comply with HIPAA regulations is:

- **Each violation:** \$100
- **Maximum penalty** for all violations of an identical requirement: may not exceed \$25,000

Penalties for Wrongful Disclosure of INDIVIDUALLY Identifiable Health Information include:

- **Wrongful disclosure offense:** \$50,000, imprisonment of not more than one year or both
- **Offense under false pretenses:** \$100,000, imprisonment of not more than five years, or both
- **Offense with intent to sell information:** \$250,000, imprisonment of not more than ten years, or both

## Gramm-Leach-Bliley Act of 1999 (GLBA)

### What is GLBA?

The Gramm-Leach-Bliley Act of 1999 is fundamentally intended to ensure the protection of consumers' private financial data. It is the sister legislation of HIPAA, but targeted at the financial industry.

The essence of the regulation is to protect consumer's financial information such as credit card numbers, social security numbers, account numbers, etc., which the Act refers to as Nonpublic Personal Information (NPI) and protect NPI from unauthorized use or access.

GLBA AT A GLANCE	
WHAT	Protect consumer's non-public information (NPI)
WHO	Financial institutions of all sizes
HOW	Strong authentication, server defenses, encryption
PENALTIES	Imprisonment of company officers for up to 5 years and steep monetary fines ranging from \$10,000 to \$100,000 per offense

Every financial institution that handles consumer non-public information (NPI) is subject to the GLBA legislation. This includes banks, brokerage firms, mortgage lenders, financial planners, and insurance companies (which are also subject to HIPAA).

### Who is impacted by GLBA?

GLBA affects U.S. financial institutions such as banks, credit unions, securities brokerages, and insurance firms. Companies providing other types of financial products and services to consumers are also affected, including: lending, brokering or servicing any type of consumer loan, transferring or safeguarding money,

preparing individual tax returns, providing financial advice or credit counseling, providing residential real estate settlement services, collecting consumer debts, and so on.

## **GLBA IT Security Requirements**

GLBA states the following requirements in Title V of the regulation:

### **Financial Privacy Rule (The Privacy of Non-Public Personal Information)**

“Each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ non-public personal information.” The Financial Privacy Rule provides for a privacy policy agreement between the company and the consumer pertaining to the protection of the consumer’s personal non-public information.

### **Safeguards Rule (The Establishment of Customer Financial Data Protection Measures)**

“Each agency or authority...shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards” to:

1. **Ensure the security and confidentiality** of customer records and information
2. **Protect against any anticipated threats** or hazards to the security or integrity of such records
3. **Protect against unauthorized access** to or use of such records or information which could result in substantial harm or inconvenience to any customer

From a messaging security perspective, GLBA ultimately breaks down protection into three larger contexts:

1. **Financial Privacy:** covers the collection and distribution of information, including how NPI is used in operations
2. **Safeguards:** requires that certain processes and technologies be implemented to protect collected NPI
3. **Pretexting:** lays out the ramifications of impersonating someone to fraudulently obtain private information

Similarly to HIPAA and SOX, GLBA does not specify technologies to implement the safeguards; however, the Safeguards Rule means that companies should implement policy enforcement tools that can apply appropriate remediation (i.e., encrypt or block email traffic), as appropriate, based on message sender, context, recipient, and/or content. Furthermore, to allow organizations to demonstrate compliance or to allow them the ability to track NPI data loss incidents, the Act dictates that companies must implement systems that provide detailed logging and reporting.

## **Penalties Associated With Non-Compliance to HIPAA**

The GLBA gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule and the Safeguard Rule. Non-compliance of GLBA can result in a variety of fines and up to five years imprisonment for each violation.

Violation of the GLBA may result in a civil action brought by the United States Attorney General. A 2003 amendment to the act specified:

1. "...the financial institution shall be subject to a civil penalty of not more than \$100,000 for each such violation," and
2. "...the officers and directors of the financial institution shall be subject to, and shall be personally liable for, a civil penalty of not more than \$10,000 for each such violation."

## How WatchGuard Addresses Compliance

WatchGuard solutions encompass several of the technology requirements for securing data-in-motion as dictated by SOX, HIPAA, and GLBA, including authentication, encryption, content filtering, hardened message server software, on-box remediation, and message logging and archiving.

The WatchGuard Security Platform is an easy-to-use, all-inclusive email and web appliance that provides security and privacy of inbound and outbound traffic. As a set-and-forget appliance, WatchGuard Security Platform is the first product to enable organizations to centrally control, protect, and manage both inbound and outbound messaging across multiple protocols with consolidated administration and reporting. It provides content security that enables instant-on data loss prevention, encryption and content filtering with integrated threat prevention for viruses, spam, spyware, phishing, crimeware and malware attacks, all in a secured appliance.

### Comprehensive Protection to Eliminate Gaps

When investigating the various methods for data-in-motion protection from data loss, it is vital to evaluate the entire landscape of content that employees use. Today's employee has instant access to the Web and email through which content can escape, including sending data via popmail systems such as Hotmail®, wikis, blogs, and sending messages and files via email to unlimited, unknown, and mostly unrestricted recipients. This fact highlights the risks of data loss prevention as a silo, versus a consolidated platform. The security and administration risks are gaps that place policies into various places in the network versus a single location.

Further broadening the gap are disparate scanning of email and web mediums, and reporting data loss prevention activities and violations across multiple protocols and technical silos. With the WatchGuard Security Platform, data loss prevention is provided for both email and web protocols in a single administrative access point for creating, managing, and enforcing policies for protecting your organization from leakage. WatchGuard Data Loss Prevention, which is built within the WatchGuard Security Platform, is not only transparent from end users as a secure content and threat prevention security platform appliance, it provides effective and efficient security.

The WatchGuard Security Platform, when implemented at the perimeter in front of email and web servers, protects the message store from direct attack and enforces proper access control and authentication requirements inherent to each of the regulations discussed in this paper.

The WatchGuard Security Platform has the ability to block infrastructure attacks (directory harvest, denial of service, etc.) and provide both strongly authenticated management access and secure web mail access makes it the foundation that drives privacy and compliance.

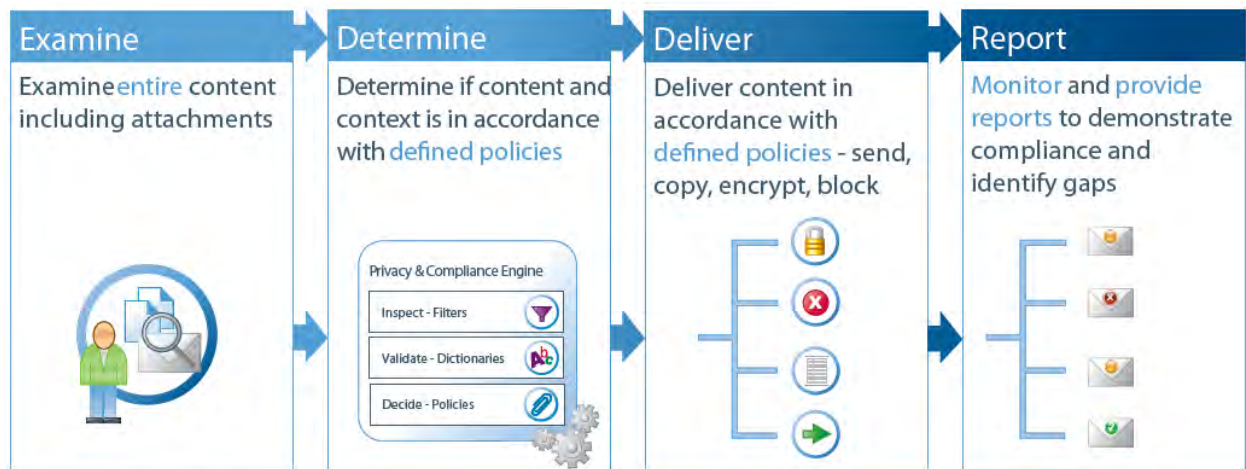
### Centralized Policy Management

WatchGuard Security Platform's management console is a best-in-class administration and control center that consolidates all email and web features providing a single, easy-to-use interface for centralized management of reporting, policy management, policy remediation, on-demand feature enablement and clustering. Displayed in a secure and delegated administrative web interface that can be both remotely and locally managed, the WatchGuard Security Platform provides total visibility and control of all email and web traffic, thus enabling organizations to centrally create, control, and enforce policies across multiple protocols and lines of business for enhanced visibility into data-in-motion for regulatory compliance purposes.

## Integrated Process for Privacy & Compliance Protection

Once securing the messaging infrastructure, the four key integrated processes involved in meeting the spirit of the regulations discussed in this paper are:

1. **Examine:** Each message passing through the WatchGuard Security Platform must be checked for private/sensitive data.
2. **Determine:** Based on the policies and the content discovered, determine the appropriate action to take on the message.
3. **Deliver:** Take the appropriate action on the message, whether it be handling the identified message in accordance with the defined policy – allow, block, encrypt, copy to compliance officer, message stamping, return to sender, audit/log.
4. **Report:** It is important to be able to document both the policies that have been implemented to enforce the regulations, as well as tracking actual message traffic to ensure compliance.



## Examination of Content

To provide the required flexibility for compliance, the messaging security appliance must provide pre-defined dictionaries for each of the applicable regulations. For example, having a dictionary to catch ID-9 codes (healthcare diagnosis codes) is a key component of HIPAA compliance. It is also critical to be able to customize the dictionaries for organization-specific data and formats. Finally, the ability to catch universal data formats (also known as regular expressions) such as social security numbers is also a requirement.

Knowing where to look for potential data loss is as important as knowing what to look for. Common places include:

- **Message Headers:** Who is sending the message? Who is receiving it? Supporting sender authentication and looking for header inconsistencies is important.
- **Body Content:** What is in the message? Are there key words that violate the regulation? What about account numbers or social security information? All of this must be discovered.
- **Attachments:** Being able to deeply analyze attachments to look for sensitive data, regardless of the type of file or its size.

## Powerful Deep Content & Contextual Analysis

With the WatchGuard Security Platform, deep content inspection is performed for email and web traffic using a content and contextual methodology. WatchGuard Data Loss Prevention scans all email and web traffic, including files and attachments, in an effort to discover violations, but it goes further by also inspecting the context of the traffic. Inspection of context enables WatchGuard to inspect who is sending the content and where or whom the content is being sent to, which is vital in determining if the content is a violation or not, and the proper remediation tactic to employ. For example, if the CFO is emailing an attachment that contains sensitive financial data to the business auditors, that context is vital because the proper policy and remediation would be to log it for reporting and then encrypt the email, including the attachment, for delivery to the auditor.



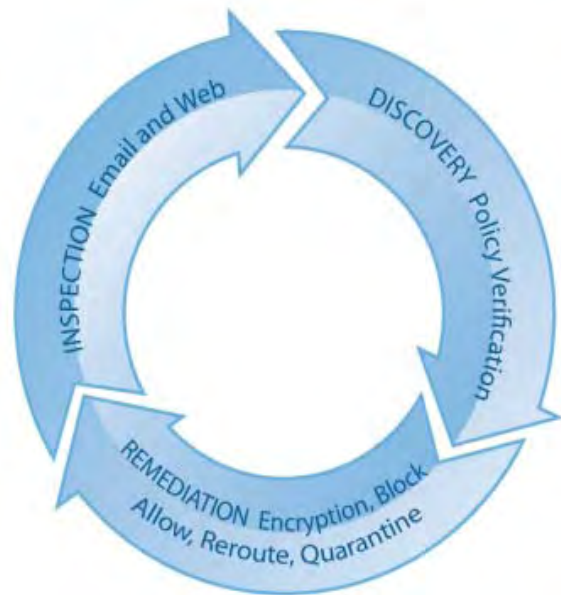
Without context, a typical data loss prevention system would easily block or quarantine this important communication, thus impeding business processes. The opposite scenario can also be true, if, by policy, an employee in customer service is sending the same document to an unknown or unauthorized recipient, the communications should be blocked or quarantined to prevent the leakage of this data.

## On-Box Remediation

Once the content of a message is examined, the messaging security appliance must utilize a sophisticated policy engine to determine the appropriate remediation to take on the message based on pre-defined policies which can be set across multiple protocols. Policies should be easy to set up and applicable to large groups as well as individual users, depending on their job functions and requirements, across an enterprise of thousands of users.

The policies must allow for both single and compound actions to be taken on a message. For example, a company may want to simply block a message that violates the SOX policy.

Or there may be the need to allow the message to go through, but encrypt it using a third-party encryption server.



Those are just a few simplistic examples of potential policies, but the policy engine must be able to support multiple options and actions.

As demonstrated in the figure above, WatchGuard Security Platform provides a series of templates to create policies. The flexible templates allow users and groups to be attached to the policy by either listing the user's email address, an applicable domain, or using native LDAP lookups. WatchGuard Security Platform policies also define the processing rules, which can be inherited from system default policies.

### **Message Delivery Based on Predefined Policies**

Once the content is examined and the appropriate actions are determined, the messaging security platform must be able to execute the policy in an efficient and scalable fashion.

WatchGuard Security Platform provides a number of different message actions which can be associated with any policy and can also be different depending on whether the message is inbound or outbound.

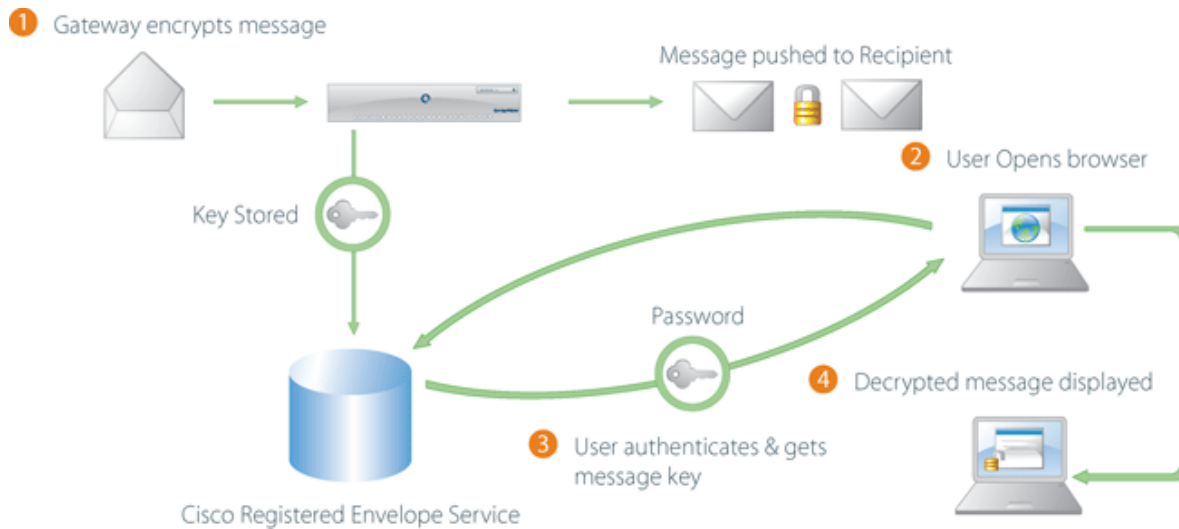
1. **Allow**
2. **Block**
3. **Quarantine**
4. **Encrypt:** WatchGuard Security Platform supports a variety of encryption techniques, including TLS/SSL, S/MIME, PGP, and CRES.
5. **Copy:** Message can be copied to any recipient.
6. **Message Stamping:** A disclaimer can be added to every message to govern the use of the information in that message.
7. **Audit/Log:** Regardless of the action taken, all message activity can be logged to prove compliance and provide documentation during a regulatory examination.

### **Email Encryption for Enhanced Data-In-Motion Protection**

A highly effective tool for privacy of confidential data for regulatory compliance is WatchGuard Email Encryption. The solution is tightly integrated into the WatchGuard Security Platform appliance to enable instant-on security for confidential, regulated, and business-prudent data. WatchGuard Email Encryption provides an easy-to-use, secured Envelope for enterprises that do not want the burdens and costs associated with traditional encryption deployments and administration, but require:

- **Message security** for privacy and compliance with business-class features of reliable read receipts
- **Secure replying and forwarding**
- **Message expiration**
- **Customized branding** of the Envelope by your business
- **Message recalling**

The encrypted Envelope does not use clients or certificates so it does not require a pre-exchange of credentials. It is agnostic to the email and OS environment to allow the secured message to be sent to any email recipient at any time, it can be securely delivered to mobile devices like the BlackBerry, and it encrypts the entire payload including attachments.



WatchGuard Email Encryption is a valuable tool for the following:

- **Compliance regulations** including HIPAA, Sarbanes-Oxley, the Gramm-Leach-Bliley Act, the PCI Data Security Standard, PIPEDA, California Senate Bill 1386 and other state data privacy laws, SEC regulations, U.S. Federal employment standards, UK Data Protection Act, Safe Harbor Act and the EU Data Protection Directive
- **Intellectual property** including financial statements, intellectual property, mergers and acquisitions, sales and marketing plans, human resources, and legal agreements and correspondence
- **Privacy data** including customer names, addresses, government ID numbers, credit card numbers, account numbers, pass codes, health and human services, and human resources
- **Logging and reporting** of policy compliance violations for incident reporting

Perhaps the most critical aspect of compliance is the ability to document and report on the processes used and the results of the safeguards that are put in place to meet the regulations, including:

- **Reports showing policy configuration** that identify which messages were in violation of policies
- **Forensic ability** to determine what happened in the event of an offense

These are critical components of a market-leading reporting capability.

WatchGuard Security Platform compliance reports can be customized to include as little or as much detail as required. It also provides significant customization capabilities to present the appropriate data in the most applicable format. Any compliance violation flagged by the report can be investigated using the interactive tools and event database included in the WatchGuard Security Platform.

### Multi-Protocol Reporting

By capturing real-time and historical data across the WatchGuard Security Platform, the system's management reporting mechanism provides accurate, timely, and customizable auditing and reporting of all email and web traffic. Reports are designed to consolidate information for compliance officers, senior executive, and IT administrators automatically with customizable point-and-click reports generated at specified intervals, in varying file formats. WatchGuard Security Platform's management reporting captures and stores all traffic information and categorizes the data into functional, easy-to-understand and useable reports categorized by spam, threats, malware, encryption, data losses, policy violations, and

others. This reporting methodology allows a full view of the threats and information leaving your enterprise network, correlating the information across multiple protocols for a more holistic view of the issues. Custom filters allow administrators to generate reports on users, groups, and other optional areas. The platform engine also provides tracking capabilities that confirm delivery or receipt of message traffic.

## Summary

Whether it's protecting confidential information for privacy and compliance, or ensuring that critical intellectual property does not leak out of an organization, content security is heavily reliant on outbound filtering and policy enforcement. With disclosure legislation increasingly being enacted in all reaches of the world, the cost of a security breach is now material, in hard dollars, to fix the problem and the brand impact of having a high profile breach.

Though no one technology or product is a panacea for regulatory compliance, having a strong email and web boundary security posture and the ability to deeply inspect all inbound and outbound messaging provides a head start on the road to compliance. The WatchGuard Security Platform adds the capabilities that organizations need to secure, examine, determine, deliver, and report on their messaging infrastructure, and take a major step towards compliance.

Don't wait; deploy the WatchGuard Security Platform today to ensure your email and web traffic is not a regulatory liability. To learn more, visit us at [www.watchguard.com](http://www.watchguard.com).

*This document provides general information about personal privacy and compliance initiatives in North America. It is intended to be used for resource and reference purposes only and does not constitute legal advice. Readers of this paper are encouraged to speak with their legal counsel to understand how the general issues discussed above apply to their particular circumstances. WatchGuard Technologies Inc. disclaims any and all liability for damages, costs, lost profits, fines, fees or financial penalties of any kind suffered by any party acting or relying on the general information contained herein.*

---

**ADDRESS:**  
505 Fifth Avenue South  
Suite 500  
Seattle, WA 98104

**WEB:**  
[www.watchguard.com](http://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. Our Firebox X family of extensible threat management (XTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. Our newest appliances – the WatchGuard XTM 8 Series and XTM 1050 – provide high performance and fully extensible, enterprise-grade security at an affordable price. WatchGuard extensible content security (XCS) appliances deliver comprehensive email and web traffic protection for security, privacy, and compliance. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. For more information, please visit [www.watchguard.com](http://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. ©2009 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, and WatchGuard ReputationAuthority 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.WGCE66658\_010710