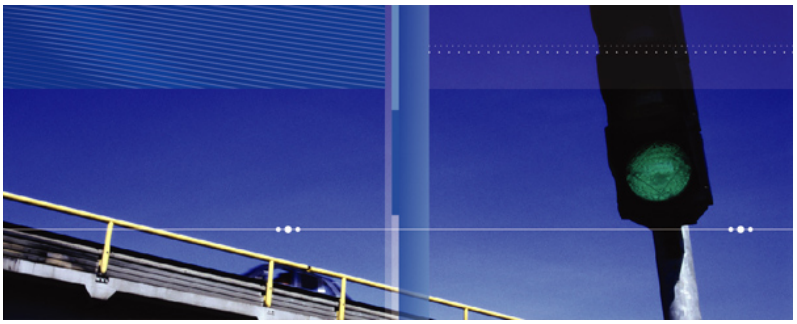
Entrust® Securing Digital Identities & Information



Securing Your Digital Life

Stopping Email Violations Before They Occur:

Using Advanced Content Scanning to Help Achieve Email Compliance

September 2004

Entrust®
Securing Digital Identities & Information

Table of Contents

1 Introduction

Email is by far the most frequently-used productivity tool in any organization. In fact, virtually all of an organization's communications now occur over email.[1] And why not? The business value of email is clear. No other tool can allow individuals to share information and make decisions quite so cost-effectively and quickly.

However, with so much email now flowing in and out of organizations, there are new risks to be managed. Enterprises and government departments are asking new questions of themselves:

- Are we concerned about sensitive information leaving our organization?
- Are we prepared to state that all email moving in and out of our organization meet the requirements of corporate and regulatory policies?
- If not, do we know what risks we are facing?
- Are we prepared to enable proactive solutions for dealing with potential violations before they cause problems?
- What are the benefits of effectively addressing compliance issues?

Organizations must deal with the immediate concern of costly and annoying spam entering their networks—if only to deal with the *real* issues at hand concerning corporate and regulatory compliance.

One of the greatest challenges relating to email facing organizations today relate to compliance. Organizations must decide how to enforce corporate email policy pertaining to offensive language and the protection of private or sensitive information. And, perhaps more daunting a challenge, industry specific issues pertaining to regulatory compliance.

This white paper will examine the many challenges faced by organizations who are striving to comply with corporate and regulatory policies, and identify potential solutions to address these challenges.

[1] Source: Pitney-Bowes Email Productivity Study, 2001

2 The Value of Email

With the increased reliance on email for communications not only among employees, but also outside the organization with partners and customers, it is important to reflect on the value of information that flows over email. Understanding the *nature* of information communicated by email is an important step in assessing and managing any associated risks. For example, in most organizations, email is used to share valuable information such as the following:

97% of an organization's communications occur by email

Source: Pitney-Bowes Email Productivity Study, 2001

- **Intellectual property** such as product designs, client information, and source code
- **Private information** pertaining to customers, patients and employees
- **Internal communications** governing policies, key decisions and strategic plans that are intended for employees' eyes only
- **Sensitive financial information** such as quarterly results, sales pipelines and projections
- **Business communications** such as contract negotiations and supplier information
- **Broad customer communications** such as newsletters and monthly statements

So how does one measure the true *value* of email as an asset to an organization? Perhaps the best way to measure its value is to assess what would happen in the event that the email is viewed by someone other than the intended recipients. In the examples above, improper disclosure or malicious attainment of information could possibly lead to:

- Competitive disadvantage contributing to a reduced revenue and market share
- Violation of corporate privacy or regulatory guidelines, that may result in potential law suits, financial penalties and/or public embarrassment

So how much information is leaking out of an organization? A CSI/FBI survey indicated that organizations lose millions of dollars a year through the loss or theft of information, with the largest loss last year at **$70 million**.[2]

And there are now very real examples of penalties being given out to individuals and organizations violating government regulations. For example, infamous banker, Frank Quattrone, was recently charged with three counts of obstruction of justice and witness tampering for emailing subordinates to "clean up" files, although he knew his firm was being investigated. He has been sentenced to 18 months in prison, a $90,000 fine and two years' probation.[3]

Of course, email is also used as a vehicle for communications that are not valued by an organization such as spam and irrelevant junk mail. In addition to balancing the risks around managing valuable email, organizations are also dealing with the overabundance of unwanted email traffic.

[2] Source: 2003 CSI/FBI Computer Crime and Security Survey

[3] Source: San Francisco Chronicle, Thursday, September 9, 2004

3 The Challenges Relating to Email Compliance

With such a huge increase in the amount of email now flowing in and out of organizations, managing issues relating to efficiency, compliance and information disclosure are more important than ever. Organizations must deal with the following challenges:

- ***Network and Productivity Protection*** – maintaining an efficient email system so that more challenges and issues can be addressed
- ***Corporate and Regulatory Policy –*** enforcing email policy pertaining to corporate and regulatory guidelines
- ***Message Security –*** protecting private and sensitive information for compliance and risk mitigation

3.1 Network and Productivity Protection

In order for email to remain a productive and useful tool, organizations are challenged with ensuring that their networks are free from malicious viruses and are not bogged down by spam. Now reaching higher than 50% of email traffic in 2004[4], the rapid rise in spam has had a significant impact on network efficiency and ultimately on the productivity of employees. Organizations spend an additional $86 per user mailbox per year just to deal with the volume of spam[5], effectively doubling their infrastructure costs. Meanwhile, employees spend on average 10 minutes per day dealing with spam[6], which can cost a 25,000-user organization over **$50 million dollars per year in lost productivity costs alone.**[7]

> ***"In 2004, we project that about 52% of all email traffic (both corporate and consumer) will be classified as spam. This number is expected to skyrocket to 74% by 2008."***
>
> Source: "Anti-Spam Market 2004-2008" THE RADICATI GROUP, INC., April 2004

Certainly, all employees within an organization are concerned about spam and viruses affecting their ability to work effectively. However, typically it is the sole responsibility of **IT departments** to keep the network running smoothly and efficiently. With the increased pressure on cost-cutting in recent years, it has become a top priority for IT organizations to ensure network and employee productivity. For example, 99% of organizations currently use anti-virus applications.[8] While the deployment of anti-spam tools is not as high as those for anti-virus, most organizations have begun to tackle the spam problem as well.

An important element of an email infrastructure is the archiving system which also needs to be relatively low-cost and efficient to use—especially given the important role that archiving plays in compliance.

More difficult challenges related to maintaining the *value* of email are those of compliance and information protection. **Dealing with network and productivity issues frees the organization to more effectively address challenges relating to compliance.**

[4] Source: "Anti-Spam Market 2004-2008" THE RADICATI GROUP, INC., April 2004
[5] Source: "Anti-Spam Market 2004-2008" THE RADICATI GROUP, INC., April 2004
[6] Source: "Anti-Spam Market 2004-2008" THE RADICATI GROUP, INC., April 2004
[7] Assumes loaded labor rate of $80K per employee and a 37.5 hr work week.
[8] Source: 2003 CSI/FBI Computer Crime and Security Survey

3.2 Corporate and Regulatory Compliance

With the recent rise in public attention given to government regulations such as Sarbanes-Oxley and Health Insurance Portability and Accountability Act (HIPAA), the term 'compliance' typically evokes a sense of dread regarding looming deadlines and complex process improvements. However, 'compliance' can also be associated with adherence to everyday corporate email policy. Many of the challenges—at least from a technical perspective—are very similar. In either case, organizations must strike a critical balance between easy, low-cost email communications and the strict enforcement of policies relating to corporate and regulatory compliance.

As a critical element in most business processes, email inherently plays a role in compliance. Unlike the challenges relating to network efficiencies that are the sole responsibility of IT departments, achieving compliance affects many levels within the organization. Interestingly, many of the concerns around corporate compliance are driven by **Human Resources,** as these relate to offensive language and personal privacy protection. Issues relating to regulatory compliance are typically of interest to the **CXO community, Finance and Legal.** To bridge the issues relating to corporate or regulatory compliance, many organizations are specifically hiring **Privacy or Compliance Officers.**

Ultimately though, if a breach or violation occurs, it may be the CEO who is asking the critical questions relating to compliance. Do the stakeholders in the organization have the answers? And more importantly, what could it cost them if they don't?

In the event of a breach, the CEO may ask:

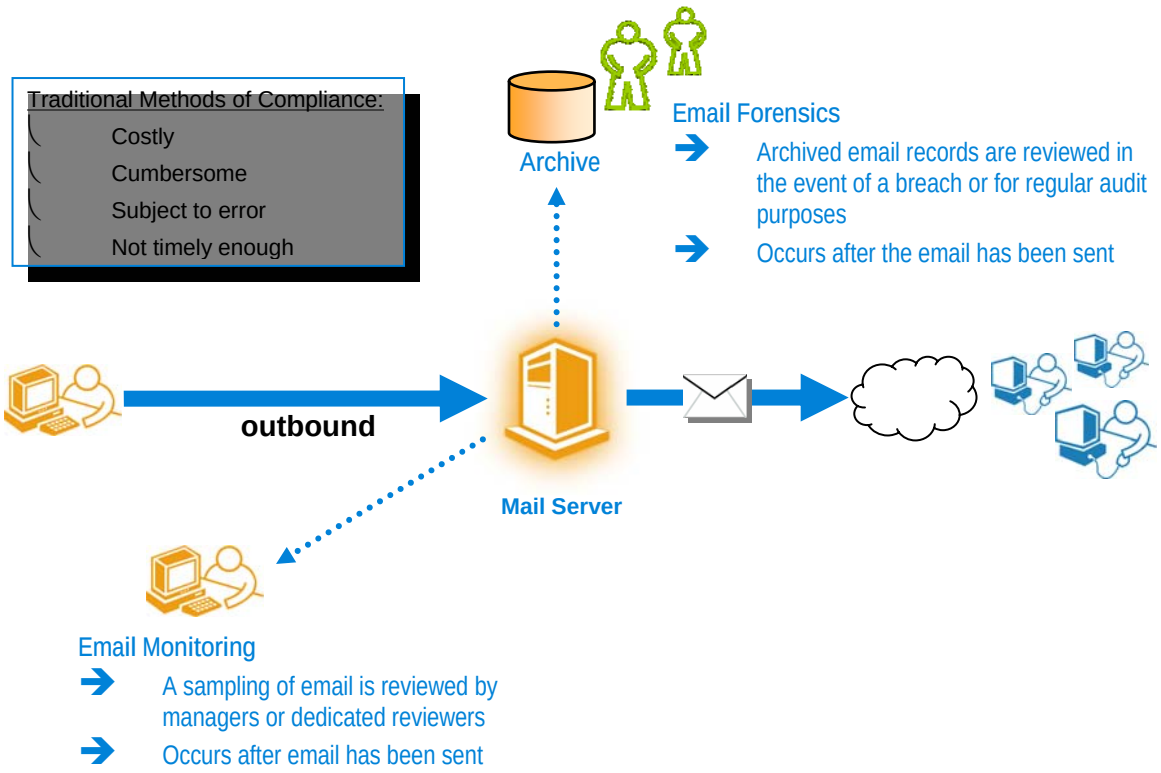
- Why didn't I know about the email?
- Who sent the email?
- Why did we not stop that email?
- Who keeps track of the email?
- Why are we allowing intellectual property to leave via email?
- Who emailed the classified document?
- What are we going to tell the regulators?
- What will this mistake cost us?

The Costs of Compliance

A critical element of achieving either corporate or regulatory compliance is the ability to monitor email traffic so that any risky email messages can be managed. Traditional methods for addressing email monitoring are cumbersome and costly. Most large organizations employ staff to monitor outbound email, which can not only be costly, but is also subject to human error and the nature of probability. A large organization would need to spend about **$4 million per** year just to review 1 out of every 10 email messages per day[9]—how many times does the process miss the email that actually contained the violation?

In the event of a breach, or as part of a regular audit process, organizations must also be able to produce audit trails of communications found in the email archives. Email forensics can be costly and is subject to error, especially given the huge number of messages stored in the archives. Typically, most organizations archive *all* email messages including spam and non-business communications, making it much more expensive and cumbersome to perform email forensics.

Most importantly, manual email monitoring and forensics usually occurs ***after*** the damage has already been done! For example, even if the monitoring process has revealed an email containing private information that should have been protected, the email has already been sent, and hence the privacy violation has already occurred. In this example, the potential for regulatory fines or public embarrassment cannot be reversed.



[9] Assumes a large organization has 25,000 employees; assumes that someone reviewing email messages for compliance can manually scan 50 email messages per day; assumes loaded labor rate of $80K/employee

Corporate Email Policy

Organizations are facing new challenges as the use of email outpaces the use of the telephone for communicating information within the workplace or externally to customers and other parties. The persistence of email has both its pros and its cons. Certainly, the ability to store email messages can be attractive, as it provides both parties with a legal record of the communications. However, this can be problematic for organizations that are sensitive to potential HR issues or risks associated with a record of improper communications.

Top Concerns for Corporate Compliance:

- *IP protection*
- *Limiting of profane or harassing language*
- *Privacy protection*
- *Automatic policy enforcement*

Of particular concern for organizations, is not simply the drafting of policies that limit the use of profanity, harassing language or distribution of intellectual property and other sensitive information, but also how to **automatically enforce** these policies and educate users on the proper usage of email. Organizations cannot fully rely on users to enforce corporate policies, so there must be a mechanism in place to centrally define and enforce policy.

Perhaps one of the most infamous violations of corporate policy occurred when Eli Lilly sent out an email to nearly 700 Prozac®[10] users and accidentally addressed the users in the CC: line instead of the BCC: line, thus violating the company's published privacy policy.[11] The company will pay $160,000 in a multi-action suit, and is required to strengthen its internal privacy protections and have safeguards audited annually for effectiveness by an independent third party.[12] While the financial penalties may not seem overly severe, the brand damage has been irreparable as this has become a widely cited case study, and the annual audits are very costly.

A recent survey found that 25% of employers have fired employees for violating email policy, and 13% of employers actually had to go to court and battle an email related law suit.[13] Without an understanding of the corporate policy, or simply through human error, employees may be more likely to violate email policy and potentially expose the organization to a public embarrassment or security breach.

"Typically, it's a sexual harassment or a racial discrimination claim. Typically in a harassment or hostile work environment claim, there's an element of either off-colored jokes, sexual content, maybe even pornography."

Source: Nancy Flynn, the executive director of the ePolicy Institute, CBS Early Show, August 24, 2004

[10] PROZAC® is a registered trademark of Eli Lilly and Company.
[11] Source: http://www.e-health-insider.com/news/item.cfm?ID=98
http://www.ago.state.ma.us/sp.cfm?pageid=986&id=777
[12] Source: http://www.ftc.gov/os/2002/01/lillycmp.pdf
[13] Source: "2004 Workplace E-Mail & IM Survey" from American Management Association & The ePolicy Institute

Government Regulatory Policy

The incredible rise in the use of computer networks and email as a transportation medium has resulted in **increased availability of and access to personal and corporate information.** In light of this growing concern, governments around the world have been formalizing regulations that govern the use, storage and transmission of personal information via computer networks.

Organizations are also faced with an ever-growing pressure to comply with government regulations such as Sarbanes-Oxley, SB-1386, HIPAA and others. By not complying with these regulations, organizations can face not only **heavy fines,** and in some cases even **legal action** which can place executives in jail, but also potential **damage to their brand** and customer confidence. Given its importance to the organization, and due to the complexity surrounding regulatory policy, organizations cannot fully rely on users to protect the privacy or information and maintain compliance with regulations. As with corporate compliance, there must be a mechanism in place to centrally define and enforce policy to enable regulatory compliance.

Top Concerns for Regulatory Compliance:

- *Privacy protection*
- *Audit and reporting*
- *Automatic policy enforcement*

While certain regulations such as Sarbanes-Oxley apply to all public companies, most government regulations are industry-specific, and may vary by geographic region. There is, however, a common thread that runs throughout the industry-specific regulations pertaining to the privacy of personal and corporate information.

The following is a high-level overview of how significant government regulations impact the operations of public companies and key vertical industries:

Across Vertical Industries

Affecting all public companies—and with a significant deadline fast approaching—**Sarbanes-Oxley Act** is causing large companies to re-examine their internal processes and controls. Designed to help protect resources against loss, **Section 404** requires the safeguarding of the assets against unauthorized access. By November 2004, companies with valuations of $75 million or more must evidence that their internal controls and audit trails are sound and that their processes are capable of producing certifiably correct data. Organizations need to be able to access data (including email messages) in real time and produce proper sign-off audit trails, and the inability to comply can lead to serious financial penalties. For example, the Securities and Exchange Commission (SEC) recently fined Bank of America **$10 million** for its inability to respond to a disclosure request in a reasonable timeframe.[14]

*Major bank recently fined **$10 million** for its inability to respond to a disclosure request in reasonable timeframe*

Source: InfoWorld, June 11, 2004.

Another regulation affecting organizations across verticals is **California SB 1386**. In effect as of July 2003, all organizations doing business in California and holding personal information of California residents are subject to this regulation. Under this law, companies and government agencies are required to notify customers if their unencrypted **personal information** has been acquired by an unauthorized entity. When breaches occur, the organization is required to notify the affected customers, likely resulting in loss of trust, brand damage and expense. Although there are no directly legislated fines, violators are subject to class action civil law suits.

[14] Source: InfoWorld, June 11, 2004.

Interestingly, encryption is the "safe harbor," meaning that the notification requirements do not apply to encrypted data.

Financial Services

Organizations in the financial services industry are faced with a number of regulations regarding data privacy and security such as **Gramm-Leach Bliley**. Additionally, Sarbanes-Oxley and other regulations and requirements from the **SEC** and **National Association of Security Dealers (NASD)** place restrictions on what information can be released and how it is distributed. Ensuring compliance with this myriad of regulations significantly affects an organization's email policies and the resulting technology requirements. For example, financial services organizations need to be able to monitor email communications, perform silent audits, archive efficiently, control access to client information, maintain a record of brokerage transactions and more.

While sound policy is critical, automatic enforcement of the policy via a proven technology solution can help to enable compliance and reduce the risk of unpleasant legal penalties and brand damage resulting from violations.

Government

Government agencies often deal with the challenges of **privacy** legislation. Most users are not aware of how often they may be communicating privacy-protected information and are not sure how to protect it.

As agencies collect, transmit and store large amounts of personal and sensitive data, they are subject to a variety of restrictions on how that information can be released. Laws such as the **US Privacy Act, Canada's Privacy Act,** and the **EU Directive on Privacy and Electronic Communications,** are all designed to protect personal citizen information.

Legislations Affecting Email Compliance

- *Sarbanes-Oxley Act*
- *California SB 1386*
- *Gramm-Leach-Bliley Act (GLBA)*
- *Health Insurance Portability and Accountability Act (HIPAA)*
- *Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)*
- *EU Data Directive*

Healthcare

Healthcare organizations are required by privacy and security laws such as **HIPAA** to keep patients' electronic protected health information (ePHI) safe from unauthorized disclosure. In general, organizations must ensure the confidentiality, integrity, and availability of all ePHI throughout the data lifecycle and protect against reasonably anticipated threats to its security. Simultaneously, email is a vital productivity tool that speeds communication of important ePHI, as well as sensitive business information, resulting in better patient care and improved efficiency.

In summary, the number of government regulations that can affect an organization is rising. It can be very challenging to understand the impact of each regulation and how it affects an organization's various information technology systems such as email, and it is even more challenging to understand the aggregate view of all of these regulations and the overall impact on email risk management.

3.3 Message Security

Many of the concerns around corporate and regulatory compliance result in the need to protect sensitive or private information such, as the case with intellectual property or personal client information. Security becomes an essential element of managing the risk of communicating valuable information effectively.

Given its intrinsic association with the issues of compliance, email security and the protection of information is of interest to a broad range of individuals, most specifically, the **Chief Security Officer (CSO), CIO** and the security team.

So, how do organizations mitigate the risks associated with communicating sensitive information internally to employees or externally to customers and other parties?

Top Email Security Concerns:

- *Protection of sensitive or private information*
- *Creation of an audit trail of communications*
- *Monitoring of specific user behavior*

For some organizations, mitigating the risk associated with communicating sensitive information might simply mean protecting that information as it leaves the organization. However, organizations seeking better risk mitigation need to consider how to protect information at all times, or "end-to-end." After all, 80% of organizations list 'insider abuse of network access' as one of the top reasons for loss of proprietary information.[15] For an even higher level of risk mitigation, email messages can be protected in transit, and during storage on employee workstations or servers.

As email is the primary tool for collaboration and contains a record of important decisions, organizations are also concerned with message integrity and need to be able to assign accountability for email communications. And although most organizations don't like to talk about it, the security arm of most organizations needs a way to easily monitor individual email behavior.

Specifically, in order to protect information in an effort to comply with policy, organizations must:

- Restrict access to email messages to intended recipients
- Know whether or not the email contents have ever been changed
- Be able to bind the user to an email message
- Know that the email contents have been kept confidential

The most important element for implementing secure email is to ensure its ease of use. If it is difficult for users to protect information, the information will not be protected.

"The most-essential characteristic is ease of use. Even when the sender or the recipient is highly motivated to protect the information, if the system is so complex that it is perceived as interfering with the delivery or readability of the information, that system will not be consistently used."

Source: J. Graff, Gartner (IGG-08282002-02)

[15] Source: 2003 CSI/FBI Computer Crime and Security Survey.

4 Summary of Email Compliance Challenges and the Requirements to Address Them

So what is needed in order to address the challenges of network and productivity protection, corporate and regulatory compliance and security? Let us reflect on the major challenges that have been identified in order to best define the ideal requirements.

4.1 Spam Interferes with Management of Valuable Information

In order to maintain an efficient email system and protect employee productivity, organizations must find a way to help eliminate costly and annoying spam. Care must be given to selecting an **intelligent, efficient anti-spam solution** as organizations can find themselves spending an inordinate amount of time tuning the spam engine by updating word lists and rules, for example. By helping to reduce spam, organizations can better deal with the more critical challenges of compliance.

4.2 Manual Email Monitoring and Forensics is Expensive and Ineffective

Understanding the flow of information that enters and leaves an organization is a critical component of achieving compliance. To be effective in identifying potentially risky emails, and in an effort to reduce costs, organizations need **an automated way to scan all inbound and outbound email.**

4.3 Discovery *After* the Violation Has Already Occurred

Using traditional methods for email monitoring and forensics, discovery of a risky email message typically occurs after the email violation has already occurred. For example, finding an email in the archive that contains sensitive intellectual property or business-to-business communications is too late—the information has already been sent outside the organization, potentially placing the information at risk and the company at a competitive disadvantage. Organizations need a way to enforce policies in **real-time** and stop violations ***before*** they occur.

4.4 Archiving *All* Email Can Be Expensive

Most organizations simply archive ***all*** of their email. Given that over half of email traffic is junk mail, organizations are needlessly storing additional email messages, making it harder to find the valuable information if required. Organizations need a way to streamline the information that is archived, including the elimination of unwanted email and the **automatic categorization** of email messages for more efficient forensics in future.

4.5 Users Cannot Be Relied Upon to Understand and Enforce Policy

It is inconceivable that all employees in an organization would fully understand the corporate or regulatory email policies sufficiently to enforce them at all times. Users should be offered the option to enforce policy, however, organizations need a way to **automatically enforce policy** should a user forget or makes an error. Ideally, organizations also need a way to **subtly educate users** about the appropriate email guidelines.

4.6 Regulatory Policies Are Complex

Organizations can be subject to many government regulations, and understanding all of them in detail and at an aggregate level can be difficult. Organizations need an **easier** way to manage the many policies that are relevant to them.

4.7 Protecting Private or Sensitive Information is Difficult

To achieve compliance with any number of the corporate and regulatory guidelines, private or sensitive information needs to be protected while stored and in transit. The use of **encryption** is critical for restricting access to information and helping to maintain its confidentiality. **Digital signatures** are required to enable an audit trail for communications and to verify that the information has not been tampered with in any way. For maximum ease of use and improved compliance, the process of protecting information would be **automated**, although in some cases, allowing users the option to protect information may provide a greater level of security.

In Summary, Addressing Email Compliance Challenges Requires:

- **Intelligent, efficient anti-spam solution** to allow a focus on management of valuable email
- **Automatic scanning** of all inbound and outbound email to simplify and reduce the costs of monitoring for potential violations
- **Real-time policy enforcement** to stop potential violations before they occur
- **Automatic categorization of email messages** for more efficient archiving and easier forensics at a later date
- **Automatic policy enforcement** to alleviate reliance on end users to understand and enforce policies
- **Method to subtly educate users** about the appropriate email guidelines
- **Easier way to configure and administer the many policies** that are relevant to email within an organization
- **Automatic encryption** for maximum ease of use and risk management, with option for users to protect information

5 The Entrust Solution for Email Compliance

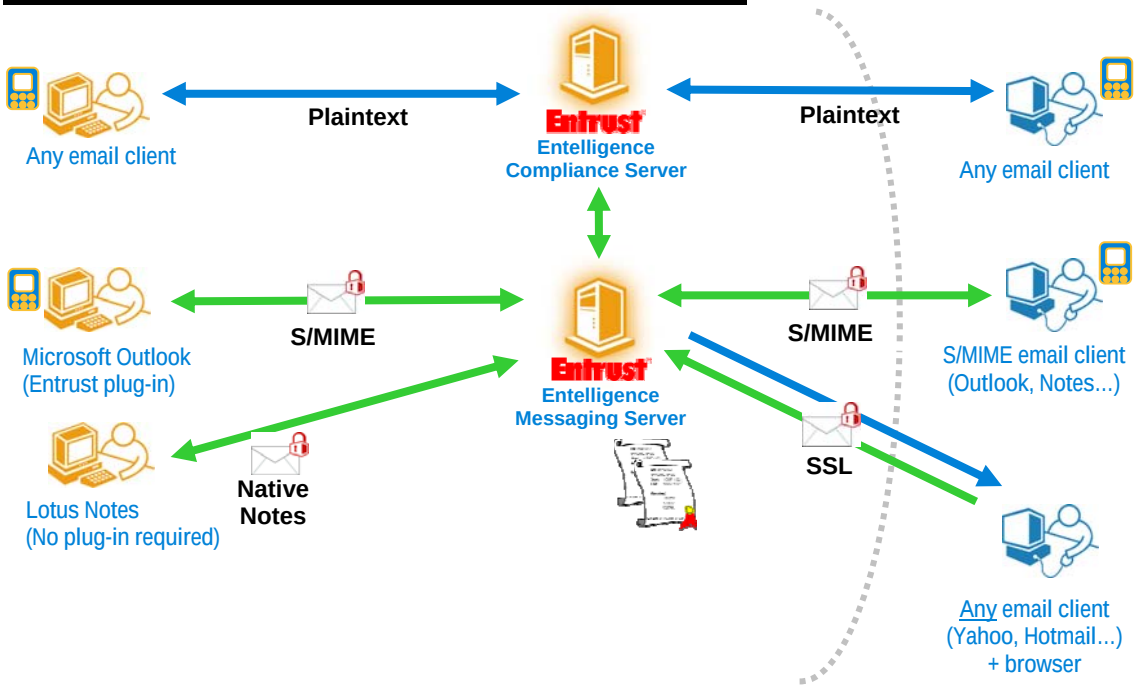
The Entrust Secure Messaging Solution is an integrated suite of components that can provide advanced content scanning of inbound and outbound email messages, centralized policy enforcement, automatic email encryption, support for mobile devices and more. The capabilities have been designed for large enterprises and government organizations needing to enforce corporate or regulatory compliance, protect their networks from unwanted spam or viruses, and mitigate the risks of communicating sensitive information.

A highly scalable, reliable and flexible solution, components can be installed standalone or as part of an integrated suite, making it easier for IT managers to add secure messaging capabilities to their existing email environments. Leveraging centrally defined policies and automatic enforcement of those policies—whether it be to reject spam, archive regulated information, bounce back emails with profane language or automatically encrypt emails containing intellectual property—the solution does not rely on users to enforce policy and provides the most comprehensive set of capabilities for customers.

By implementing the solution, customers can help avoid the penalties or brand damage associated with non-compliance and reduce the risks associated with communicating sensitive information while optimizing performance of their email systems.

Deployment Options:

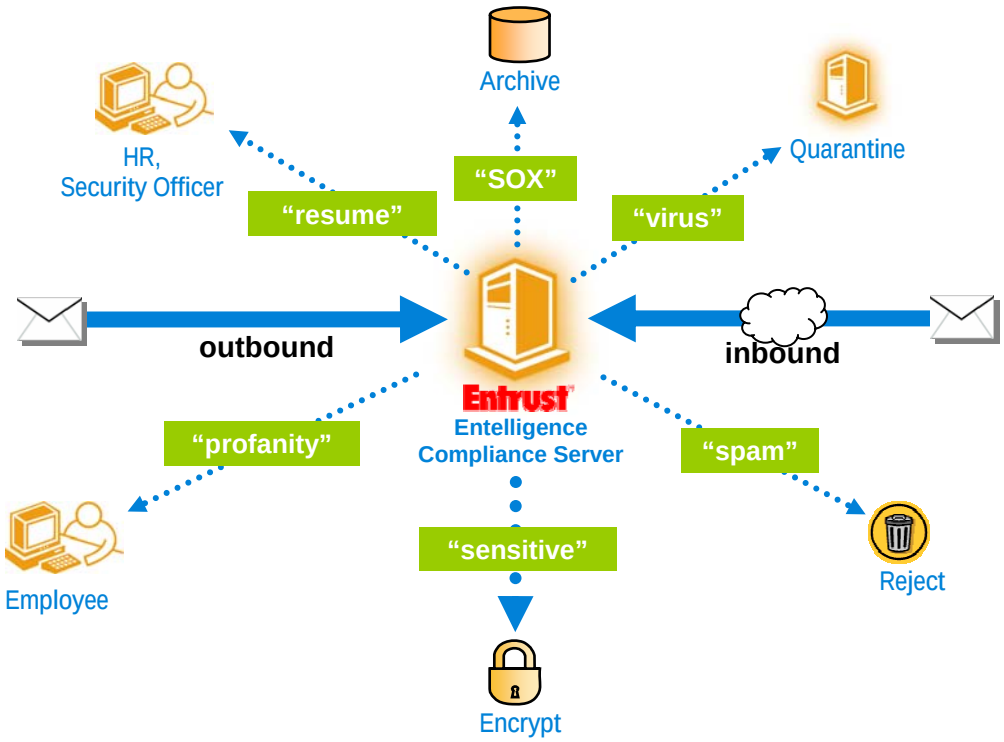
- Advanced content analysis for email compliance and anti-spam
- Boundary security (S/MIME and/or Web-based delivery)
- End-to-end security
- Mobile security



5.1 Advanced Content Scanning Capabilities

A critical component of the solution is the advanced content analysis technology. Available as a standalone appliance or as part of a comprehensive Secure Messaging Solution, the Entrust Entelligence™ Compliance Server analyzes all incoming and outgoing email messages and attachments, and then can automatically enforce policies according to the nature of the message. Unlike most content scanning solutions on the market that only look for a pre-defined list of words, that are often encoded as rule bases, the Entrust Entelligence Compliance Server is based on a patented approach with a structure extraction engine that can more accurately recognize the nature of the unstructured email messages and attachments based on their context and meaning.

This new technology combines many years of R&D advances in information theory and artificial intelligence and leverages both statistical analysis and bounded natural language processing (NLP). This capability can be used to better identify spam, valid business communications, sensitive communications, or messages that violate corporate or regulatory policies. Once identified, these messages can be rejected, forwarded to a compliance officer, quarantined, forwarded to a server for encryption or dealt with many other ways.



Unlike other products that require extensive creation of policies, the Entrust Entelligence Compliance Server uses predefined, robust policy modules pertaining to intellectual property protection, spam, privacy, profanity, regulatory compliance (including SOX, SEC, NASD, GLBA, HIPAA, PIPEDA) that are 'plug-and-play.' The policies can also be tailored to meet specific needs of the customer environment.

To get an understanding of the nature of email flowing in and out of an organization, customers may leverage the audit and forensics tools. These are also important for on-going monitoring of the system and for real-time information regarding email compliance.

5.2 Secure Email Capabilities

As discussed, protecting private or sensitive information is a critical element of achieving compliance. With a strong foundation in the area of security, and having provided secure email solutions since 1995, Entrust delivers a very robust, flexible set of tools for protecting information through the use of encryption and digital signatures.

Boundary Security

To make it easy to communicate securely with external partners and customers, Entrust provides a server-based email gateway called the Entrust Entelligence™ Messaging Server.

Key Features of Boundary Security:

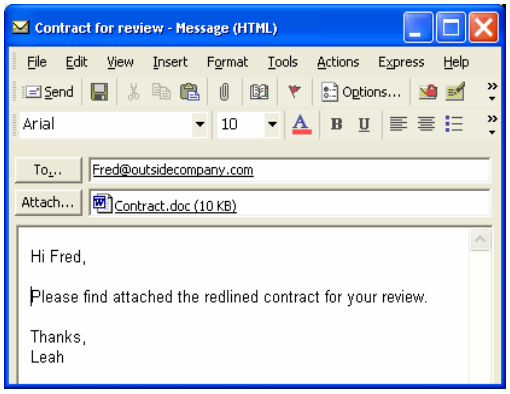
- Integration with content scanner for **automatic encryption** of "sensitive" messages
- Eases secure external communications
- No need to rely on user to enforce compliance
- Centralized policy enforcement
- Maintains end-to-end encryption
- Offers flexible delivery options

An important component of the secure messaging solution, Entrust Entelligence Messaging Server transparently manages security functions and can enforces corporate secure email policies, making it easier for users to securely communicate with their colleagues **outside the organization**. By enabling "end-to-end" or "boundary-only" encryption, the Messaging Server **helps to protect the privacy of sensitive communications**, and **enables an audit trail** for email communications.

Offering both standards-based S/MIME and Web-based options for message delivery, the Messaging Server can be used to **reduce the time and cost** of conducting a wide range of tasks, including the distribution of HR information, contract negotiations, personalized customer statements and more.

Desktop Security

Entrust seamlessly extends 'end-to-end' security to client-based email environments (i.e. MS Outlook, Lotus Notes), and is designed to meet even the most stringent of government standards (US Federal Bridge, PKITS, FIPS-compliant…). Through the use of an optional desktop plug-in, users can 'single-click' encrypt and/or digitally sign emails, helping to protect private or sensitive information.



Mobile Security

With so much sensitive information now making its way onto wireless devices, Entrust also provides solutions for mobile email security. Through a relationship with Research in Motion (RIM), Entrust provides optimized support for Java-based RIM Blackberry handheld devices. Using Entrust Entelligence Mobile Security, email can be protected on PocketPC, Palm and Symbian devices.

5.3 Business Value of the Entrust Secure Messaging Solution

Designed to help address the many challenges of compliance, the Entrust Secure Messaging Solution can provide significant business value to its customers. Most importantly, the solution can help improve customers compliance, helping to **avoid the costs** associated with defending a compliance violation, improper disclosure or loss of public trust through the use of:

- **Real-time corporate and regulatory policy enforcement**
- **Automatic protection of private or sensitive information**

And more specifically, the solution can help customers:

- Automatically scan emails for violations in real-time, avoiding the costs and risks associated with more manual, traditional compliance activities
- Enforce a robust set of policies automatically at the boundary, alleviating the need to rely on users for policy enforcement
- Automatically protect information using policy-based encryption at the boundary, helping organizations comply with regulations more easily
- Automatic categorization of email messages for more efficient archiving and easier forensics
- Mitigate risk by securing information, enabling real-time email monitoring, and protecting email on mobile devices
- Educate users on policy by sending messages back for 'reconsideration'

Additionally, the Entrust solution is designed to enable IT organizations to:

- Deploy content scanning quickly and more efficiently using an appliance platform and plug-and-play policy modules
- Reduce costs and increase productivity by eliminating spam, allowing the organization to focus on the management of valuable email and related compliance challenges

5.4 Unique Competitive Advantage

Most advanced content scanning technology

- Patented hybrid approach provides improved categorization of email leading to fewer false positives than other word and rule-based approaches
- Policies are defined using a concept-based approach, which leads to easier policy updates and customization, and a reduced cost of administration
- Fine-grained email classification can enables more efficient email flow and archiving
- Solution provides a variety of policy modules that can be used 'out-of-the-box' or tailored to an organization's corporate and regulatory compliance requirements

Most comprehensive secure messaging capabilities

- Seamless integration with MS Exchange and Lotus Notes environments
- Automatic encryption of sensitive data at boundary
- Flexibility to extend 'end-to-end' security to the desktop
- Mobile security for RIM Blackberry, PocketPC, Palm and Symbian

Delivered by a market-leader in security

- For over 10 years, Entrust has delivered security solutions to 1450+ customers
- Global organization with large, experienced Professional Services team
- Entrust is leading activities around ISG (Information Security Governance)

6 Conclusion

As organizations consider the challenges of email compliance, they must evaluate their own circumstances and evaluate the risks and potential financial impacts of non-compliance. While it may be difficult to consider how the wide range of corporate and regulatory policies affects email usage, it is a necessary step in achieving compliance. Due to an organization's heavy reliance on email as the primary collaboration tool, **email is inherently tied to policies that govern the protection of and access to private or sensitive information.**

Government regulations are on the rise and the penalties are real. Many are already in effect, and are soon joined by Sarbanes-Oxley Section 404 in November 2004, and the next round of HIPAA requirements in April 2005.

And, the challenges of compliance go beyond the well-publicized regulatory issues. With many employers firing employees for violating email policy and even going to court to battle email related law suits, it is clear that enforcing corporate policy is important.

While some organizations already have some form of email monitoring in place, it is typically cumbersome and fraught with risk. As a key element of compliance, organizations also need a way to automatically scan and monitor email traffic to identify potentially risky items.

As well, knowing that users cannot be relied upon to fully understand and enforce policy, organizations need a way to **automatically enforce corporate or regulatory policy**, including the automatic protection of private or sensitive information.

Entrust and its customers understand the challenges of email compliance. The Entrust Secure Messaging Solution can help to address these challenges using **advanced content analysis, centralized policy enforcement** and **automatic encryption of email,** allowing customers to improve compliance and mitigate the risks associated with defending a compliance violation, improper disclosure or public embarrassment.

7 About Entrust

Entrust, Inc. [NASDAQ: ENTU] is a world-leader in securing digital identities and information. Over 1,400 enterprises and government agencies in more than 50 countries rely on Entrust solutions to help secure the digital lives of their citizens, customers, employees and partners. Our proven software and services help customers achieve regulatory and corporate compliance, while turning security challenges such as identity theft and email security into business opportunities.