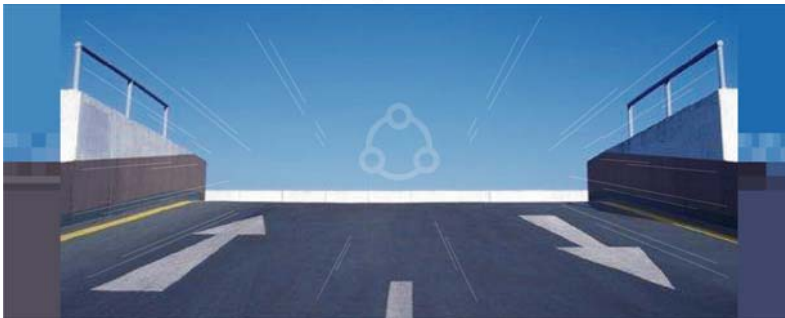


Entrust[®] Securing Digital Identities & Information



**Securing Your
Digital Life**

Best Practices for Choosing a Content Control Solution

March 2006

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

© Copyright 2006 Entrust. All rights reserved.

Table of Contents

1	Introduction	3
2	The Challenge.....	3
3	Addressing the Challenge: Steps for Practitioners.....	5
4	Meeting the Challenge: A 12-Point Checklist.....	6
	4.1 <i>Underlying Content Scanning and Analysis Technology.....</i>	6
	4.2 <i>Monitoring Versus Remediation of Compliance Solution</i>	6
	4.3 <i>Coverage of Traffic Types for Compliance</i>	6
	4.4 <i>Desktop vs. Server Solution</i>	7
	4.5 <i>Reporting/Auditing Capability of the Content Control Solution.....</i>	7
	4.6 <i>Encryption Capability and Selective Use of Encryption on Key Emails</i>	7
	4.7 <i>Control of Key Underlying Technology.....</i>	7
	4.7 <i>Ease of Use and Deployment: Set-up, Maintenance, Updates.....</i>	7
	4.9 <i>Integration with Back-end Systems</i>	7
	4.10 <i>Support.....</i>	8
	4.11 <i>Scalability.....</i>	8
	4.12 <i>Financial Health of Vendor</i>	8
4	The Entrust Solution	8
5	About Entrust	10

1 Introduction

Compliance continues to pose a strong challenge to the enterprise. Teams of people from within IT Security and Corporate and Regulatory Governance departments are responding to auditors, Chief Compliance and Security Officers as well as Chief Legal Council and CEOs. All public company executives are required by a variety of laws (depending on the industry sector in which they operate) to adhere to the Sarbanes-Oxley Act that was passed in 2002 in response to the Enron debacle¹. This act, commonly referred to as SOX, makes all public corporations accountable for the protection of customer and employee information including Social Security, credit card numbers and account numbers. Other regulations including the Federal Privacy Act and the Health Insurance Portability and Accountability Act (HIPAA) dictate that all Personal Identifiable Information (PII) as well as Personal Healthcare Information (PHI) must be protected². In some cases, this implies that sensitive data at rest must be encrypted and accessed only by persons in the enterprise who require access. There have been some very high profile cases of breaches of data at rest that have caused scrutiny and brand damage³. It also implies that sensitive data in motion or data that is being communicated via email, IM or even web email must be suitably protected and sent only to individuals who have a right to view it. There have also been significant breaches of such types of information, as in the case of a contractor at Blue Shield emailing himself 27,000 Social Security Numbers⁴ that were later found on his home computer.

This whitepaper aims to present some of the challenges and best practices associated with demystifying the process of addressing compliance from a regulatory and corporate governance perspective. Organizations are using a combination of processes and technologies to address the challenge posed by demonstrating compliance to auditors. As auditors review how regulations are being met with process and technology, it is important to review the available best practices.

2 The Challenge

When discussing compliance of electronic communications, there are a multitude of legislative and regulatory issues to consider. For example, financial institutions face well over a dozen compliance regulations. An enterprise that is regulated may have obligations such as, examining any outbound content whether it is through email, instant messaging, file transfer or web postings, and this can vary by industry, creating a complex overall set of policy objectives. In response, many organizations have established compliance and risk management teams focussed on electronic communications with Compliance Officers being asked to report to the CEO on any risks that affect operations.

Depending on the industry sector, an organization may be dealing with a number of compliance issues, including:

- √ Public-company regulations, such as Sarbanes-Oxley, established in response to the Enron debacle;
- √ Regulations affecting financial companies (such as banks and brokerages) that have to adhere to Securities (SEC) rules, Graham-Leach Bliley (GLBA) and NASD;
- √ Regulations affecting healthcare privacy information, such as Health Insurance Portability and Accountability Act (HIPAA); and

¹ A copy of the Sarbanes-Oxley Act and FAQ is available at the securities exchange website. Refer to <http://www.sec.gov/divisions/corpfin/faqs/soxact2002.htm>

² A detailed description and FAQ about HIPAA is available off the Department of Health and Human Services Website at <http://www.hhs.gov/ocr/hipaa/>

³ http://news.com.com/Bank+of+America+loses+a+million+customer+records/2100-1029_3-5590989.html

⁴ <http://www.bradenton.com/mld/bradenton/news/local/13887977.htm>

- √ Intellectual property law, which is important for information asset protection particularly for those organizations in the Pharmaceutical and Technology industry.
- √ Regulations affecting the privacy of information, including personal identification information, such as PII information regularly collected from employees, customers and end users.
- √ Corporate Governance Policies, including disclosures to Boards of Directors and Auditors as well as Human Resources, Governance, Harassment and Code of Conduct and Ethics policies.

While compliance and risk management teams are trying to solve their online information transfer problems, it seems that there is a backlash building against the term "compliance." Vendors have been rushing to provide one-size-fits-all solutions for the many regulatory and governance requirements in the enterprise. However, in their drive to create the perfect solution, many vendors have lost sight of customer needs and end users have become confused about compliance requirements. This whitepaper aims to assist the enterprise in choosing a content control solution best suited to their regulatory requirements.

3 Addressing the Challenge: Steps for Practitioners

With the many products available in the marketplace to address regulatory and corporate governance requirements, and the confusion that appears to have been created with the number of vendors competing to deliver the ultimate one-size-fits-all compliance solution, enterprises are unsure of where to begin in addressing their requirements. Here are five key steps to keep in mind:

1. Create a Task Force of Key Stakeholders

The key to finding the right solution for an organization is to first pull together the key stakeholders to determine the many requirements and policies that need to be satisfied. Key stakeholders from individual business units, the regulatory or compliance team, the legal team, human resources and executive team members need to outline their concerns to determine the organization's overall policy requirements. Many legislated enterprises already have such task forces set up and have spent time enumerating the regulatory and corporate governance requirements.

2. Detail the Organization's Requirements and Policies

With the stakeholders' input as the basis for the organization's requirements, a list of regulations, corporate policies and guidelines should be created. If it is found that new policies and guidelines are required, they should be created and documented to ensure that the information is communicated clearly to the employees that are affected by the policies. For well-understood regulations and corporate governance policies, the team should determine what processes are used to meet the policies and what possible technologies may be required. These could include technologies such as content filtering and control, encryption, access controls, authentication, etc. The processes may include identifying the groups of people and their roles in the compliance process and requirements for access to the sensitive information. Identified groups may include insiders, auditors, etc.

3. Determine Technology Requirements and Select a Group of Vendors to Review

Once the policies for compliance are enumerated, the processes requiring the humans in the loop and technology requirements are identified, vendor lists can be formed. Vendors will likely provide various solutions and not all are easily compared. It may also be necessary to combine vendor solutions to get full coverage. For example, not all vendors address encryption requirements but some encryption vendors can work with other content control solution providers. The selection of vendors is very important to ensure that a comprehensive solution is chosen. Conduct research on the Internet and invite vendors to give presentations and demos. More importantly, ask for referrals from other organizations in the same sector that have already deployed a compliance solution. Finally, select a group of vendors—typically five to ten—and begin the interview and selection process.

4. Select the Solution

Review the myths associated with content control for compliance for key takeaways⁵. For a good solution, an enterprise should be looking for:

- Advanced pattern-matching technology, possibly through a hybrid solution: contextual analysis vs. only exact keyword list matching; exact matching through monitoring of packets or rules-based pattern matching solutions;
- Ease-of-use and maintenance: with easily updated modules or templates, easy deployment and a highly scalable solution that integrates with other technologies including encryption;

⁵ Entrust Whitepaper: Myths and Realities in Content Control for Compliance, February 2006 available at www.entrust.com.

- A vendor with strong financial health that is likely to be able to provide continuous 24x7 support services.

5. Monitor the deployed solution and its effectiveness - Remember that Compliance is a process that requires user education, technology, and continual process improvements

Once a technology solution has been selected, it needs to be integrated into the process of compliance within the enterprise, and that involves individuals who can ensure that the solutions meet expectations, that end users are trained and that auditor requirements are being continually fed into the compliance solution.

4 Meeting the Challenge: A 12-Point Checklist

The following checklist can be used as a guideline by the team responsible for selecting a content control solution. Using this checklist, the team should be able to quickly assess a vendor solution and compare its capabilities across vendors.

4.1 Underlying Content Scanning and Analysis Technology

This is a key area of comparison that can help to identify which pattern matching technology is being used:

- a. Are emails matched against only a list of keywords (sometimes called “dirty words”)? Who makes up the list? Note that the English language has 250,000 words with 20,000 in daily use so this is not the most tractable approach.
- b. Are emails analyzed against only a list of rules (e.g. {if you see the word “patient disease is AIDS” then email is sensitive and quarantine it})? Again, this would require somehow encoding the 250,000 words in the English dictionary and any exceptions. The rules and exceptions will be difficult to maintain.
- c. Are emails analyzed against a set of related concepts or patterns in a library (if the concept “patient illness”, and the concept “AIDS”, and the concept “disclosed” then email is likely sensitive and ask user to reconsider)? Can concepts be easily re-used? Concept libraries are new and encapsulate the 250,000 words in the dictionary into a more manageable set of relevant concepts.

4.2 Monitoring Versus Remediation of Compliance Solution

- √ Does the solution offer extensive actions or remediation in the case of non-compliance, such as quarantine, forward to compliance officer, reconsider or audit?
- √ Does the solution offer monitoring only with no remediation? Most organizations will need some form of remediation even if it is based on monitoring, auditing and reporting. Others will need to offer quarantining and review.

4.3 Coverage of Traffic Types for Compliance

- √ What communication traffic types are covered and what analysis capability is possible given the nature of the traffic content?
- √ Can the solution review email, instant messaging, web and file transfer content? How accurate is that analysis?
- √ How does it compare in its analysis to other solutions? As more organizations use IM, web, file transfer, in addition to email, this becomes an important question in relation to outbound content control.

4.4 Desktop vs. Server Solution

- √ Is the solution primarily desktop-based, with limited central management capabilities?
- √ If the solution is desktop-based, how are compliance policies synchronized across desktops?
- √ If the solution is server-based, does it provide central policy management capabilities? Large organizations with thousands of desktops will likely prefer a server-based solution to help reduce deployment maintenance costs.

4.5 Reporting/Auditing Capability of the Content Control Solution

- √ Does the server have a daily, weekly or on-demand reporting capability?
- √ Can the reports be taken to an off-board database? Reporting is an important aspect for compliance teams and auditors who review various processes.

4.6 Encryption Capability and Selective Use of Encryption on Key Emails

- √ Does the solution integrate with encryption capability?
- √ Can a sensitive email be encrypted before it leaves the organization?
- √ Can encrypted emails be delivered to public email addresses for third parties (contractors, practitioners, etc.)? Sensitive information should be encrypted. This is a key regulatory requirement for email use, especially in financial and healthcare contexts.

4.7 Control of Key Underlying Technology

- √ Who controls the underlying pattern matching or encryption technology?
- √ How will a third party affect responsiveness in terms of customer support? Some vendors OEM parts of their solution from other vendors, while others own the underlying technology. This is typically true for the underlying content analysis or encryption technology used within a compliance solution.

4.7 Ease of Use and Deployment: Set-up, Maintenance, Updates

- √ How hard is it to set up the solution?
- √ Are there compliance pattern templates or modules for various regulations provided? Who creates them? How often are they updated?
- √ How fast can an organization be set up? How easy are the templates to maintain? Are there useful tools provided? Some solutions are very high maintenance while others are not. This will affect the load on the IT and compliance teams.

4.9 Integration with Back-end Systems

- √ Is the solution integrated with a back-end compliance solution?
- √ Can the content control meta-tags be generated for emails or electronic communications or be re-used for categorization or search on a back-end solution? Most regulated organizations also run email archives and document repositories for records management purposes. It is important to ensure that such components leverage the tagging or categorization from the real-time solution for e-discovery and litigation response.

4.10 Support

- √ What levels of customer support does the vendor offer? In some cases 24x7 will be essential.
- √ Is the support outsourced or native to the vendor organization? Some vendors do not have adequate support services in place. This should be a key requirement to enable consistent monitoring of sensitive information.

4.11 Scalability

- √ How scalable is the vendor solution?
- √ Has it been tested for millions of emails a day?
- √ How well does it perform at full load?
- √ How is it architected for distributed sites? Some vendor solutions have been tested for hundreds of users, not thousands of users generating millions of messages a day. Deploying non-scalable solutions in complex environments delays and frustrates IT and compliance teams.

4.12 Financial Health of Vendor

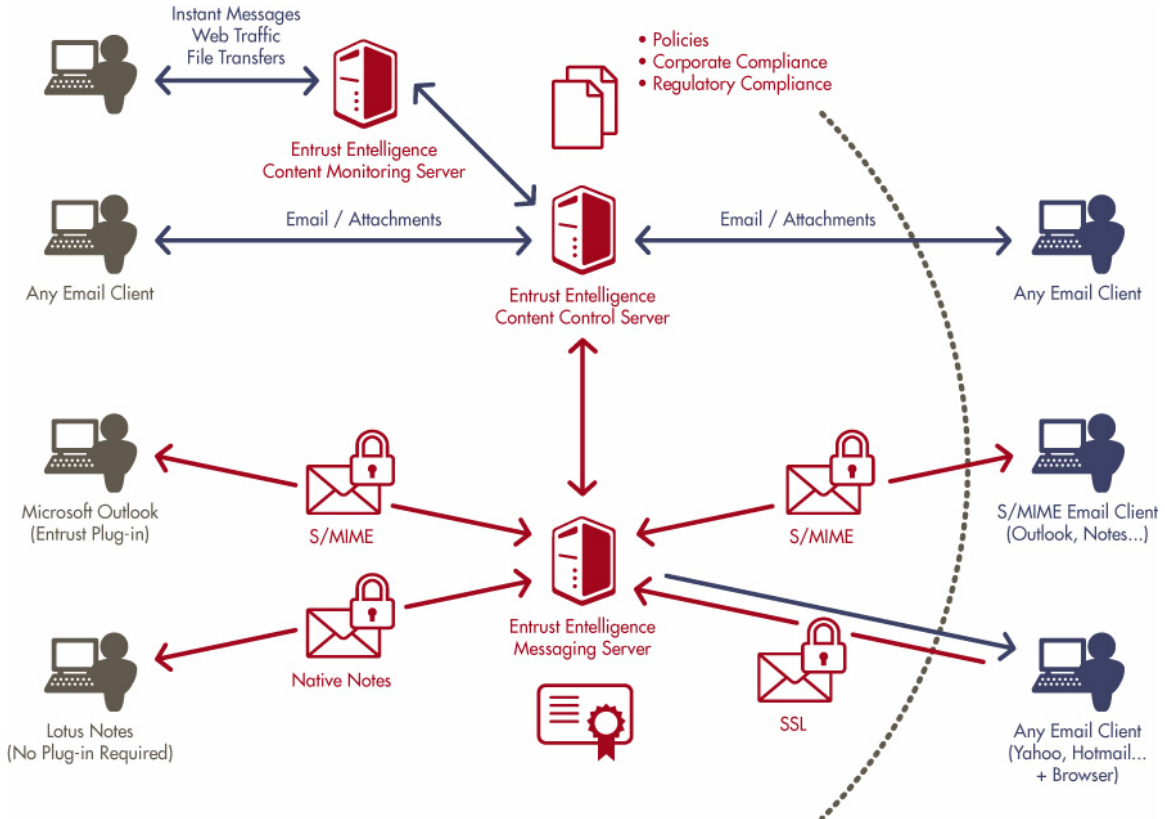
- √ How many years has the vendor been in business?
- √ Are they public or private? How well funded are they? Will they be in business for many years to come? As the technology industry shifts rapidly, so will vendors. Longer standing vendors are the better choice for compliancy requirements that require audit trails that range from a minimum of 5 years to decades.

4 The Entrust Solution

The Entrust Content Control and Secure Messaging Solutions offer a comprehensive solution with an integrated suite of components that can provide advanced content analysis of inbound and outbound messages, centralized policy enforcement, automatic and content-based email encryption, support for mobile devices and more. The solutions can also be set up to monitor in real-time email, instant messaging, web traffic and file transfers. The capabilities have been designed for large enterprises and government organizations needing to enforce corporate or regulatory compliance and mitigate the risks of communicating sensitive information for thousands of users sending millions of messages a day.

The Entrust Secure Messaging solution can also be used in forensic or real-time mode, assisting an organization in their e-discovery activities as well as offering a solution for immediate tagging of archives for discovery requirements and auditors.

Pre-defined or custom policies offer organizations the choice of subscribing to “plug-and-play” policy modules for: **Corporate Governance** (privacy of customer and employee information, detecting harassment, offensive language, IP protection) and **Regulatory Compliance** (Sarbanes-Oxley, Securities Rules, NASD rules, Graham-Leach-Bliley – GLBA, Healthcare Portability and Accountability Act - HIPAA, etc.). Leveraging automatic enforcement of those policies—whether it is to block non-compliant communication, archive regulated information, bounce back emails with offensive language for reconsideration or automatically encrypt emails containing sensitive content or intellectual property—the solution does not rely on users to enforce policy and can provide a comprehensive set of capabilities that can be tailored for customer environments.



To learn more about the Entrust Solution for Content Control and Secure Messaging, please visit <http://www.entrust.com>.

5 About Entrust

Entrust, Inc. [NASDAQ: ENTU] is a world-leader in securing digital identities and information. Over 1,500 enterprises and government agencies in more than 50 countries use Entrust solutions to help secure the digital lives of their citizens, customers, employees and partners. Our proven software and services help customers in achieving regulatory and corporate compliance, while helping to turn security challenges such as identity theft and e-mail security into business opportunities.