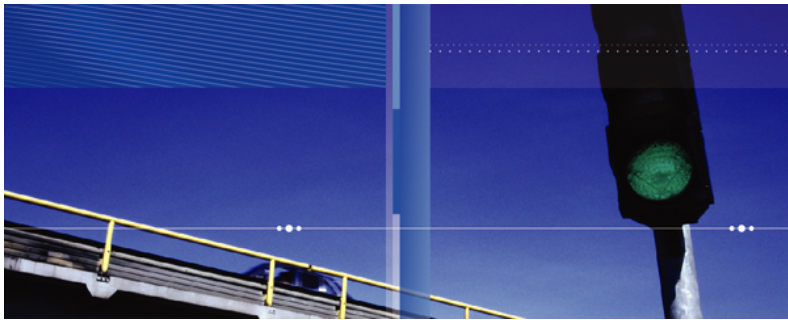


Entrust[®] Securing Digital Identities & Information



**Securing Your
Digital Life**

Encrypting Email with Your Eyes Closed

The Benefits of Next Generation Boundary Email Encryption for IP Protection and Compliance

November 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

Introduction	3
Why Secure Email?	3
Protect Brand Equity	4
Practice Good Corporate Governance.....	4
Mitigate Risk and Achieve Regulatory Compliance	4
Meeting the Needs of Your Different Messaging Environments	5
Internal Communication Between Employees (Enterprise)	5
Communication With Partners (B-to-B).....	5
Communication With Consumers or Citizens (B-to-C).....	6
Risk Mitigation vs. Productivity—Automation is Key	6
Ease of Use and Administration.....	6
Interoperability.....	7
Requirements Based on Messaging Environment.....	8
Choices for Securing Email	9
End-to-End Desktop Email Encryption Solutions.....	9
Boundary Email Encryption Solutions.....	10
Secure Web Mail Solutions.....	11
<i>Benefits of Secure Web Mail Delivery</i>	12
Options for Setting-up A Secure Email Infrastructure.....	12
Entrust Boundary Email Encryption: A New Approach	14
Entrust Entelligence Messaging Server	14
<i>Features and Benefits</i>	14
<i>Deployment Flexibility</i>	15
<i>Options For Enabling Email Encryption Within Your Organization</i>	15
The Benefits of Entrust Entelligence Messaging Server.....	17
The PKI Alternative: End-to-End Email Encryption	20
Managing Digital Identities & Encrypting Messages for External Recipients	20
The Need to Act Now	22
About Entrust.....	22

Introduction

With the increasing number of disclosures of poor corporate governance practices throughout corporate America, organizations are taking greater notice of the flow of communications in and out of their networks. Email is the lifeblood of the organization, but can expose it to the very serious risk of information breach, not to mention potential fines for non-compliance with the growing number of information security and privacy regulations. Email encryption is still the best technology defense against unwanted disclosure of sensitive communications, and the great news is, security software vendors have been working hard to make it easier for organizations to implement. No longer reserved for only the most secretive of businesses or government departments, email encryption is now readily available for businesses of all kinds to enable encryption across their communications (both internally and externally with third party recipients) without relying on users to understand cryptography or take responsibility for security practices.

"Messaging security spending will increase from \$919 million in 2005 to \$2.8 billion in 2010 representing a 25% CAGR."

Source: IDC "Worldwide Secure Content Management 2006 - 2010 Forecast", # 203550, Oct 2006.

According to Forrester Research, *"Organizations are moving beyond malicious code protection to deploy technologies that protect against the loss of confidential information, help enforce compliance with appropriate use policies, and encrypt email."*¹ So grab a coffee, sit back and read this white paper to learn how the next generation of **boundary email encryption** and advanced content control solutions can monitor for sensitive data and apply encryption to the email communications in your company—even with your eyes closed.

Why Secure Email?

The benefits of email communication are numerous and widely recognized, but because of its vast size and reach, many people have a false sense of security with respect to email—and think that a breach could never happen to their communications. Due to this false sense of security, individuals within organizations exchange sensitive information online without giving it a second thought—but at what potential cost to your organization? According to a survey conducted by Osterman Research, *"83% of organizations believe that most sensitive information leakage is accidental, due in part to employees simply not knowing the policy or not realizing the information they are sending is sensitive."*²

Secured email can provide not only peace of mind for privacy protection, but also productivity enhancement by enabling organizations to move more sensitive and higher value transactions online, as well as enabling electronic delivery of regular communications with customers and partners (such as billing and account statements, insurance claims and application processing documents). Messages that were previously limited to more traditional methods of communication such as fax or postal mail due to concerns about information security can now be moved online with a similar level of assurance of confidentiality as before. However, in order to mitigate risk while helping to enable new and higher sensitive communications online, security and trust are essential. Unauthorized access to customer account information, client records, sales forecasts, intellectual property or other valuable information can do significant damage to an organization's brand and competitive position. And—with the recent expansion of government and industry regulations such as Sarbanes-Oxley, HIPAA and PCI, the need to secure email communications has become an important element of corporate compliance. The ability to secure email

¹ Forrester "You've Got Mail: 2006 Messaging Security Adoption", Natalie Lambert, April 26, 2006

² Osterman Research / Entrust "Sensitive Information Leak Survey", November 2005.

communications will not only help protect and build a company's brand equity, but can also help to strengthen relationships with its suppliers, partners and customers—all while helping to contribute to good internal controls and compliance with government regulations surrounding the protection of information privacy.

Protect Brand Equity

Examples abound of both private and public organizations whose brand and reputation has been tarnished by the exposure of sensitive information that was contained within unprotected emails sent over the internet or found on stolen laptops. Credit card databases, personally identifiable citizen information and intellectual property have all been mentioned in the media in recent unwanted disclosures. An email encryption solution can help to prevent such losses.

Practice Good Corporate Governance

With the current focus on good corporate governance practices, notably in Sarbanes-Oxley Section 404, organizations must consider secure email as a means to address internal controls for data access and data integrity. Email encryption can be used to avoid security breaches and to provide transaction integrity.

Mitigate Risk and Achieve Regulatory Compliance

Heightened regulatory requirements are forcing businesses and governments to protect communications containing confidential information. Global awareness about information privacy has resulted in numerous privacy-related regulations such as HIPAA, Gramm-Leach-Bliley, and California SB-1386 in the US, PIPEDA in Canada, and the European Data Directives in Europe. Furthermore, the Payment Card Industry (PCI) Regulations stipulate the need to protect access to cardholder data both at rest and in transit. Several of these privacy regulations specifically refer to the need for email encryption as a means to protect the privacy of customer data and some prescribe regulatory penalties for non-compliance. Through every new publicized incidence of breach, people become more knowledgeable about the risks of doing business online, and they begin to place greater emphasis on mitigating risk with tighter security practices. ***Encryption can significantly reduce the risks of exposure and tampering with sensitive information as it is exchanged or stored within email systems.*** In addition to these factors, a number of other key drivers are encouraging organizations to deploy email security solutions:

- **Competitive pressures** are forcing organizations to accelerate business processes through the rapid exchange of sensitive and/or high-value information.
- **Market pressures** are rewarding organizations with tighter supply chain relationships that are being enabled with secure email-based collaboration.
- **Consumer pressures** are forcing organizations to enable the ability for secure online communications with their customers, who are increasing their use of the Internet for online services such as banking, insurance and government services but are painfully aware of the threat of identity theft.
- **Time-to-market and cost pressures** are forcing organizations to use email to replace more expensive communication methods such as courier, long distance telephone and fax, typically used for sensitive and high-value communications such as contract negotiations.
- **Public concern** over identity theft and data privacy is mandating organizations to protect sensitive customer information and take measures to prevent its loss or compromise.

Meeting the Needs of Your Different Messaging Environments

Generally speaking, messaging environments can be broadly classified by the nature of the exchange—*internal* or *external*—each with its own unique set of requirements and challenges when deploying security. Furthermore, email is not the only form of electronic communication medium available to employees. Instant Messaging (IM), web based email and FTP are also easily accessible means of sending and receiving email and attachments, and also need to be secured. In the past, organizations were often forced to make compromises in the security requirements across the needs of these various environments. Today, however, Entrust can address the needs of each of these groups with one boundary email encryption solution that will be discussed later in the paper.

For the purpose of painting a full picture of the various communication requirements of a comprehensive email security solution, we will address the unique needs of each of the following messaging environments:

- Internal Communication Between Employees (Enterprise)
- External Communication with Business Partners (B-to-B)
- External Communication with Customers or Citizens (B-to-C)

Internal Communication Between Employees (Enterprise)

Email generated by day-to-day communications between employees within an enterprise constitutes the vast majority of communications. These internal messaging environments tend to be relatively homogeneous and are usually based on a single email infrastructure, such as Microsoft Exchange or Lotus Notes, although many companies must manage multiple messaging platforms as a result of consolidations, mergers, acquisitions or local/regional IT deployments. The requirement for security is often departmentalized in areas such as Legal, R&D, HR and Finance, or at the Senior Management level, where highly confidential information is frequently exchanged.

Some of the key characteristics of an enterprise messaging environment are as follows:

- Email is a primary tool for collaboration
- The majority of email is exchanged **within** the enterprise
- Email reach is expanding to the mobile workforce through the use of email-enabled wireless devices
- Employees often have to **work offline** with email via mobile devices
- Security is provided as an extension to the existing email infrastructure—usually via Secure Multipurpose Internet Mail Extensions (S/MIME)
- Instant Messenger applications such as MSN IM, if enabled within an organization, are widely used by employees to discuss both work and non-work related topics, and even to exchange file attachments

Communication With Partners (B-to-B)

Inter-organizational email is growing rapidly as organizations exploit the business advantages of fostering closer relationships with their customers, partners and suppliers. In this type of exchange, we are more likely to encounter a heterogeneous environment where organizations are communicating between two interoperable, yet different email infrastructures. Typically these environments can be characterized by the following points:

- Information exchanges are between individuals collaborating to accomplish a specific goal, and flow both ways
- The partner has an existing email environment that they are not prepared to change
- Web mail access to the email environment may be an option used by the partner company
- Both parties have a vested interest in securing their information exchange
- Security is dictated by standards-based protocols that are mutually supported by each organization's email infrastructure (primarily S/MIME)

Examples of this type of information exchange are wide-ranging, covering service contracts, financial auditing, legal counseling and management consulting to more cooperative ventures like joint design and development, organizational mergers or inter-governmental collaboration.

Communication With Consumers or Citizens (B-to-C)

Email environments in which businesses or government departments are communicating with their customers and citizens exhibit yet another set of characteristics. In this type of environment, the technology used for communication is **fragmented**, with the lowest common denominator being a basic Web browser. From a secure messaging perspective, this environment is further characterized by the following points:

- Secure email communications flow is often **one-way**, such as electronic statements being pushed out via email from the organization to the individual for 'read-only' access
- The onus for security is placed primarily on the organization as a 'caretaker' of the confidential client information
- The communication is between the organization and the individual only
- Security is governed by the lowest common denominator—generally Secure Sockets Layer (SSL) / Transport Layer Security (TLS)—via protected Web-based email applications

Risk Mitigation vs. Productivity—Automation is Key

Regardless of the types of messaging environments in use, for email to succeed as a medium of communication for sensitive information, it must have security capabilities that are comparable to those provided in the meta physical world. However, **security functionality by itself is not enough**—users must actually 'use' it. While a Compliance Officer or Chief Security Officer (CSO) is naturally most concerned about mitigating exposure to risks or non-compliance, they must also uphold the productivity of the organization. To remain successful, security must be easy-to-use and seamless/interoperable with the messaging environments of desired recipients, so that users do not have to change the way they work to securely collaborate and exchange information. They must not be required to understand the inner workings of email security or even make decisions about *what to encrypt*, and *when, or for whom*.

Ease of Use and Administration

Ease-of-use poses a significant potential barrier to securing email. If security cannot be applied easily and transparently for end users, they will most likely circumvent the policy. From the user's perspective, ease-of-use can be simply defined as, **"requiring no more effort to send a secured email than is required to send a regular email."** However, from an organizational perspective, ease-of-use has a different meaning. An email security solution should be easy to configure and deploy and easily support mobile workers, for whom off-line use and limited bandwidth connections are common. When considering the external parties that an organization is dealing with, an email security solution should not require customers or partners to install new software, change a customer's or partner's email behavior or interfere with their own security

systems or their ability to delegate to co-workers, the right to read and respond to emails. Users should also be able to establish secure communications with recipients without requiring administrator intervention.

Interoperability

One major challenge for a secured email is interoperability. If the security provided by one infrastructure or email client is not interoperable with another email client or infrastructure, secure messages cannot be exchanged. This can either pose a barrier to collaboration or, even worse, drive users to exchange information without security at all. Although it is fairly straightforward to achieve interoperability *within an organization* where there is some level of control over the types of systems deployed to users' desktops, the same cannot be said when communicating with external third parties such as customers or business partners. Reaching consensus among supply chain partners on a non-standards-based security scheme can be extremely difficult. Using a non-standard approach often locks all participants into a particular vendor contract and limits ongoing flexibility to adapt to changes in either organization's networking environment.

When analyzing the market acceptance of security protocols, research indicates that no single lowest common denominator exists for all types of messaging environments. When communicating between organizations, S/MIME or OpenPGP seem to be the preferred protocols, whereas SSL or TLS seem to be the most widely accepted approach when communicating with consumers or citizens. Both SSL and TLS are the fastest growing means of widespread email access for corporations, who often provide web-based email access options to augment their S/MIME or OpenPGP email application environments. Unless you are willing and able to insist that your customers and partners switch to an email solution that supports your chosen standard, or change their email behavior, finding a single interoperable delivery mechanism can be a challenge. Whatever solution you choose for securing your email, it should be flexible enough to support alternative delivery methods that will meet the needs of your diverse recipients.

Requirements Based on Messaging Environment

While the types of challenges facing email security systems can be easily categorized, key requirements differ significantly depending on the type of messaging environment at play, as the following table demonstrates:

REQUIREMENTS	ENTERPRISE	INTER-ORGANIZATIONAL (B-TO-B)	CUSTOMER/CITIZEN (B-TO-C)
Type of Security	<ul style="list-style-type: none"> • Strong identification of sender and recipients (hierarchical trust) • Ability to assign delegates to read and respond to email • Automatic encryption of email without user intervention • Individual-selected message signature and verification • Individual-selected message privacy 	<ul style="list-style-type: none"> • Peer-to-peer identification of sender and recipients (associative trust) • Ability to delegate applications (content monitor) to process email • Automatic encryption of email based on type of content, without user intervention • Individual-selected message signature and verification • Policy-based privacy enforcement 	<ul style="list-style-type: none"> • Strong identification of sender through public root of trust (third-party trust) • Protection of recipient's privacy • Organization-based message signature or receipt
Ease of Use	<ul style="list-style-type: none"> • Integrated with common security infrastructure • Support for mobile workforce (Off-line use, bandwidth constrained connections) • Security functionality that is easy and transparent to users 	<ul style="list-style-type: none"> • No requirement for partner to deploy new software • No change in partner's email behavior 	<ul style="list-style-type: none"> • No requirement for recipients to deploy any software • No change in recipients' email behavior
Interoperability	<ul style="list-style-type: none"> • Support for email-enabled devices (PDAs and smartphones) 	<ul style="list-style-type: none"> • Support for a common message security protocol (S/MIME) 	<ul style="list-style-type: none"> • Support for a common communication protocol (SSL)

Choices for Securing Email

End-to-End Desktop Email Encryption Solutions

Encrypted email is widely recognized as being the most secure method of electronic communication. Before the advent of boundary email encryption, public key encryption via a public key infrastructure (PKI) was the only method available for sending encrypted messages. Email exchanged in this manner can be encrypted and/or digitally signed at the sender's desktop and remain that way throughout its journey to the recipient's desktop, where it can continue to remain encrypted even when in storage. There are a few different ways in which end-to-end email encryption can be deployed.

Desktop-to-Desktop

Email exchanged in this manner can be encrypted and/or digitally signed at the sender's desktop and decrypted at the recipient's desktop. To facilitate this form of encryption, a desktop-based email encryption solution uses a client desktop application or an email plug-in with enhanced security functionality to work with a Public Key Infrastructure (PKI). By leveraging the sender's digital certificate (issued by the PKI) the PKI desktop client can apply a digital signature to a message to provide verification of the sender's authenticity and credentials. The PKI also applies the encryption capability.

Though this type of email security solution provides a high level of email privacy, it can be complicated to set up and manage, as well as cumbersome for users to work with. With a 'click-to-encrypt' methodology, individual users must click to sign and encrypt messages, and if recipients are not using the same PKI infrastructure, it can be frustrating for users to go through the process required to enable secure email communications with external third party recipients who may not be using mail clients that can accept and decrypt signed or encrypted messages. As a result, they will often forego sending secure messages, thereby exposing your organization to a potential breach.

The benefits of deploying such a complex identity management and encryption platform might outweigh the costs to deploy and manage. However, within many large organizations you will no doubt find pockets of people who have desktop encryption installed, so whatever you deploy for your organization will need to be able to interoperate with these deployments.

Native Encryption Within Email Clients

Individuals using email clients that have 'native encryption capability' built-in, ***but without accessing a PKI***, can still send encrypted messages. Typically, such a mail client would provide the user with a click-to-encrypt methodology for sending the encrypted message to a particular recipient. Encryption keys are still used to apply the encryption, but the email client alone does not manage the keys for users. Although this is the least difficult desktop solution to deploy, native encryption email client solutions generally suffer from a lack of enhanced security features as well as relying heavily on the user to understand how the security works. Specifically, these types of solutions tend to lack the following features and functionality:

- No key update
- No key recovery
- No maintenance of key histories
- No Certificate Revocation List (CRL) checks
- No centralized management

Often, native email encryption client solutions use proprietary technology for encryption and decryption. The result is that organizations have to rely on the long-term viability of the vendor company to continue supporting the encryption technology. Furthermore, in order for this type of

deployment to be successful, each user requires a substantial amount of training to understand the process for encrypting and sending messages to different types of recipients (internal or external) and knowing the consequences of trying to send an encrypted message to a recipient who will be unable to decrypt the message. One benefit of such a solution, however, is that it gives end-to-end encryption for privacy, but the main disadvantage is that you need to know what type of email client or application your intended recipients are using before sending them an encrypted message. Generally speaking, this type of solution is best recommended for small groups of knowledgeable users.

Security Plug-ins

Unlike native encryption email client capabilities, security plug-ins are typically designed to work with a specific security infrastructure (a PKI) and remove much of the burden placed on the individual user, making plug-ins virtually ideal for enterprise deployments. Factors that make these types of solutions less than ideal are noted below:

- They suffer from the same deployment problems associated with having to deploy any desktop client software
- Some vendors use proprietary security schemes instead of S/MIME or SSL standards
- Unless the certificates for all possible recipients are automatically cached locally, off-line usage of secured messages will require a change in user behavior (and some training)
- Certain security operations, such as encrypting for a large recipient list, can add significant size to an email and impair overall mail processing performance when working over a low-bandwidth connection (such as via wireless-enabled mobile devices)

Another challenge involves the task of associating boundary-type certificates with multiple external recipient emails—advanced features that alert senders when the email address found in the certificate is not the same as that of the recipient—as well as manually associating a single certificate with multiple people. Lastly, not all email systems support S/MIME or OpenPGP encryption standards. Web messaging services such as Hotmail and Yahoo are primary examples, making it difficult to exchange secured messages with users of these types of mail applications.

In summary, email encryption clients and plug-ins have several challenges. Both require some degree of end user knowledge when sending and managing secure communications with external parties, and they place the responsibility to manually 'encrypt' messages on users.

Boundary Email Encryption Solutions

The development of **boundary email encryption capability** has taken the complexity and responsibility of encrypting email away from end users to simplify secure email communications for organizations of all types. There are several key advantages of the boundary encryption method:

- It is the easiest type of email encryption to deploy and manage
- Does not require the installation of new software on individual PCs, so all types of users can take advantage of its benefits
- Enables secure communications with external users who do not use a mail client with email encryption capability
- Enables the ability to set automatic email encryption policies such as 'encrypt-all' messages before they leave the corporate network

Boundary email encryption solutions (also known as 'email-gateway' solutions) are generally deployed with hardware (an appliance) or software solutions installed at the boundary of an organization. In their simplest form they are used to **encrypt all** outgoing messages and **decrypt**

any incoming emails based on a straightforward set of rules. More advanced solutions offer policy-based configurations that allow the system to encrypt and sign an email on a sender's behalf as well as decrypt and verify incoming messages. The boundary approach has the main advantage of enabling easier deployment relative to desktop-based solutions, and providing policy-based security vs. security that is dependent upon individual user behavior.

There are however, a few potential trade-offs with boundary email encryption solutions. They provide a lower level of privacy, as an email message is not secured until it reaches the organization's boundary—which can be a critical issue, since 60-80% of all security breaches are internal. Additionally, there is a lack of strong sender identification and verification, as the sender (message creator) is not actually digitally signing the message on their own behalf to verify its origin. In addition, boundary email solutions do not enable internal end-to-end encryption capability, so if one department wants to secure messages sent internally to another department on the same network (within the same organization), it cannot do so with a boundary solution alone.

Despite these trade-offs, however, according to industry analysts, gateway-based encryption is on track to become a widespread method of securing email communications.

"In 2006, nearly 50% of organizations will deploy email security at the gateway, focusing as much on compliance with messaging policy as on combating spam and malware."

Source: Forrester "You've Got Mail: 2006 Messaging Security Adoption", Natalie Lambert, April 26, 2006.

Secure Web Mail Solutions

Instead of using S/MIME, Web mail systems use SSL/TLS-based protocols in the delivery of secured messages. There are two primary models for secure web mail delivery—pull and push.

Pull Models

Within pull models, a notification message along with a URL, is sent to the recipient to **pull the user back to a portal where a secure 'inbox' is displayed**. The recipient can then view the secured message using a common browser authenticated via a SSL/TLS session. Solutions using this approach should integrate well with an organization's existing web portal and authentication systems. Capabilities and requirements will vary among vendors, such as those for securing attachments, replying securely, and interoperating with desktop clients. A pull solution should be able to work with desktop clients that activate boundary encryption (not just use policy to encrypt) and also work with existing desktop encryption tools. Vendors such as Entrust will also offer companies the option to 'brand' the secure web mail interface to provide service provider transparency to their users. This is particularly valuable to business to consumer deployments.

According to Gartner, *"Secure e-mail solutions using a "pull" approach are best for business-to-consumer (B2C) communications."*³

Push Models

Within push models, a secured message is delivered to a recipient i.e., pushed as an attachment along with executable code to decrypt and display the message in the recipient's Web browser. Decryption keys for the push methodology are managed by the sending organization and delivered to recipients through an authenticated SSL connection.

Web mail-based secure email implementations have the benefit of providing a solution with the lowest common denominator in terms of system requirements for external recipients. For this

³ Gartner "Differentiators of Leading Secure E-Mail Architectures", Eric Ouellet, Feb 28, 2006

reason, web mail solutions can be a preferred approach for ad hoc messaging and certain types of messaging applications such as consumer-based statement delivery.

Benefits of Secure Web Mail Delivery

Customers considering a boundary-based email security solution (push or pull approach) should take into account certain trade-offs inherent to web mail-based delivery, including the following points:

- Users are asked to change their email behavior since the message is not displayed in their normal mail client, they must use a web browser to access the messages
- Offline usage is not typically available
- Secured mail messages, or the corresponding keys, must be stored on a server for a period of time
- User ID and password authentication of the SSL session does not provide the same level of enhanced identification that is provided by digital certificates. However, multi-factor authentication could be added to enhance the security for the

According to Gartner, "*Secure e-mail solutions using a "push" approach are best for business-to-business (B2B) communications.*"⁴

Options for Setting-up A Secure Email Infrastructure

Based on your internal security requirements and the messaging environments of your target recipients, there are several potential scenarios for enabling secure email communications. The diagram below breaks these scenarios down based on where encryption and decryption will occur—***whether at the desktop client or at the boundary.***

⁴ Gartner "Differentiators of Leading Secure E-Mail Architectures", Eric Ouellet, Feb 28, 2006.

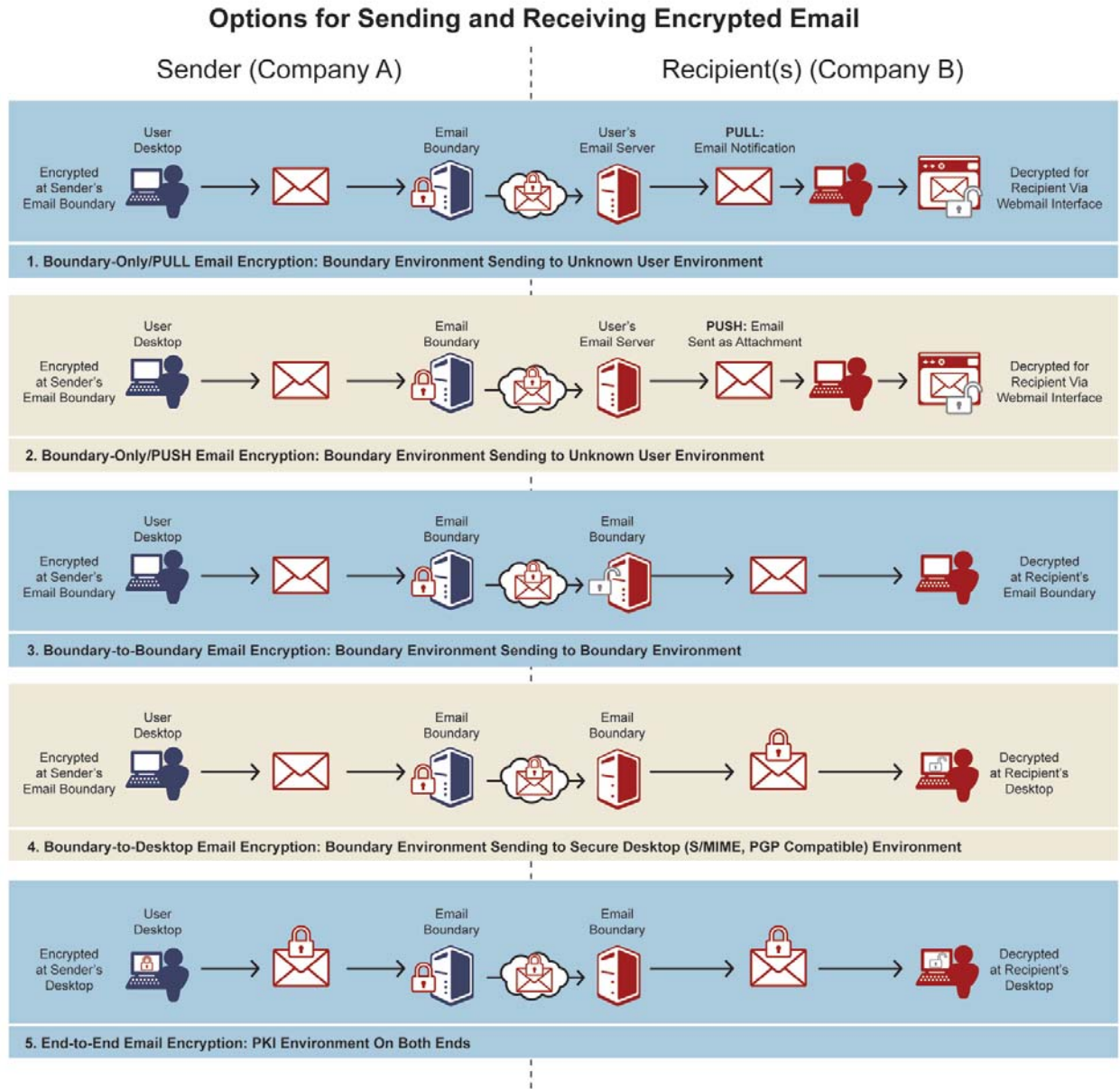


Figure 2: Choices for Securing Email

Entrust Boundary Email Encryption: A New Approach

Entrust has been a leading provider of email security solutions for over ten years. Companies have successfully deployed the Entrust Entelligence portfolio of PKI security products to send secure email text and attachments for full end-to-end, desktop-to-desktop security, both within their organizations and externally with partner organizations. As companies have expanded their email usage to integrate more transactions outside their corporate boundaries, Entrust has been enhancing its approach to securing email. Entrust's next generation email solution is called the **Entrust Entelligence Messaging Server**, a boundary-based email encryption solution designed with ease of use and management in mind, to encrypt messages at the boundary or 'edge' of your corporate network, for secure communications with various kinds of third party recipients from business partners to consumers.

Entrust Entelligence Messaging Server

Entrust's Email Security Solution monitors and secures a broad range of messaging environments. By helping to protect the confidentiality of message content and enforce corporate policy for email communication, it can reduce the risks associated with communicating sensitive information to employees, partners, customers, and constituents. Entrust Email Security provides boundary-based and/or end-to-end desktop security built on open standards. It offers flexible delivery options to provide comprehensive email security that can interoperate with advanced content monitoring and analysis of communications with internal and external users—regardless of their particular type of email application. Through support for mobile devices such as the BlackBerry™ wireless handheld, Entrust Email Security can also enhance productivity by adding security to email transactions taking place throughout daily work life.

Entrust Entelligence Messaging Server is a core component of Entrust's Email Security Solution that can address many of the issues and requirements of sending secure email to employees and business partners. It is based on an appliance-based server that streamlines deployment and management. The Messaging Server architecture provides flexible secure delivery methods such as a secure web mail interface, is based on open standards, and easily integrates with other boundary services such as anti-virus, anti-spam and content monitoring and analysis technology.

Messaging Server transparently manages security functions and enforces corporate secure email policies, making it easier for users to securely communicate with their colleagues inside and outside of the organization. The product offers standards-based S/MIME, OpenPGP, and Web-based options for secure message delivery. The Messaging Server can be deployed in a variety of email environments, including Microsoft Outlook/Exchange and Lotus Notes. External recipients can use either S/MIME or OpenPGP enabled email clients—like those contained in the Microsoft Outlook or Microsoft Outlook Express products—or common Web-based email services (for example, Yahoo!® MAIL or MSN® Hotmail).

Entrust Entelligence Messaging Server is offered as an appliance that provides encryption and decryption capability for an organization's messaging infrastructure. It can be used to provide either Boundary-only email encryption, or Boundary and end-to-end secure communications, depending upon an organization's existing security infrastructure and email encryption requirements.

Features and Benefits

- Web-based configuration and user administration
- Single or multi-node appliance architecture with built-in clustering capability

- Customer-controlled software update and migration service
- Flexible secure delivery—per recipient, per domain, and system default
- Interoperability with external S/MIME-based and OpenPGP-based secure email users
- Automated credential management for S/MIME and OpenPGP, based on key and certificate harvesting
- Integration with content monitoring and analysis services, enabling filtering of encrypted mail (See section, “Opening Your Eyes” on Integration with Vericept Content 360^o)
- Interoperability with Microsoft® Certificate Services certification authority
- Support for native Lotus Notes security format and identities

Deployment Flexibility

Entrust Intelligence Messaging Server allows multiple email encryption deployment models and flexible delivery options to suit both internal and external user requirements. The Messaging Server appliance hosts an email encryption application. The application encrypts email messages on the server side before sending them to recipients. This behavior contrasts with many competitive email encryption solutions in which email encryption is completed on the client side. When a Messaging Server user sends an email to a recipient, the email is encrypted for Messaging Server, sent to Messaging Server where it is re-encrypted for the intended recipient and then sent to the recipient. The sender does not need to exchange encryption keys with the recipient, or even know the recipient’s type of email application or preferred method of secure delivery in order to send a secured message.

Options For Enabling Email Encryption Within Your Organization

A Boundary-based solution secures email at the external boundary of your network for delivery to external recipients. This is accomplished in conjunction with one or more of the following:

- Desktop software (user directed)
- By basic Messaging Server policy (for example, encrypt all messages to a particular domain, or with a particular value in the header)
- By automatically scanning the contents of the message and encrypting based on context, meaning, and sensitivity of the contents (active policy enforcement using a Content Control application such as Vericept Content 360^o)
- Flexible secure message delivery. The delivery option is automatically selected based upon the recipient’s preferred delivery method. Delivery options include:
 - S/MIME
 - OpenPGP®
 - Web mail Pull
 - Web mail Push

Entrust Intelligence Messaging Server offers many possible options for sending encrypted email:

- Automated boundary email encryption based on corporate policies
- Automated email encryption based on the domain of the recipient
- Automated email encryption based on values in the email header
- Sender determined boundary encryption (Messaging Server and Boundary Encryption Plug-in required)
- End-to-end encryption with Microsoft Outlook® or IBM® Lotus Notes (Messaging Server and a desktop plug-in required for use with Microsoft Outlook)
- Mobile security with BlackBerry™ handhelds (Messaging Server required)
- Off-board secure storage of Web-based secure email (can be included in any deployment of Messaging Server)

- Web-based secure email communication to external recipients who may not have secure email capability (Messaging Server required)
- Strong authentication of external Web users through integration with Entrust TruePass (Messaging Server and Entrust TruePass required – as your Entrust Solution Consultant)
- Seamless integration with an external Entrust Authority Security Manager Installation for credential management (Messaging Server and Security Manager required)
- Compatibility with Microsoft® Certificate Services or other Certification Authorities using PKCS#12 (Messaging Server and third Party CA required)

Push and Pull Technology: Secure Web Mail Delivery

One of the key advantages of Entrust's Boundary based email security solution is that, in addition to S/MIME delivery, organizations can employ secure web mail to exchange secure email with external partners who do not have S/MIME or OpenPGP capabilities. Entrust Entelligence Messaging Server uses both push and pull technology. Using a compatible Web browser and any common email account, external recipients can receive (and authenticate) secure messages with internal desktop users. Specific features and benefits of the Web-based delivery are as follows:

- Facilitates secure email communication with external recipients without the need for S/MIME certificates or OpenPGP keys
- Does not require client-side software (leverages existing email client and browser)
- Provides rich email functionality: read, reply, compose, delete, send/receive attachments, sort and manage personal folders
- Enables self-service account management (register, enroll, reset password and set preferences)
- Offers a Web-based administration model with support for user self-administration

Sending an Email

When using Entrust Entelligence Messaging Server, there are several different ways in which a secure email message can be sent. The server can be set up to encrypt messages 'automatically' based on certain criteria, or messages can be encrypted by individual users. Here are some of the possible send options:

- **Automatic (Autonomous) encryption:** autonomous encryption of a message if it is coming from certain individuals or departments (such as CEO), is going to a specific domain or partner company, has a particular key word in the subject line, or if there are specific identified features of the message (such as attachments)
- **Click-to-Encrypt:** on-demand encryption of specific messages based on 'click-to-encrypt' basis, by using The Entrust Entelligence Boundary Encryption Plug-in for Microsoft Outlook

How Boundary-Only Email Solution Deployment Works

In a deployment where the Boundary-Only feature is enabled, emails that stay within your organizational boundary remain un-encrypted. Emails going outside your organizational boundary are routed to a policy engine, which decides whether the email should be encrypted and/or signed based on the email's content or other selected criteria. The policy engine then forwards emails requiring encryption and/or signing to Entrust Entelligence Messaging Server for processing.

If you are using Autonomous Encryption, Messaging Server can be configured to determine if a message requires encryption based on a regular expression in one of the header fields. Messages can have a number of headers—for example, **Importance, From and Subject**. The Messaging Server enables you to specify a header and a particular expression associated with that header to use as an encryption trigger. For example, using the From header, you could

configure Messaging Server to encrypt all email from the CEO of the company. Similarly, Entrust Intelligence Messaging Server could be configured to encrypt all email with the word 'restricted' anywhere in the subject or any email of "high" importance. This feature can also be configured so that all email addressed to certain domains is encrypted. You would specify these domains in Entrust Intelligence Messaging Server so that, for example, all email going to a particular business partner or government department is automatically encrypted.

Entrust Intelligence Boundary Encryption Plug-in

The Entrust Intelligence Boundary Encryption Plug-in is a small plug-in to Microsoft Outlook. Using the Boundary Encryption Plug-in, Messaging Server can be set up in a boundary-only deployment. In a boundary-only deployment, Messaging Server only encrypts email messages that are sent to external recipients. Email messages between internal users are sent in plaintext format. For users that want to be sure that their message is encrypted, the option is available for them to use the plug-in to flag the server to encrypt. As such, to enable encryption when sending email to external users, the Boundary Encryption Plug-in is used in conjunction with Entrust Intelligence Messaging Server and a properly configured mail infrastructure to allow internal users to choose whether an email should be encrypted for a specific external recipient. (An external recipient is anyone who does not belong to the internal domain(s), as specified when setting up Messaging Server.) It adds encryption instruction headers for the Entrust Intelligence Messaging Server to a mail message. When the Entrust Intelligence Messaging Server reads these headers, it encrypts the message for the external recipient(s).

The Benefits of Entrust Intelligence Messaging Server

Organizations can expand their electronic communication capabilities using boundary email security to help allow more high-value, paper-based communications to be moved online. The Entrust Intelligence Messaging Server provides support for message privacy, integrity and sender identification. Messaging Server has capabilities that can be used for securing email to a wider range of customers, partners and employees, no matter what their particular email infrastructure. The following are some of the benefits of utilizing the Entrust Intelligence Messaging Server within your organization.

Enables Automatic Email Encryption

Employees, customers or partners do not have to change the way they currently work or the messaging environment they are using in order to communicate securely with your organization. The comprehensive Messaging Server is easy-to-use, configurable and interoperable with a wide range of messaging solutions. In addition, its flexibility allows it to be combined with content monitoring technology to add additional security capability (see next section, "Opening Your Eyes"). Many competitive security solutions require users to understand and manage their own security, but the Entrust Intelligence Solution provides autonomous encryption, a transparent mechanism for securing electronic communications. Some solutions can be so difficult to manage that users end up reverting back to traditional methods of communication. The ease of use associated with the Entrust solution enables ongoing utilization of email as a transport vehicle for sensitive communication, which can help improve productivity and help to reduce the risk of information breach by users not following security guidelines.

Helps Achieve Compliance

A direct benefit of deploying automatic encryption of email communications is that your organization can help achieve compliance with information privacy regulations. You can rest assured that your organization will be protected from accidental email disclosures of sensitive customer information, confidential documents or other types of data that should not leave the network unprotected. By taking the responsibility away from the users, you can help reduce your risk of breach significantly.

Reduces Costs and Improves Productivity

Unlike competitive solutions that require users to understand and manage their own security, sending a secured email using the Entrust Boundary Email Solution is no more difficult than sending a regular email. Security is managed transparently and automatically on behalf of the user. This ease of use, coupled with privacy and trust, encourages employees to move away from more expensive forms of communication (registered mail, private courier, etc.) and move towards using faster, less expensive, secured email communication. Broader adoption of security can add up to greater savings. By accelerating business processes with secure electronic communications, it is possible to work more efficiently with business partners, and extend greater value added services to those you were unable to reach with traditional mechanisms.

Extends Security Beyond the Organization

The Entrust Boundary Email Solution now allows business partners and customers who do not use digital IDs traditionally required for encrypted email, to communicate securely with your organization via the web mail interface provided by Entrust Entelligence Messaging Server. This next-generation email security solution extends secure email communications from B-to-E into B-to-B and B-to-C environments, helping to get even more out of your investment in an email security solution.

Offers Flexibility and Interoperability

The secure messaging market has been characterized by a lack of standards and the introduction of non-integrated, patchwork solutions that solve specific messaging issues. This lack of interoperability causes problems with messaging systems and makes it difficult for organizations to communicate with partners and customers. With its strong standards support, Entrust's flexible and interoperable boundary email security solution provides enhanced security across a broad range of messaging environments—including widely deployed enterprise email systems such as Microsoft Exchange, Lotus Notes, and any range of web-based email applications. In addition, it interoperates with a variety of third party solutions to enable additional capabilities such as virus and content monitoring.

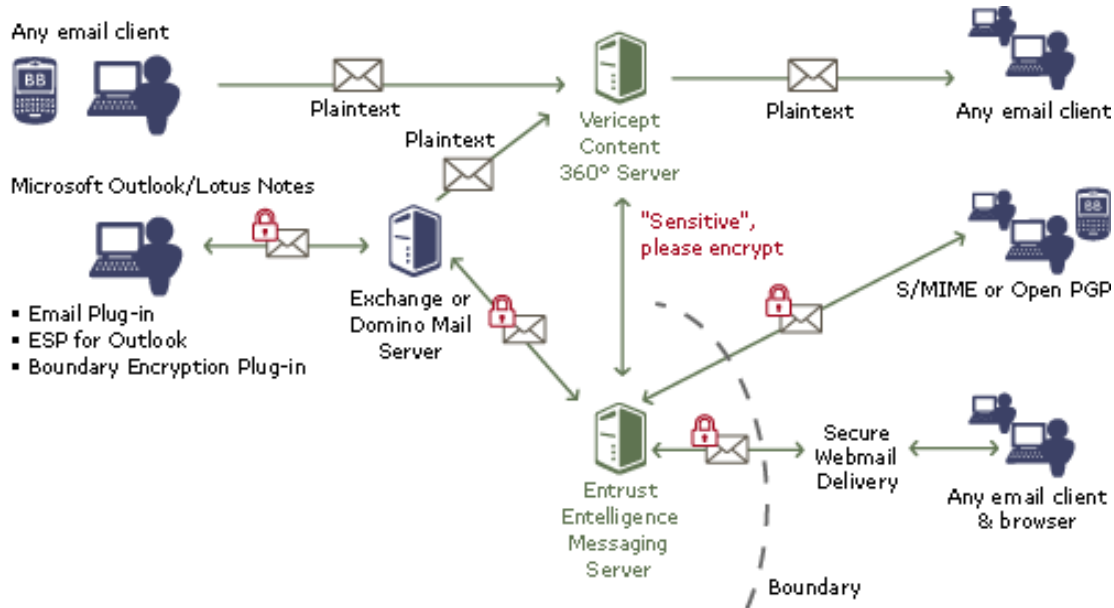
Opening Your Eyes: Integrating Email Encryption with Content Monitoring and Control

In a recent survey conducted by Osterman Research, 6% of companies surveyed experienced a sensitive information leak, of which 83% of reported losses were considered accidental.⁵ With the growing concern of corporate data breach and loss of sensitive information, organizations are increasing their adoption of outbound content control for regulatory compliance, protection against identity theft and safeguarding of intellectual property. If you could have visibility into the flow of communications in your company, you could be in a better position to help prevent corporate information leakage and brand degradation. Together, content control and automatic email encryption can provide an effective security solution for organizations to mitigate their risk of information breach and protect their corporate brand.

In partnership with Vericept, a leading content control solution provider, Entrust offers Vericept Content 360°, a multi-protocol content monitoring and control solution that provides visibility into how sensitive content is handled in an organization. Utilizing a suite of content detection techniques and over 70 risk categories, Vericept Content 360° works with Entrust Intelligence



Messaging Server to identify which messages need to be encrypted before they leave the boundary of an organization. With Content 360°, email content can be monitored with greater accuracy to detect intellectual property, personally identifiable employee information or sensitive customer data. When this type of content is detected, the system can be configured to take immediate action such as automatically encrypt the email, or even block delivery.



⁵ Osterman Research / Entrust "Sensitive Information Leak Survey", November 2005.

The PKI Alternative: End-to-End Email Encryption

For organizations who need or want to deploy end-to-end email encryption (particularly those requiring encryption internally among employees), PKI-based email encryption solution is the best option. According to Gartner:

"An end-to-end secure e-mail solution is best-suited for highly stringent security environments in which there is a specific requirement for securing an e-mail from the time it is created until it is read."

Source: Gartner "Differentiators of Leading Secure E-Mail Architectures", Eric Ouellet, Feb 28, 2006

The Entrust Entelligence™ PKI product portfolio is an integrated suite of security solutions that delivers a single security layer across multiple enterprise applications enabling strong authentication, authorization, digital signatures and encryption. Entrust Entelligence products help empower employees to work efficiently, communicate effectively and improve corporate and regulatory compliance. This infrastructure can be deployed to enable full end-to-end, desktop-to-desktop email encryption within an enterprise and for secure communications with external recipients. It can be deployed instead of Boundary-based email encryption, or it can also be deployed along with the Entrust Boundary Email Solution since, as previously discussed, the Entrust Entelligence Messaging Server is capable of acting in both capacities. Unlike solutions limited to boundary-based security or solutions that simply maintain message encryption during transit, the Entrust PKI-based email encryption solution can provide end-to-end encryption that secures messages in transit from the sender's desktop to that of the recipient, and also maintains messages in an encrypted state during storage.

Managing Digital Identities & Encrypting Messages for External Recipients

Digital identities, by way of digital certificates, are used by the Entrust PKI email encryption solution. The Entrust Entelligence Messaging Server manages the digital identities for internal and external recipients as messages flow through the server. Once a digital identity, in the form of a digital certificate, is received for an external recipient, the Messaging Server makes that certificate available for all internal users as required. If a certificate is not found for a particular user, the Server will conduct a 'harvest,' in which it will send an email message to the recipient asking for their encryption certificate and then place the certificate in the Messaging Server's database if they are received.

The Messaging Server also enables inbound and outbound translation between the internal email security format and the Internet standard S/MIME, OpenPGP or SSL secure delivery methods that external recipients may be using. This simplifies secure communications with external recipients without changing user behavior.

The key components of the Entrust PKI-based Email Encryption Solutions are as follows:

Entrust Entelligence™ Security Provider

Delivers managed Entrust digital IDs across applications via thin-client enterprise desktop security software. Can be used in conjunction with Microsoft Outlook's native S/MIME email encryption capabilities to provide end-to-end email encryption capability.

Entrust Entelligence™ Messaging Server

Provides a server-based email security gateway that provides encryption of email and attachments and routes messages and certificates as required.

Entrust Entelligence™ Email Plug-in for Outlook

Enables users to encrypt and digitally sign messages via an easy-to-use plug-in for Microsoft Outlook that integrates with Entrust Entelligence™ Desktop Manager.

The Need to Act Now

Regardless of whether organizations are being driven by competitive pressures, corporate governance guidelines, regulatory requirements or an increased need for sharing sensitive information, the added value and lower costs of using email encryption are clear. Most organizations that want to leverage the benefits of email security are searching for security solutions that address more than just the enterprise-messaging environment and Entrust has a solution.

The boundary-based approach of the Entrust Entelligence Messaging Server is designed to address security, ease-of-use and interoperability requirements to communicate securely with recipients in various types of messaging environments, including consumers. Entrust Entelligence Messaging Server is easy to deploy, transparent to end users, and can leverage existing email infrastructures, making it easier to implement and manage, one of the key requirements for a successful email encryption infrastructure. Furthermore, the solution is designed to operate with other types of security applications such as the Vericept Content Control products, to enable full visibility into the flow of communications in your organization. Organizations can help mitigate the risk of breach posed by electronic communications, and potentially benefit from the added value and lower cost of moving more types of business processes to an email format.

For more information about how Entrust can help assess your needs for email security, please contact us at entrust@entrust.com or call **1-888-690-2424**.

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 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. For more information on how Entrust can secure your digital life, please visit: www.entrust.com.