Email Encryption Buyer's Guide 2008

An Osterman Research Publication

Published March 2008

Osterman Research, Inc. • P.O. Box 1058 • Black Diamond, Washington 98010-1058
Phone: +1 253 630 5839 • Fax: +1 866 842 3274 • info@ostermanresearch.com • www.ostermanresearch.com

Chapter 1

Executive Summary

Purpose of this Guide

Many prospective encryption users have not deployed encryption technology because of perceptions that encryption mechanisms are too difficult for the average employee to use, that they do not scale well, or that they are too expensive to deploy. Although these limitations may have been true for many early-generation encryption systems, most encryption technologies available today do not suffer from these problems. Because many decision-makers still hold to outdated perceptions about encrypted messaging, however, this guide was written to help explain the benefits associated with the current generation of systems and their ease of use.

The Critical Nature of Email

Email is clearly the most critical communication medium used in business today – more important than the telephone, instant messaging, fax, or postal mail. About 75%[1] of the information the typical email user employs on a daily basis is bound up in email in the form of email threads, calendar entries, tasks, attachments, and other content. Email users in the workplace send and receive an average of 140 messages on a typical workday[2]. Although email represents an enormous productivity tool for both users and enterprises, its pervasive and largely unsecured nature also represents one of their greatest threats: the potential loss of critical information.

Loss of sensitive or otherwise confidential business information can occur when this content is sent in clear text. It can be intercepted at any point along its route, such as when stored on email servers, on personal computers used by employees when checking email at home, or at any other point between the sender and the recipient.

> **As a result of this growing threat, encryption of email is a critical strategy to mitigate security risks, protect important information, and prevent these losses. It is no wonder that nearly all regulations concerning information security either directly or indirectly require encryption.**

Security Threats are Increasing

The Privacy Rights Clearinghouse has chronicled the breach of more than 216 million records between January 2005 and December 2007, as shown in the following examples[3]:

- **December 10, 2007**
  An email was released by an employee with Cameron County, Texas, containing a list of all county officials and employees, including their Social Security numbers and salaries.

[1] All data is sourced by Osterman Research, Inc. unless otherwise noted.
[2] Results from an Osterman Research, Inc. survey conducted in June 2007.
[3] Privacy Rights Clearinghouse (http://www.privacyrights.org/ar/ChronDataBreaches.htm)

- **November 16, 2007**
  A home computer owned by a former auditor of the US Department of Veterans Affairs was found to contain 185,000 unique Social Security numbers.

- **November 17, 2006**
  An email that contained the names and Social Security numbers of 143 students that should have been sent to just one employee of the Jefferson College of Health Sciences in Roanoke, Virginia was mistakenly sent to all 900 students in the college.

- **March 30, 2006**
  The Social Security numbers of 1,250 faculty and students in the Connecticut Technical High School System were accidentally distributed by email.

Although privacy considerations are of growing importance in the United States, privacy is even more of a concern in Europe and in several Asian countries with a variety of laws, such as the UK Data Protection Act, focused on protecting consumer and other confidential information. These breaches are the result of a wide range of problems, including hackers breaking into email servers, lost laptops and other mobile devices, identity theft, and other compromises of sensitive data that could have been mitigated through the use of appropriate encryption technologies. This is particularly important for multi-national organizations that must share data between jurisdictions that have different levels of privacy protection for consumer and other information.

> **An Osterman Research survey conducted in 2006 found that if a data breach were to occur in which disclosure of the breach would have to be made to customers and other external contacts, nearly two-thirds of organizations estimated that a single such breach would cost their organization at least $100,000, not to mention additional operational costs, damage to their brand, and other problems. Further, The Ponemon Institute© found that in 2007, the cost of a data breach in the United States is $197 per record, which represents a 42% increase from 2005. A data breach in the UK costs £47 (US$93) in 2007.**

Business Requirements Need to be Considered

It is critical to understand how an organization's business requirements impact the proper selection of an enterprise email encryption solution. Supply chains, branch offices, mergers and acquisitions, and a mobile workforce create a variety of unique demands that must be accommodated by an enterprise encryption strategy:

- **The CIO**
  Wants the solution to seamlessly integrate with the existing email architecture, have a low total cost of ownership, and be easily upgradeable.

- **The CEO**
  Wants a secure email system with zero downtime that is always accessible via handhelds, such as the RIM® BlackBerry® device.

- **IT directors and managers**
  Want technology that is easy to deploy and use so that it can minimize the time IT staff spend deploying and maintaining the system as well as minimize help desk calls.

- **Users**
  Want technology that is simple to use or completely transparent and that doesn't require changes to their normal business routines and processes.

The encryption solution an organization ultimately selects must offer flexibility, compatibility, manageability, and reliability.

> **The business requirements for enterprise email encryption can be translated into specific features that should be required by virtually every enterprise. However, most commercially available encryption solutions lack many of these features:**

- **Flexible encryption modes**
  Organizations need to be able to protect their sensitive information with the most rigorous end-to-end encryption available, but also have the flexibility to protect less-critical data with strong, server-based encryption that is less expensive and easy to manage. These modes must not only work together seamlessly, but also support mobile users and handheld devices.

- **Standards compatibility**
  An email encryption solution must be compliant with the various Internet and vendor standards on which the existing email system is based. To achieve reasonable interoperability with partners, customers, vendors, and the rest of the world, the solution must support both OpenPGP and S/MIME encoding – without exception.

- **Ease of management**
  An encryption solution must support the existing corporate user directory automatically, without duplicating effort. Organizations must be able to leverage their existing IT management tools to deploy and administer the encryption solution. The solution should support a single management interface for additional encryption applications.

- **Integration beyond email encryption**
  Beyond securing email communication, an email encryption solution should support an integrated solution that will protect all files and data stored on a desktop or notebook computer as they are moved out of the email system. The use of full disk encryption allows an organization to address risk mitigation for security breaches due to system loss or theft.

- **Coexistence with anti-virus, anti-spam, and content filtering**
  An encryption solution should plug into the existing messaging security architecture, not go around it. That means a desirable email encryption solution will interoperate

seamlessly with installed anti-spam, anti-virus, and content-filtering applications.

- **Policy and compliance tools**
  An email encryption solution should help enforce the organization's email usage policy from the server to the desktop through to wireless handhelds. Its reporting system should help demonstrate compliance with necessary regulations. Additionally, the optimal solution should be extensible to manage other encryption applications, enhancing an organization's compliance capabilities by protecting sensitive data wherever it resides.

Acquiring a complete encryption solution today and ensuring that it can also solve security needs tomorrow – and into the future – mandates that organizations partner with an experienced, enterprise-tested, and established vendor.

What is the Status of Email Encryption Deployment Today?

An Osterman Research survey of mid-sized and large organizations in North America conducted in August and September 2007 found that:

- 38% of organizations have a gateway-to-gateway email encryption solution today, but another 23% plan to deploy such a solution by Summer 2008.

- 33% have a desktop-to-desktop email encryption solution in place today, but another 20% plan to deploy this capability by Summer 2008.

What Should You Look For in an Encryption Solution?

Email encryption is a critical component of any messaging architecture and must be available to protect confidential and other sensitive content sent outside of an organization. There are several key issues to consider when planning an email encryption capability, when evaluating vendors and when deploying a solution:

- **Protect sensitive content with transparent email encryption**
  A data security breach due to unauthorized access to email communications can lead to significant financial consequences and brand damage. Automated, policy-driven email encryption is preferable to manual encryption solutions because it locks down the content of email communications without changing user behavior or workflow.

- **Simple email encryption protection should not impact the user**
  Automated, policy-driven email encryption protects communications without changing the user's email client configuration or burdening the user with additional actions to ensure protection of email communications. End-users do not require special training or knowledge, thus accelerating deployment time, reducing training costs, and eliminating the potential for increased help desk load.

- **Centralize the deployment and management of policies**
  Automate provisioning, user and key management, and policy enforcement across

email, disk, and network file encryption in order to minimize the IT and other resources required to manage the encryption solution.

- **Use standards-based technologies**
  This is a critical requirement in order to ensure interoperability with communications partners that have existing, standards-based email encryption solutions.

- **Deploy a solution with granular capabilities**
  It is important to be able to fine tune and lock down which features and capabilities are enabled, which are visible to specific users and which are enforced in order to best match encryption capabilities with user requirements and organizational needs.

- **Deploy a solution with expansion in mind**
  Email encryption is critical, but so are additional capabilities, such as disk encryption. Any solution should be extensible to meet current and future requirements.

- **Support all of the platforms that will be used today and in the future**
  An encryption solution should be supported on all of the client and server platforms that an organization will operate, including Windows, Mac and Linux.

- **Beware of solutions that:**
  - Are limited to protecting only one type of data, such as those that are built on proprietary messaging formats.
  - Are incapable of interoperating with communication partners' pre-existing, standards-based solutions.
  - Require the purchase, deployment and management of multiple products for comprehensive protection beyond email encryption, thereby increasing the TCO of the overall encryption solution.
  - Provide removable drive protection at an additional licensing cost.
  - Increase the time to deploy protection for additional applications.
  - Use multiple, non-integrated management systems, increasing the time and effort to learn, deploy, manage and support the system.
  - Use different applications and interfaces, thereby increasing the complexity of the system for end users and necessitating additional training.

This Guide Will be Worth Your Time

Please take the time to review this guide thoroughly. The value and simplicity of an enterprise email encryption solution is directly correlated to the time an organization spends understanding all of its critical requirements.

(This page intentionally left blank)

Chapter 2

Introduction

The rise of email from its humble origins in the late 1980s to the most widely used form of person-to-person communications in the workplace today is an impressive story. Today, the volume of email sent on a daily basis far exceeds the total number of delivered phone calls, instant messages, and physical letters combined[4]. Few would have planned for or foreseen the rapid ascension of email into the global economy's most vital messenger, the key role it would play in reshaping business, and the critical role it would play as the repository and file transport mechanism for critical and sensitive business records.

Email is a Huge Threat Vector

It is only natural that email's dominant role in global communications has also allowed it to become a medium for fraud, unsolicited commercial overtures, malicious code, and other undesirable activities. Despite corporate policies that may dictate otherwise, all forms of sensitive business information may find their way into email, making it the primary means by which that data is inadvertently disclosed or purposefully stolen. Incidents of loss or disclosure of sensitive data via email are widespread according to reports from several industry analysts, privacy rights groups and others.

Further, organizational requirements to secure email are made all the more important by the tremendous business value that can be derived from providing secure, one-way communications between organizations and their customers. For example, banks, credit card processors, merchants and a host of other types of organizations can provide additional value to their customers and significantly reduce their costs through the use of secure email to transmit invoices, statements and other sensitive information.

> **Businesses realize they cannot reverse the growing use of email, nor do the vast majority want to do so. To the contrary, most acknowledge this "always-on", pervasive communications system is an evolving but permanent fixture, a requirement for doing business, and thoroughly engrained into a variety of business processes. However, the consequences of data breaches can create financial, legal and reputational problems from which some businesses may never recover. One solution exists to protect the information in email, which when implemented properly, is proven to be immune to the most well-equipped and talented hackers: encryption.**

Encryption is Becoming More Commonplace Today

Although only small pockets of email users had adopted encryption in the early 1990s, enterprise email encryption is much more common today. Changes driven by business and regulatory needs, combined with technological innovation, are integrating all necessary components into complete solutions that enable the flexible email encryption business demands.

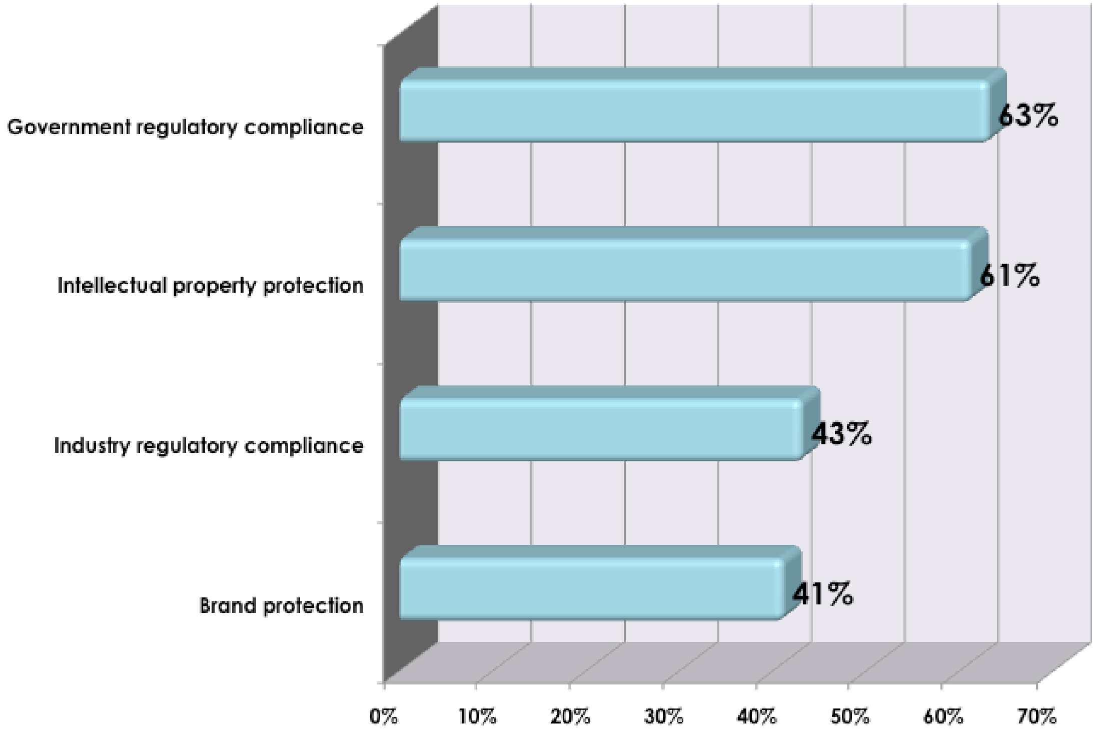
[4] According to the Radicati Group, 76.8 billion emails were sent daily in 2004. Compare this figure with 1.2 billion letters daily according to the Universal Postal Union (http://www.upu.org/about_us/en/glance.html), 7 billion instant messages according to IDC (http://tinyurl.com/3l3tx), and 3 billion phone calls in the United States according to Google Answers (http://dimacs.rutgers.edu/Workshops/NJHomeland/abstracts.html).

Despite these improvements, however, many IT and business decision-makers still do not understand what constitutes state-of-the-art enterprise email encryption and how to let business needs and risk metrics dictate their choice of an appropriate solution. In fact, many messaging architects still believe that email encryption requires significant end-user training and many full-time equivalent staff members devoted to key management. Today, however, this assumption could not be further from the truth.

Justifying Encryption Technologies

Decision-makers use a number of arguments to justify the deployment of email encryption capabilities, including regulatory compliance, protection of intellectual property, compliance with industry standards or requirements, and protection of the corporate brand, as shown in the following figure.

Importance of Various Issues in
Justifying an Email Encryption Solution
(% Responding Important or Very Important)



In a typical organization, about one in five users would be considered a "frequent" user of encryption technology: legal counsel, senior managers, HR managers and the like. However, Osterman Research believes that email encryption is what we call a "serendipitous" technology in that its mere presence in an organization can create demand for its use. For example, a marketing manager that never had a perceived need for encryption would likely begin using it to trade new logo designs with an external graphic arts provider assuming that encryption was easy to use. As a result, we anticipate that many more users would become users of encryption if the technology were available, inexpensive and easy to use.

Choosing the Right Encryption Solution

There are three steps all organizations should take in choosing the right encryption solution:

- **Define the business requirements**
  Take a risk management approach to understand the value of the data the organization seeks to protect, the impact email compromises will have on that data, the new business opportunities provided by securing previously insecure communications channels, and future business plans.

- **Define the technical functional requirements**
  Translate business needs into more specific processes that can be automated by encryption technology. The key functional specifications to analyze are flexibility of solution, user transparency, low cost of ownership, adherence to standards, compatibility, auditability, and management reporting.

- **Evaluate potential solutions and vendors**
  Analyze the stability, management team, and current customers of potential vendors. Ensure that the chosen vendor has a vision and long term roadmap that align with the organization's goals, and that their offerings will integrate well into the organization's business processes and network infrastructure.

(This page intentionally left blank)

Chapter 3

Business Drivers for Enterprise Email Encryption

While email is an extremely useful tool that enables a wide range of capabilities and business processes, it also carries with it several potential avenues for harming an organization:

- **Financial losses**
  The threats to an organization's email and other systems are both externally and internally based, involve both malicious attackers and poorly trained users, and can result in a variety of negative consequences. Several independent studies have pegged the associated financial losses for poor use of email at several billion dollars annually – and growing.

- **External threats**
  Among the external threats most commonly associated with email are viruses, spam, spyware and denial of service (DoS) attacks. The risks and costs associated with these attacks are well-documented and beyond the scope of this guide to discuss in detail. Indirect external threats include phishing, where recipients receive fraudulent messages enticing them to divulge personal information that can later be used in identity theft–based attacks; and "drive-by" attacks, in which users are directed to a Web page that, when simply viewed, can cause substantial changes to their Web or network configuration.

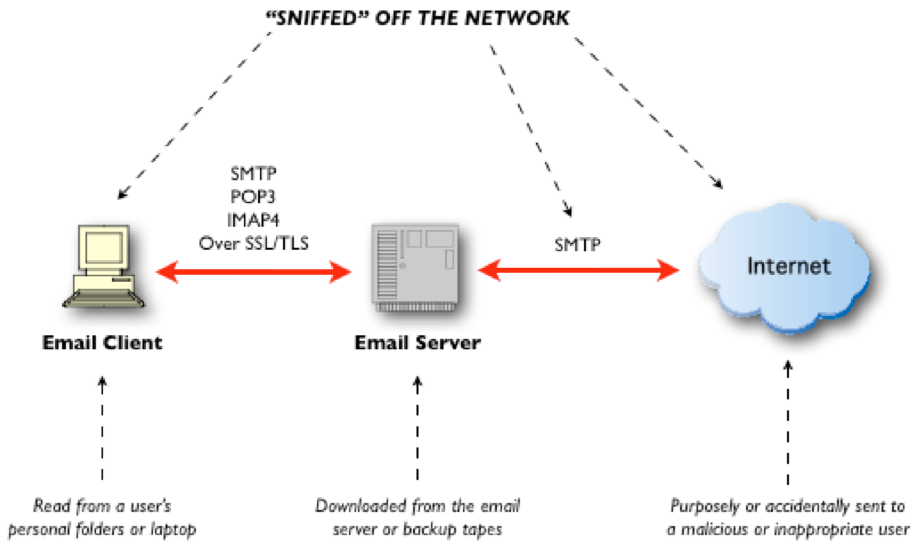
- **Internal threats**
  Internal threats to email can come from malicious insiders, such as employees who are abusing privileges, or others who fraudulently gain access to corporate email systems. Malicious insiders often seek to steal or destroy proprietary information. As serious as this threat is, mistakes made by well-meaning users who inadvertently violate corporate email policies and divulge sensitive data is much more significant danger.

Due to the pervasive nature of email, a clear majority of corporate information travels through the email system. Laptops and wireless handhelds have extended the reach of corporate networks, increasing the usability and timeliness of information, including email. Thus, the consequences of these email-borne threats can include network downtime, lost productivity, theft of sensitive data, and disclosure of other embarrassing information. The impact can be financial, legal, regulatory, or reputational. The severity can range from a small financial loss to putting the entire business in jeopardy.

The Perpetrators are Getting Smarter

The most disturbing trend in email security threats is the nature of the people behind them. Early email viruses were the province of hackers who were often experimenting with the medium and saw themselves as the high-tech equivalent of graffiti artists. In comparison, today's threats often come from well-organized crime syndicates that see email abuse as a lucrative business. This change has led to a marked increase in the frequency and sophistication of the attacks.

Points at Which Corporate Data is Vulnerable


"SNIFFED" OFF THE NETWORK
SMTP
POP3
IMAP4
Over SSL/TLS
SMTP
Internet
Email Client
Email Server
Read from a user's personal folders or laptop
Downloaded from the email server or backup tapes
Purposely or accidentally sent to a malicious or inappropriate user

Unprotected Email is a Critical Threat

The risks to email are varied, requiring layered defenses that span people, processes, and technology. Building greater awareness is part of the solution, as is building strong incident-response capabilities. However, several email-based threats exist because a preponderance of sensitive information is stored in plain text within email messages. As the figure above demonstrates, there are several points at which plain text email can be compromised. It is important to be mindful of these risks and to understand the solutions available to mitigate them.

For organizations today, these threats are compelling and are experienced daily. The mandate for IT and business decision makers alike is clear:

- **Protect the organization and its information.**
- **Mitigate the threats that directly attack email system stability.**
- **Block attacks that use email delivery as a medium.**

Business Requirements

When establishing the business requirements for email encryption, organizations should bear in mind the wide range of business scenarios that may affect the final choice of the solution. Following are some of the areas they need to consider before making a decision:

- **Integration of the supply chain**
  When an organization is part of a supply chain, integration with its suppliers' and customers' systems can be a vital consideration. In general, encrypted email should create new opportunities for the supply chain. However, the company must ensure the proposed encryption solution does not preclude communications with partners and

customers who use incompatible software, for example.

- **Integration of regional and branch offices**
  Organizations with branch offices, particularly those overseas, need to be cognizant of regulations and technical issues that might affect the integration of these offices into the overall system. These offices also may lack many of the technical skills and management resources available at a company's primary facilities. Further, there are significant differences between national requirements, particularly those that address privacy issues, that must be taken into account when planning and deploying any encryption capability.

- **Mergers and acquisitions**
  Mergers and acquisitions can create a wide range of IT integration challenges, most of which are unanticipated. If the organization ensures its email encryption architecture supports multiple standards, it will significantly reduce potential problems.

- **Increased use of mobile computing**
  The increasing use of mobile devices, ranging from notebook computers to highly sophisticated wireless handhelds with "push" email and intranet access, adds significant challenges to the protection of confidential and sensitive data. Further complicating the problem is the ease with which mobile devices are lost or stolen, thereby compromising sensitive data.

Regulations

There are a variety of regulations that are having a widespread influence on information assurance programs and that have elevated security to a boardroom concern. Following are some of the types of regulations that have proven to have a direct or indirect influence on the need for encryption:

- **Consumer protection regulations**
  These regulations include the Payment Card Industry Data Security Standard (PCI DSS), California Senate Bill 1386 (and similar laws in more than 30 states), the Gramm-Leach-Bliley Act, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), the UK Data Protection Act, and Japan's Personal Data Protection Law (often called J-SOX). For example, PCI DSS requires encrypted transmission of cardholder data when it is transmited across open, public networks; this includes the encryption of personal information sent via email prior to transmission. The UK Data Protection Act is the UK Parliament's response to the EU mandate regarding proper disclosure, appropriate access and transmission of sensitive data.

- **Government oversight regulations**
  These regulations include the US Food and Drug Administration's 21 CFR 11, which focuses on life sciences organizations, such as pharmaceutical companies; the Health Insurance Portability and Accountability Act (HIPAA); and the Sarbanes-Oxley Act. For example, HIPAA requires holders of Protected Health Information (PHI) to establish a mechanism for encrypting PHI when it is sent across public networks or where it could

otherwise be exposed. The Sarbanes-Oxley Act calls for mandatory encryption for financial reporting data and related sensitive information both at rest and in transit.

- **Government specifications**
  These include the U.S. Federal Information Processing Standard 140-2 (FIPS 140-2), which outlines standards for encryption software against which vendors may be validated for compliance; and the Family Educational Rights and Privacy Act of 1974, which includes provisions for how states can transmit data to Federal entities.

Enterprise Information Technology Design Considerations

The role of the CIO in any organization is to align information technology with the business mission and to lead initiatives to bring innovation to the business. In most organizations, the CIO has evolved into an indispensable member of the executive team by adroitly straddling two worlds: a) legacy systems that keep the business running smoothly and b) disruptive technologies that propel the business forward. Implementing enterprise email encryption illustrates this duality and includes several design requirements that CIOs must consider before beginning the development of an encryption architecture:

- **Email is mission-critical**
  Email now can be considered an important legacy application. A typical enterprise email system is the end product of several years of experience, fine-tuning and integration with a growing variety of business processes. We believe, and studies have shown, that if the average CEO had to choose between a day of corporate email downtime and a day without the corporate PBX telephone exchange, the vast majority would choose to do without phones. Within larger organizations, acceptable email downtime is typically only a few hours per year. With such demands for email system reliability, an important design consideration is that email encryption not disrupt the overall email system.

- **User productivity is paramount**
  Any modification to systems or business practices must have no negative impact on user productivity – ideally, it will actually improve it. Users should not have to suffer through an onerous new process to encrypt email that requires additional keystrokes, mouse clicks or other new procedures.

- **Support the status quo**
  Features added to an enterprise email system need to be incorporated without adding resource requirements, particularly additional IT labor. CIOs prefer that existing network, email, and desktop administrators be able to handle any new email security functions with as little additional effort as possible.

- **Limits in dictating to business partners**
  In the late 1980s and early 1990s, many organizations built proprietary value-added networks (VANs) to enable the sharing of data and applications. These VANs were a major step beyond earlier solutions. Considering the number of business partners with which a global organization needed to communicate, however, VANs quickly became

expensive and cumbersome to manage. In addition, VANs created a variety of security and reliability issues that were addressed by the public data networks that replaced them. Today, few organizations would build proprietary networks to communicate with business partners, nor would they force them to adopt a proprietary email encryption solution. Instead, the chosen solution must support all popular standards that allow encrypted emails to be sent between heterogeneous networks.

Encrypted Messaging Users

Email encryption is a "serendipitous" capability. In other words, although legal, executive management, and other selected groups may have the most pronounced need for encrypting messages, as shown in the following table, there are many others that can benefit from easy-to-use or policy-based encryption technology. For example, although only 11% of marketing organizations use email encryption today, there are a variety of activities – such as sending embargoed content to press and analysts – that could take advantage of encryption. Even though encryption in certain cases may not seem necessary today, the email encryption solution should be flexible enough to meet an organization's needs as they emerge and evolve.

Groups That Use and Will Use Email Encryption
2007 and 2008

Organization	Early 2007	Mid-2008
Legal	25%	53%
Executive management	21%	50%
Payroll	21%	47%
IT	20%	39%
Finance	19%	43%
Business development / M&A	13%	33%
Operations	13%	29%
Sales	12%	28%
Customer support	12%	27%
Marketing	11%	27%
Engineering / R&D	10%	29%

(This page intentionally left blank)

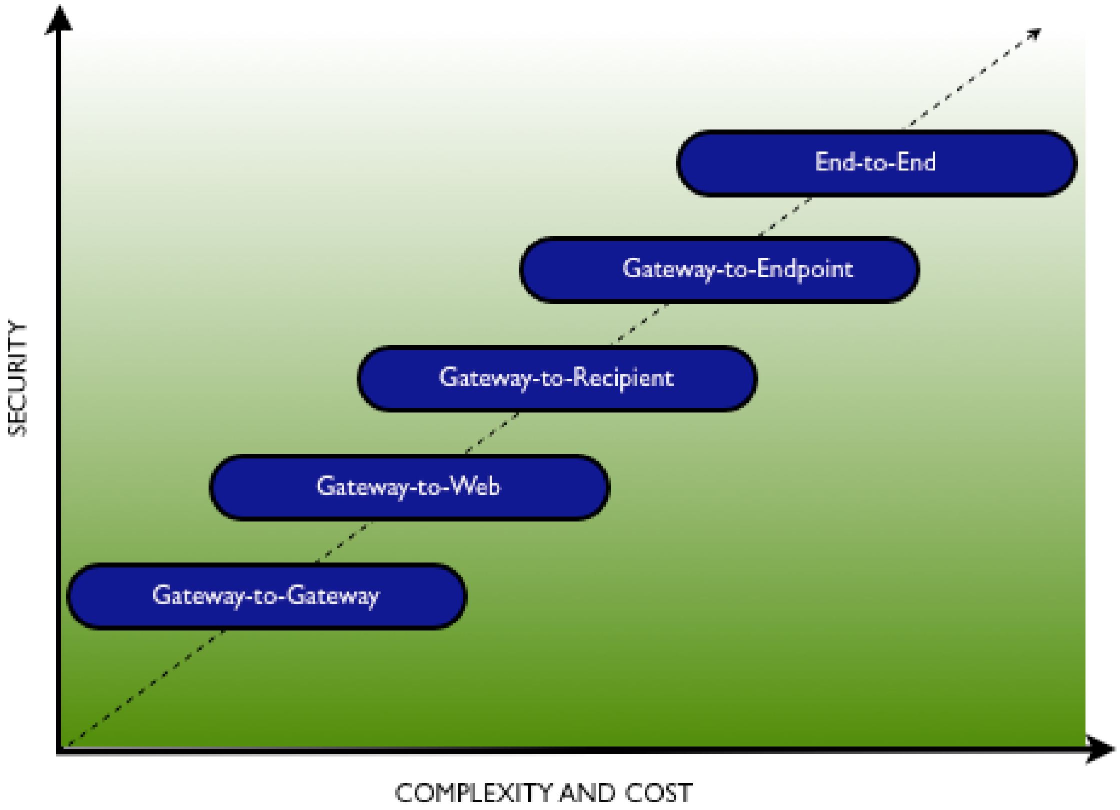
Chapter 4

Protecting Enterprise Email Communications

Encryption Modes

The term "encryption mode" describes at which points a message is encrypted and decrypted. There are several possible encryption modes, each requiring a specific tradeoff between higher security and increased complexity. Simply selecting one encryption mode and universally applying it to all types of encryption requirements is an ineffective approach. Instead, organizations should adopt a risk management approach that balances the security and complexity of an encryption mode with the business value of the data.

Security vs. Complexity



An enterprise encryption architecture and the resulting email encryption solution must be able to support all five of these encryption modes:

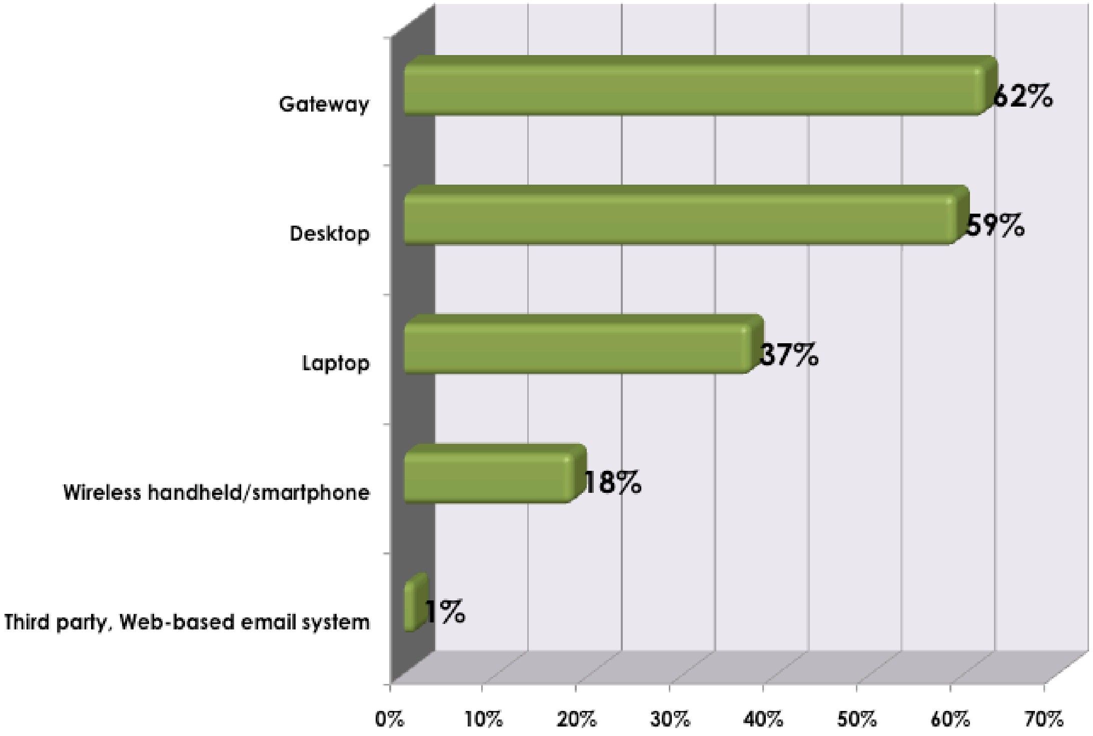
- Endpoint-to-Endpoint
- Gateway-to-Endpoint
- Gateway-to-Gateway
- Gateway-to-Web
- Gateway-to-Recipient

The Gateway-to-Recipient, or Statement Delivery, option is a capability that should seriously be considered by organizations of all sizes, regardless of the volume of their secure traffic. This option allows users to send documents securely using a widely deployed, industry-standard format, such as Adobe's Portable Document Format.

Although more combinations are possible, these five encryption modes represent typical options that organizations must take into account when making architectural decisions to allow any-to-any encryption. In addition, all these encryption modes should be integrated with each other to facilitate seamless switching between modes, even in real time.

Osterman Research has found that organizations currently prefer gateway- and desktop-based email encryption, although encryption needs to be available for a variety of other applications and venues, as well, as shown in the following figure.

Venues for Using Email Encryption



Endpoint-to-Endpoint

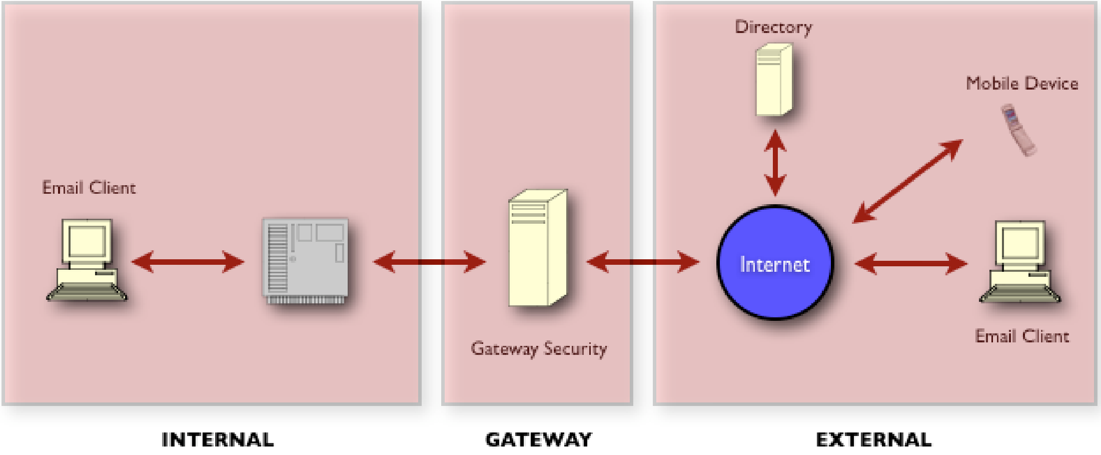
This mode:

- Represents full encryption from the originating device to the recipient device.
- Provides the highest level of security by allowing no intervening points at which plain text data can be read by anyone but the intended parties.

- Creates the greatest amount of complexity from an implementation, administration, and management perspective. This complexity results mainly from the fact that encryption software must be installed and maintained on the endpoint that integrates with the client email software.

Endpoint-to-endpoint encryption definitely has its place in the enterprise. Endpoint-to-endpoint encryption should be considered in high-risk situations requiring the greatest security, such as protecting the organization's most valuable data traveling through email. It would also apply to situations where there is a relatively high probability that the endpoint could be compromised, such as mobile devices that are often outside standard corporate security systems and may be easily lost or stolen.

Endpoint-to-Endpoint Encryption



Although endpoint-to-endpoint encryption is relatively more complex than other options, not all endpoint solutions are alike. The following options can decrease endpoint complexity:

- **User transparency**
  Endpoint encryption typically requires the user to install email "plug-in" software that requires the user to take additional steps to configure options and send email. An option that provides simplified management is an "encryption redirector," a software module that lacks a user interface and intercepts messages at the transport layer to perform the necessary encryption and decryption functions.

- **Server-managed keys**
  Endpoint encryption typically mandates that users be responsible for key management as well as maintenance of a local store of keys of their intended recipients. If an encryption gateway will be in place for other modes of

encryption, it may be possible for endpoint clients to leverage it for their key management.

- **Centrally managed policy**
  An important functional requirement for endpoint encryption is that it integrates with a centralized server or encryption gateway to enforce corporate security policy consistently and continuously.

Gateway-to-Endpoint

This mode:

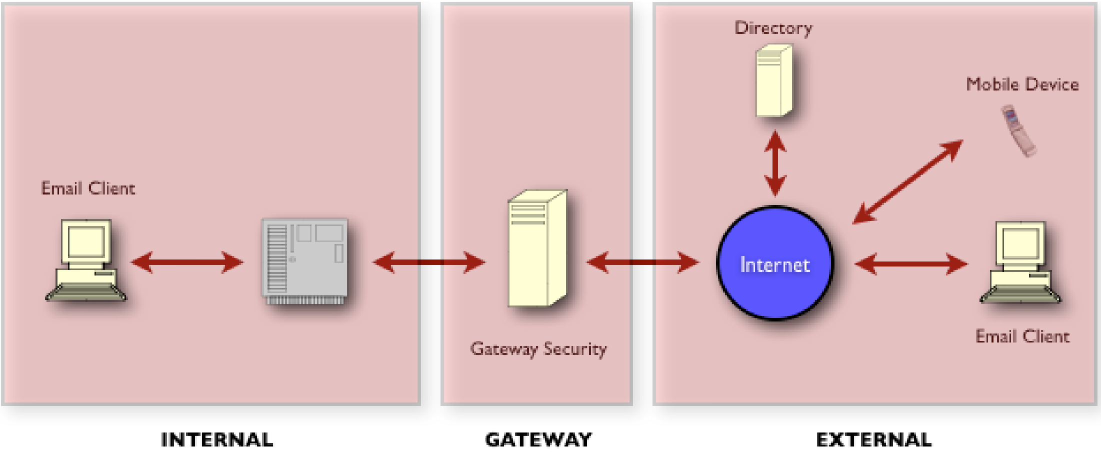
- Provides full encryption from a gateway system within the sender's network to the recipient's endpoint. In this scenario, the message leaves the sender's desktop in plaintext and is encrypted by a gateway solution located near the email server.

- Eliminates the need for any encryption software or user action on the sender's side.

- Provides significant cost savings by reducing user training and IT desktop administration costs and potentially reducing licensing costs by eliminating the need for desktop software.

Because email messages stored locally on individual systems are maintained in an unencrypted local cache, it is important to use full disk encryption to secure locally stored data. Although this is a standards-based (OpenPGP and S/MIME) approach, it requires the recipient to have a client installed on their local machine.

Gateway-to-Endpoint Encryption



Although the reduced complexity and costs of gateway-to-endpoint encryption can be advantageous, organizations should understand the risks associated with this approach to ensure it is the appropriate method for a given scenario. In particular:

- They need to understand the existing security controls on the path from the sender's desktop to the encryption gateway where the message is unencrypted. As the concept of the "disappearing perimeter" (also called "de-perimeterization") pervades more corporate networks, some organizations may find the fact that unauthorized parties will view messages during the "sender-to-gateway" segment an unacceptable risk.

- They need to evaluate the relative sensitivity of the data in the message flow according to accepted data classification standards.

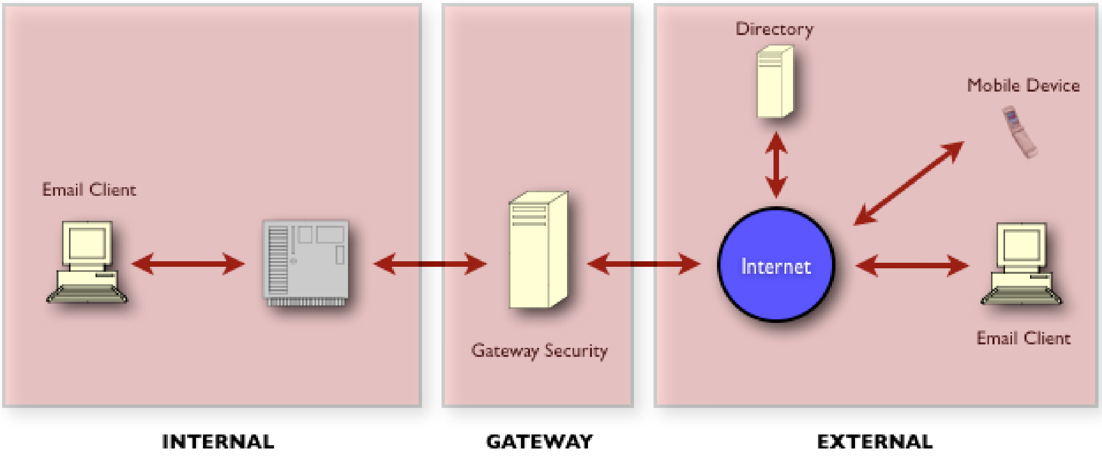
Even with these caveats, the complexity-security tradeoff of gateway-to-endpoint mode is generally sufficient to allow encryption initiated at the gateway to be the most common encryption mode in today's organizations.

An important design point for gateway-initiated encryption is authentication and non-repudiation. Unfortunately, some gateway-based solutions do not support individual keypairs to provide assurance that the message not only came from Company A, but that it also came from Individual X within Company A. Instead, messages from all individuals are signed with the same company key. This is rarely an acceptable practice, and regulations increasingly mandate a combination of individual and corporate responsibility and liability.

Gateway-to-Gateway

This mode is similar to the previous gateway-to-endpoint mode, but also adds an encryption gateway on the recipient's side, eliminating desktop software and administrative costs on that end as well. Dictating the recipient-side architecture is not always possible, however, although it is often desirable. Depending on the relationship an organization has with recipient domains, it may play an active role in extending its encryption architecture to its partners' organizations.

Gateway-to-Gateway Encryption



Comparing gateway-to-gateway and gateway-to-endpoint encryption modes provides some interesting revelations. Gateway-to-endpoint mode appears relatively more secure because it ensures only a small overall window of plaintext data transmission. If both communication partners have implemented encryption gateways, however, an organization has greater assurance that its sensitive data is still being actively protected by its partners' corporate security policies. For example, when the recipient of an encrypted message from the organization decides to forward it to a third party, his or her encryption gateway may force encryption or even bounce the message altogether. Sensitive data can exist within several dimensions and endure through multiple generations. Without taking an active role in its partners' encryption architecture, an organization cannot ensure ongoing security. In the big picture, the more encryption gateways that are implemented within an organization's ecosystem, the better its overall data security will be.

Gateway-to-Web

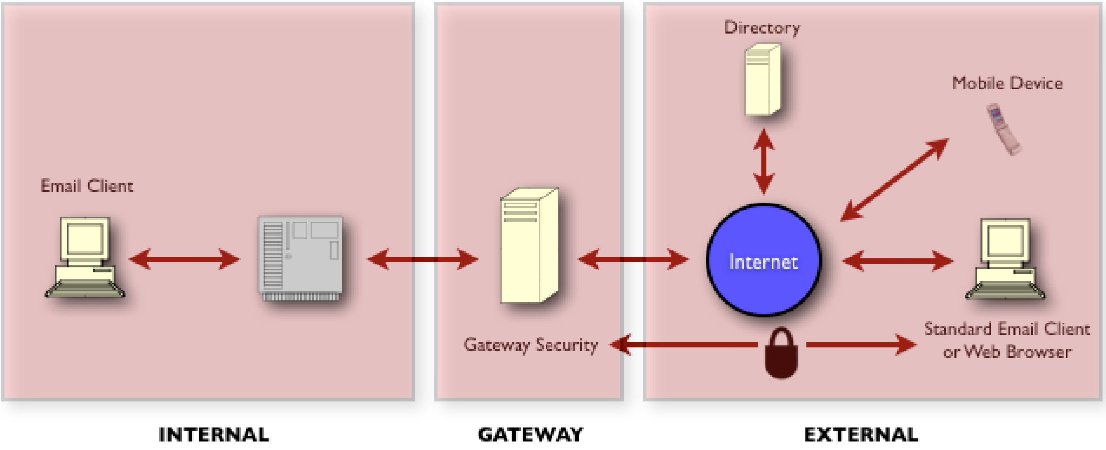
In this mode:

- The encryption gateway provides access to sensitive data via a Web server, possibly co-located on the gateway itself.

- The data is typically protected via transport layer encryption, such as Secure Sockets Layer (SSL), allowing secure communication to occur with any recipient, regardless of its architecture or level of sophistication.

- A standard message is sent to the recipient, advising that a secure message is waiting at the gateway. The recipient then retrieves this message via a secure connection, which may also require authentication with credentials delivered by an out-of-band mechanism.

Gateway-to-Web Encryption



Gateway-to-Web mode:

- Provides simple, broad-based encryption without needing to consider either the recipient's architecture or capabilities.

- Can be ideal for encrypting communications to a large number of recipients, particularly if they are unsophisticated consumers or small businesses. If the recipients know how to use a Web browser, they have all the skills needed to read the encrypted message.

- Provides the lowest level of security among all the modes.

- Requires minimal support resources from the sender's perspective.

This type of communication is often one-way encryption only, creating a risk that sensitive data will be subsequently transmitted in plaintext. However, some Gateway-to-Web solutions allow for encrypted replies, so it is important to select a solution that features a bidirectional, such as the Gateway-to-Recipient encryption capability discussed elsewhere in this report.

Gateway-to-Recipient

- Clientless email encryption is provided for secure email communications with large groups of customers and partners.

- This delivery mode ensures data is protected from unauthorized access in transit over the public Internet, at rest on a recipient's mail server, and at the endpoint by encrypting data down to the individual recipient.

- Secures email messages automatically as they leave the enterprise network according to highly configurable encryption rules, eliminating the need for client software or user intervention.

Key Management and Directories

Having a clear understanding of the issues surrounding key management and leveraging corporate directories is another critical success factor in an enterprise email encryption architecture. Because cost of ownership estimates are often incorrect by several orders of magnitude, this area is like an iceberg, with as much as 90% hidden from the analysis. To enable seamless encryption capabilities for any user, organizations must implement these critical strategies:

- **Automatic enrollment of users**
  An inordinate amount of IT cost is associated with account provisioning, authorization, and password resetting. Most organizations are unwilling to incur the additional administrative overhead needed to manually enroll users into an email encryption system. Not only is it an unacceptable cost, but it also creates a data integrity issue.

The cost of managing a traditional key infrastructure rises geometrically with the number of users because each addition, modification, and deletion of keypairs must be manually administered. It is imperative that corporate directories be leveraged for populating the keyserver(s) used by the email encryption system, including LDAP-based directories such as Microsoft Active Directory and Sun iPlanet.

- **Avoid client handling of certificates**
  Although certificates are an excellent tool to ensure the authenticity of the sender and allow for non-repudiation, they need to be automatically generated and managed for users. Requiring users to procure and implement their own certificates is not effective and leads to low encryption adoption rates.

- **Key freshness**
  Increasing the frequency with which keys are changed will decrease the risks if keys are compromised. An email encryption system should allow administrator-defined intervals for refreshing keys.

- **Archive integration**
  Archiving of messaging system content is becoming increasingly critical because of the recent amendments added to the Federal Rules of Civil Procedure and because courts and regulator are increasingly focused on messaging system content during e-discovery, regulatory audits, etc. As a result, the encryption capability chosen must be integrated with the archiving system so that encrypted content can be indexed and retrieved.

- **Additional Decryption Key (ADK)**
  In some instances, encryption can create a tension between security and reliability if the organization is unable to access the encrypted data because it lacks access to the decryption key. There are multiple strategies for mitigating this risk: the two most widely known are key backup and key escrow.

  - **Key backup**
    This term refers to an internal corporate system where backups of users' private keys are stored, allowing an authorized person to decrypt data belonging to a specific user. These systems are often necessary, but can be cumbersome to manage and keep up to date. In addition, allowing system administrators access to the keys needed to decrypt data they are not authorized to see creates a potentially risky situation and violates many corporate security policies.

  - **Key escrow**
    Similar in concept to key backup, key escrow permits an outside organization, often a government, to hold the backup keys. This approach may be problematic for organizations governed by multiple jurisdictions because different governments have widely different stances on this practice. Key escrow also potentially creates a problem with non-repudiation because of the inability to guarantee a message was created and sent by a unique entity if all the keys and passphrases reside with

a third party. An elegant solution to data access is the support of an Additional Decryption Key (ADK). The ADK can be used to decrypt data encrypted by any key within an organization without requiring users to surrender their private keys. The potential for abuse of the ADK is mitigated by the practice of key splitting (described below).

- **Key splitting**
  This approach refers to the practice of taking an important key such as an ADK and "splitting" it up among responsible parties so that no single person has access to the complete key and the data it protects. A typical example of key splitting is a 5 x 3 split, where a key is split into five separate shares, of which at least three must be combined to re-create the key needed to decrypt the data.

A Variety of Systems Require Encryption

Although a significant and growing proportion of email needs to be encrypted, there are a variety of other applications that require encryption today and will to an even greater extent during 2007 and 2008. As shown in the following table, file encryption, file transfer, and tape backup encryption are key areas that require encryption of data.

Various Types of Encryption Currently Used and Planned for Deployment 2007 and 2008

	% of Organizations	
Application/System	In use early 2007	Planned for deployment by mid-2008
File encryption	52%	53%
FTP/batch transfer encryption	48%	31%
Tape backup encryption	41%	29%
Server file encryption	38%	43%
Full disk encryption (laptop or desktop)	33%	49%
Removable storage (flash memory, USB flash drive, etc.)	33%	49%
Database encryption	31%	35%
Wireless/handheld device encryption (not including email encryption)	25%	33%
Mainframe file encryption	11%	23%

In reviewing the table above, it is important to note that the figures across a row cannot necessarily be added. For example, an organization may have already deployed file encryption for some users by early 2007, while the same organization may be planning an initiative for expanding this capability to additional users by mid-2008, placing them in both categories.

Mail Transport Agents (MTAs) in the Context of Managing Content and Data Leakage Protection (DLP)

Performing virus detection and content filtering in a gateway is a popular security measure because it provides a centralized "choke point" for incident response and threat mitigation. However, most enterprise email encryption architectures and the technologies they rely upon integrate poorly with back-end messaging systems. Because the MTA will usually reside in the middle of an encrypted "conversation," the message is opaque and is ignored by the gateway-based security systems. Some solutions attempt to solve this problem by forcing virus scanning and content filtering to occur at the encryption gateway. This approach may be adequate in some situations; however, it can also be problematic for a variety of reasons:

- **Policy violations**
  Forcing encryption to be initiated at the gateway may run counter to the desired encryption mode, creating a corporate policy violation. For example, security policy may dictate that highly sensitive documents should be encrypted endpoint-to-endpoint; however, to both encrypt and perform virus scanning on the document, the sender must use gateway-based encryption. This choice could leave copies of the highly sensitive document in plaintext on local desktops and within the email server, available to be "sniffed" through a wireless connection.

  Related to this is the fact that organizations are becoming increasingly cognizant of the need to scan outbound content for violations of corporate policy or statutes. For example, outbound messages should be scanned for sensitive or confidential content, credit card numbers, Social Security numbers and other content that either should not be sent externally, to certain parties or domains, or that should be encrypted prior to leaving the organization. Scanning for these potential violations must be designed into the system architecture in order to ensure that messages that contain policy and legal violations do not exit the organization.

- **Replace best-of-breed security tools**
  An organization may have invested significant capital and expertise in specific best-of-breed virus software and content scanners with unique feature sets. Being forced to forego these tools and use the encryption gateway's tools instead may weaken the organization's security posture and nullify its investment.

- **Additional point of failure**
  All-in-one encryption gateways must reside within the mail stream, creating an additional point of failure for all email and a potentially unacceptable risk for the organization's most critical communications system.

A more flexible approach is to select a gateway-based encryption solution that integrates with the MTA and its policy-based routing system. This approach allows the organization to place the encryption gateway outside the mail stream, letting the MTA selectively route messages requiring encryption/decryption to the gateway for on-demand servicing.

A key functional requirement for MTA integration is that the encryption gateway not "break" the sender's digital signature. Authentication and non-repudiation may be important business requirements for the messaging system. These specifications are particularly critical for instances of endpoint-to-endpoint encryption – where the encryption gateway is positioned in the middle of the encrypted flow – and mandate integration with the endpoint components.

Email encryption must be a component of an organization-wide encryption capability, rather than a standalone service that operates independently of other organizational encryption requirements. Organizations should implement a layered approach to encryption that will enforce corporate policies and permit a phased approach to rolling out new capabilities as policies, legal requirements and statutory obligations evolve over time.

Policy Management

Most organizations have an existing policy that spells out appropriate email usage. The email encryption solution an organization selects should reinforce the policies it wants to carry out and should not drive policy based on its technological limitations. The following characteristics should be included in an enterprise email encryption policy:

- **Bi-directional enforcement**
  The policy management capabilities of the email encryption system should help reinforce two-way encryption. A common risk is the plaintext reply to an encrypted message. The chosen system should provide multiple ways for recipients to retrieve and reply securely.

- **External partners**
  In some cases, it is crucial to extend the organization's encryption policy to communication partners. For example, the organization may need to outsource business functions that require handling sensitive data. The ability to enforce policy wherever the data travels is the vision behind Digital Rights Management (DRM). Unfortunately, DRM requires wholesale infrastructure changes plus modifications to both the data and the applications to make them "policy aware."

- **Granularity**
  A policy management system should allow flexibility and avoid a one-size-fits-all approach. Each recipient domain may represent a different external entity and should have the ability to create its own policy. However, achieving the most granular encryption policy often requires the MTA integration described previously or a solution that provides content-driven email policy enforcement. Only by combining the "what" (what type of content is being sent) with the "who" (who is sending and receiving this email) can the organization be certain to identify sensitive data transfers and customize encryption policy for them.

Implementation Tools

Many software solutions that are elegantly designed to solve business problems are in reality too cumbersome to deploy. The email encryption solution should take into account enterprise requirements for software implementation tools and support common IT processes for deploying and managing desktop PCs. This requirement becomes particularly critical when dealing with extranet configurations where IT organizations must support external PCs with a specific application.

What follows are minimal criteria for any software application and, in particular, for an enterprise encryption solution:

Compatibility with "Gold Code Images"

For many years, manufacturers have shipped PCs with preinstalled operating systems and productivity applications. Although this practice is helpful and universally adopted by consumers, organizations typically replace this preinstalled software with their own. A "Gold Code Image" is an organization-centric picture of what a desktop PC should look like, with specific versions of operating systems, patches, off-the-shelf applications, custom-developed software, and configuration settings. The master image is created on a reference PC, and then subjected to intensive regression testing before being duplicated for use in building new PCs for the organization. Some applications have trouble working seamlessly with the imaging process due to a number of factors, including installed file and registry locations, copy-protection schemes, and licensing controls. When choosing an encryption solution, it is important for organizations to vet the software's compatibility with disk imaging and validate compatibility with commonly used disk imaging applications.

Software Distribution Tool Support

Although imaging is popular for rolling out new PCs, enterprises typically use incremental means for deploying software to existing PCs. IT departments have developed mature systems for distributing software to provide automated, silent installs requiring little to no user interaction. If they lack a commercial software distribution system, many IT departments build deployment tools that leverage logon scripts to install software. In either case, IT should ensure encryption software has a silent install capability and supports Windows Installer .MSI packages so they can drop preconfigured packages into their deployment system. These packages should have all client-side policy and system configuration options preset, thereby eliminating the need for additional post-installation configuration.

Extranet Portal Support

Supporting external clients is among the most troublesome issues for IT in part because this group may lack the ability to control an external organization's desktop standards. In cases where external support is a business requirement, organizations need a zero-configuration, invisible client. They also need the ability to configure a self-service portal that allows external users to download the client software and easily find answers to common questions.

Reporting

Historically, email systems provided logging of sent and received email, with little additional information from add-on email encryption or anti-virus programs included in the log files. However, this situation resulted in problems when executing capacity planning, policy planning, and enforcement as well as other business requirements for third-party security software implemented with respect to email systems. The majority of client-side email encryption programs provide no or minimal logging, often leaving administrators with no idea how much (or how little) email is being encrypted by end users. In addition, the majority of email servers are not sufficiently "content aware" to know if a message is encrypted, let alone encrypted properly.

Capacity Planning

One critical aspect of deploying any encryption solution is capacity planning. Encryption and decryption are often very CPU-intensive tasks. If an organization uses server-based encryption and decryption, this load can multiply. For example, 100 users sending and receiving 50 emails per day represents 5,000 decryption and encryption operations with the associated overhead of key retrieval, key management, and the like. Server-based encryption is often combined with content filtering, anti-virus scanning, and other CPU-intensive operation that further increase the load.

An enterprise email encryption system should support a passive mode that generates logs containing information on which messages would have been encrypted and decrypted if policies were enforced. This functionality then allows an organization to deploy additional servers, consider moving encryption from the server to client systems, modify policies to reduce load, or take other appropriate actions. Once the organization has completed any remediation, IT can examine the logs again to determine if the impact is positive or negative, and make adjustments as necessary.

Policy Planning and Management

Although partially covered in capacity planning, policy planning and management are critical ongoing elements of any large email encryption deployment. Changing requirements in data encryption may result in required policy changes. Without logging and reporting, however, it is difficult to know exactly what changes should be made, if any, and whether or not those changes have been effective in fulfilling the appropriate security policy.

Reporting Policy Enforcement

As mentioned previously, an enterprise email encryption system should enforce policies and fail in a safe manner, such as by bouncing an unencrypted message that should be encrypted. Administrators should be notified of these actions in some way, although sending a copy of every bounce likely will result in a flood of messages that are ignored. With the ability to log and report such policy violations, administrators can find out where the problems are, modify policies, implement additional user training and education, and take other actions, as needed. Logging and reporting also allows administrators to spot policy modifications that may have been made in error or otherwise be incorrect. For example, a sudden drop in encrypted email traffic to a given site may indicate email is being sent without first being encrypted. This reporting also allows organizations to provide evidence to regulatory bodies and partners that email encryption policies have been implemented and are being enforced.

Integration with Existing Logging and Management Tools

One problem of many third-party logging systems that are integrated with existing mail services is their incompatibility with other programs. Interoperability cannot be emphasized strongly enough: email encryption systems should support logging methods that are standards-based and widely used. The following are two popular standards-based methods for integrating email encryption systems with third-party logging systems:

- **Syslog**
  The first method is standard UNIX syslog logging capability. To simplify centralized logging, an email encryption system should support sending logs to a remote system running syslog. This option allows a site to easily centralize logging to standard UNIX servers with no additional software and to Windows systems with the addition of inexpensive, widely available syslog server software. With this capability, an email encryption solution can leverage existing log monitoring and analysis software with only minor additional configuration.

- **SNMP**
  The second method is via support for the standard SNMP, which allows SNMP systems such as HP OpenView or IBM Tivoli to remotely access and query an email encryption solution to gather information such as CPU usage, number of messages encrypted, and so on. As mentioned previously, this option allows a site with multiple servers to easily centralize reporting to UNIX servers and to Windows systems with the addition of widely available SNMP server software.

Planning for the Future

One of the most vexing information technology problems is the issue of obsolescence. In extremely long and complicated infrastructure projects, the technology solution can be outdated by the time it is implemented. IT planners are often wary of investing in solutions that seem destined to have a short lifespan. The issue of investment protection and planning for the future has three dimensions as it pertains to email encryption and this guide:

- The nature of email is changing with the advent of new devices, new regulations, and greater expectations for the service. Among these expectations are the need to certify the authenticity of the sender and preventing anyone but the intended recipient from opening the message.

- The Gateway-to-Recipient format mentioned earlier in this document uses an industry-standard and widely deployed document format that will ensure availability of the encryption solution indefinitely.

- Encryption is spreading to other applications beyond email, and there will be a need to leverage some components of email encryption for these new frontiers. Examples of other applications and devices requiring encryption include mobile laptops, mobile email, network storage, removable storage, and databases.

Mobile Laptops

Although email encryption mitigates the risk of information sent through email, implementing full disk encryption addresses the risks and consequences from loss or theft of a complete system. Therefore, full disk encryption plays a complementary role in the deployment and use of an enterprise email encryption system.

Integration of email encryption with complementary full disk encryption solutions for protecting all files, not just those stored within an email client, is an important step in mitigating the risk and consequences from theft or loss of a system. Full disk encryption not only locks down all user files, such as Microsoft Office documents, but also protects copies of data stored in temporary, swap, and hibernation files by transparently encrypting all files and data without requiring user involvement.

In addition to full disk encryption, the following file encryption technologies are also important to consider:

- **Volume encryption**
  When users share a single system, separating work and confidential information is important to protect individual privacy. Volume encryption allows a user to encrypt a portion of a disk drive for personal use, even if the drive is already protected with full disk encryption. This capability allows each user to work with his or her encrypted data separate from that of other users on the system.

- **Archive encryption**
  Users often share confidential or sensitive files and directories with others via email, writeable media such as CDs or DVDs, and removable storage such as USB flash drives. Because these files are frequently moved, copied, and shared again, the need for encryption is crucial to protecting unauthorized access. Encrypting these files and directories is easy using archive encryption. With archive encryption, files and directories are stored in a single encrypted file that may also be compressed.

Mobile Email Platforms

Today, most email encryption occurs between traditional PCs. However, email sent from non-PC devices, such as wireless handhelds is the fastest-growing segment for email clients. For example, a 2007 study by Osterman Research found that 12.6% of email users in 2007 are using a wireless handheld device to access work-related email, and this figure will increase to 20.3% of email users by 2008 and 29.4% by 2009.[5]

With their small profile and high mobility, these devices are a ready target for theft, loss, and compromise. Therefore, just as on notebook or desktop computers, wireless email

[5] *Messaging, Web and IM Security Market Trends, 2007-2010*; Osterman Research, Inc.

should be encrypted both in transit and when stored on the mobile device. If encrypted email is unreadable on a mobile device, the value of the system decreases significantly. Additionally, mobile device encryption should be managed using a single, enterprise-wide system. To protect its investment and ensure the availability of encrypted email on mobile devices, organizations should partner with a vendor with a proven track record and product roadmap that integrates email encryption into popular wireless handhelds.

Network Storage

The use of full disk encryption to secure all information on a system is an important step in protecting confidential and private data. Beyond email, full disk encryption is needed to protect duplicate data in temporary files, swap files, and hibernation files. To complement local full disk encryption, emerging applications such as network or shared storage encryption are becoming important. There has been a growing demand for shared storage encryption, where administrators can easily assign group rights to encrypt/decrypt data.

Removable Storage

Although convenient for end users, the proliferation of inexpensive small storage devices such as USB flash drives presents a significant risk to enterprises. Whether lost, stolen, or used without the knowledge of the owner, removable media can store large, frequently used files that may include customer data or proprietary information. An emerging trend in protecting removable storage is the use of full disk encryption.

Databases

The consensus of many security and governance experts is that several regulatory compliance issues can be remediated by database encryption. Requirements such as the need to notify individuals whose personal information is compromised in a data breach are the focus of California Senate Bill 1386 and similar laws in more than 30 states. Although this is an emerging area of research, it will undoubtedly become an important area of innovation.

Planning for the Future

The industry can make encryption solutions as "future proof" as possible by implementing an on-demand encryption service in the infrastructure for applications to use, as needed. This encryption service should:

- Function as the equivalent of a dial tone or "encryption tone."

- Contain application proxies and application programming interfaces (APIs) to connect the service to existing applications.

- Enable new uses and applications to highly leverage and be easily accommodated by the existing infrastructure with a modest investment in a new proxy, rather than duplicating the entire encryption architecture for each additional application.

The challenge for enterprise email encryption buyers is to select solutions that will support the growth and changes within the organization's email architecture and will also be leveraged by non-email applications that require encryption services. The optimal strategy is to select crypto technologies that are time-tested, robust, and designed to support layers of new integration with the latest in new technology.

Organizations need to consider a number of requirements when developing a comprehensive email encryption architecture. Encrypted email requires more rigorous requirements definition and architecting than many other IT initiatives and email security projects. For example, encrypted email standards must be adhered to internally *and* externally. Following is a list of general requirements:

- **The key management lifecycle**
  Simple and automatic key management is critical to the successful implementation of an email encryption system. Managing the keys required to encrypt data can be cumbersome, limiting deployment of encryption to a few individuals within the company, which can create additional risk. Most companies need scalable solutions that meet the needs of all employees as well as external business partners, vendors, and customers.

- **Integration with existing email systems**
  It is critical that the chosen architecture integrates with both the existing organization's and partners' email systems. Solutions based on open standards for public key formats and nonproprietary technologies will ensure the widest compatibility among deployments. Products based on plug-in architectures are usually designed for purposes other than security, require significantly more user training, lack support, and change frequently, making interoperability problematic.

- **Flexibility of security policies**
  In most organizations, granular policy options are a high priority to help meet the needs of critical users who determine when and how to apply security policy to email as well as users who may not understand encryption or know how to apply it. In any given organization, when to secure outgoing email may be a corporate decision, a user decision, or a mixture of both. At the same time, organizations also need two-way policy enforcement so outgoing messages sent securely are returned encrypted and not "in the clear." In addition, a system needs to be flexible enough to accommodate users accessing email from multiple access points, including wireless handhelds.

- **Compatibility with other encryption systems**
  If encryption is used in other areas of the organization's business, such as full disk encryption for laptop and desktop computers, it is advantageous if the email encryption system is compatible with the other systems to avoid duplication of infrastructure.

- **Authentication and non-repudiation**
  Authentication is the process of verifying that the sender of an email is who he or she claims to be as well as that the email's contents have not been altered in transit.

Although encryption can be used to establish the identity of a sender, based on the sender's unique private key, authentication is not its main objective. Verifying the identity of the sender is usually accomplished via a digital signature.

- **Data recovery**
  Security regulations, such as Sarbanes-Oxley, increasingly require corporate access to encrypted data even if the key owner is unable or unwilling to provide the private key. Organizations should consider only encryption solutions that offer advanced key features such as Additional Decryption Key (ADK), key reconstruction, and key splitting that ensure policy-defined access to proprietary corporate information.

- **Compatibility with standard encryption algorithms**
  Choosing products based on current industry standards ensures interoperability with other products based on the same standards, maximizes investments in existing infrastructure technologies and products, and provides the highest level of security.

- **Support for virus-scanning, spam, and content-filtering**
  "Email hygiene" includes all the activities required to keep an organization's email system highly available and clean: virus, spam, and content blocking, plus securing email through encryption and digital signatures. These technologies must interoperate seamlessly to address potential threats to email system stability, security, and productivity.

- **Choosing between client-based and server-based solutions**
  Organizations must make a fundamental choice between relying on the end user to employ a desktop (or client-based) solution versus installing a server-based solution that eliminates dependence on the user to remember and follow security policy. This decision should be based on the cost, complexity, risk factors, and relative strengths of each security solution. Some organizations allow a combination of both approaches within specific parameters.

Chapter 5

Selecting an Enterprise Email Encryption Solution

At the highest level, the goal for any organization is to be able to cost-effectively acquire software based on the requirements outlined above with assurance that both the software and its provider will grow with the company and provide many years of uninterrupted support. This is a crucial part of the process, but organizations often focus on near-term negotiations and getting the best price while ignoring more troubling issues with their vendor of choice. The most successful enterprises go well beyond the standard of calling two client references and become intimately familiar with their prospective partners. Following are some criteria by which to evaluate potential encryption partners:

Company Viability

One of the best ways for an organization to get the enterprise email encryption solution its email security architects specified is to think like an investor. The organization's success is inextricably tied to its partner's success, and "due diligence" is the term investors use for the research that must be done to predict this success. After doing the appropriate research, decision-makers should ask, "Would I invest in this company?" If the answer is no, then why should an organization invest the security of its communications and computing infrastructure in that company by becoming a customer?

Management Team

Many investors make vetting the management team their highest priority before investigating other aspects of the company, looking for evidence of experience and past successes. Organizations should also look for a complete management team, with sales, services, marketing, product development, and technology vision all represented in top-level positions.

Financials

Traditionally, one of the more difficult areas about which to get accurate information is the financial condition of the company producing the products the organizations is interested in purchasing. In many cases, the company may be privately held and not required to release financial records publicly. Even in the case of publicly traded companies, it can often be a challenge to identify the financial contribution coming from encryption products if it comprises only a portion of overall company revenue. However, one clear consequence of the recent corporate accounting scandals is a greater predisposition toward transparency in financial reporting. Sarbanes-Oxley (SOX) mandates this transparency for companies that are publicly traded in the United States. However, privately held organizations also are becoming SOX-compliant or closely emulating compliance because they aspire to become a publicly traded company or be acquired by one. Following are the main financial metrics to understand:

- **Revenue growth**
  Positive growth is a good indicator of company success. The growth figures should be broken down between the products or product families the organization is interested in purchasing, and product revenue should be differentiated from services revenue. Unless the company is focused on services as a core business, an overly large services revenue number can indicate that a significant amount of consulting is necessary to successfully implement its products.

- **Business scalability**
  It is important to understand whether or not the company's growth can be sustained. Many businesses that seem to be fast growers reach a point of crisis where they are unable to grow further or sustain current revenue levels due to a lack of business infrastructure. Organizations should scrutinize trends between quarterly and annual reports with the goal of ensuring that revenue growth rate exceeds expense growth rate.

- **Total customers and revenue per customer**
  Although this is not a scientific metric, it can be helpful to understand how many customers comprise the revenue numbers and some representative customer deal sizes. This information can help an organization understand if the size of the email encryption project on which it will embark is within a range the company has dealt with before and whether it is too big or too small for them.

Finding the financial information needed for organizations to make a comprehensive evaluation should not be overly burdensome. Different sources are available for different types of companies:

- **Public companies**
  For U.S.-based companies, the Form 10-K report is the official annual business and financial report filed with the Securities and Exchange Commission (SEC). The easiest place to find this report is typically on the company's website. The 10-Q is the quarterly report and Form 20-F is the financial report filed with the SEC by foreign-registered companies. Although a complete country-by-country listing of similar regulatory requirements is beyond the scope of this guide, most of this information is available online from resources such as the International Organization of Securities Commissions (http://www.iosco.org/).

- **Private companies**
  Although these companies lack the mandatory reporting requirements of public entities, organizations can typically get much of the same financial information by asking for it directly and making it part of the Request for Proposal (RFP) process. Some companies may be reluctant to share this information without a Non-Disclosure Agreement (NDA) in place, and organizations should consider executing an NDA with these companies, if possible. If a private company is reluctant to provide financial statements, this attitude should raise a red flag because the corporate governance transparency trend leaves few justifiable reasons to withhold this information.

Product Track Record

Cryptography is a discipline that requires a good deal of public scrutiny to develop reliable products. Desirable products are those that have had their core technology tested through more than 10 years of long-term use by a range of organizations, individuals, and cryptography experts; proven their effectiveness in real-world situations; and verified vendor claims regarding functionality. Published and peer-reviewed source code is another positive indicator of a vendor's seriousness in developing effective, robust encryption products.

Independent Product Reviews

Another important resource is independent product reviews from reputable and independent sources, such as industry trade publications. Those publications with a long track record and a reputation of providing thorough and unbiased reviews of leading products can be a useful resource in helping corporate decision-makers to understand the attributes on which they need to evaluate products, and can help in understanding which products should be placed on their 'A' list.

References

Historically, the philosophy of "security by obscurity" has reigned supreme, and organizations have been reluctant to disclose which security products they are using. The concept of transparency is beginning to take hold here as well, and organizations are becoming more willing to talk about what solutions they're using. Even so, the process of checking references is likely to be a sensitive but crucial part of due diligence. References are one of the best indicators of an organization's probability of success in implementing the vendor's enterprise email encryption solution. Following are some suggestions for collecting references:

- **Develop a relationship with the reference**
  The main goal is to get the truth out of the references provided. The references are likely to be loyal to the vendor and may even have been coached about what to say. Decision-makers will gather the best information by building rapport with the reference and creating mutual loyalty as users of a common product with similar objectives. If appropriate, offer the reference a reward for the time investment in being a reference. Find out how the organization can help the reference. Get a commitment to hold follow-on conversations. References can be valuable resources throughout a project.

- **Obtain compatible references**
  Be certain the reference(s) interviewed have enough points of similarity to be relevant to the organization's needs. These points include enterprise size, scope of project, same or similar industry, and similar email environments. Decision-makers will likely need to talk to multiple references to cover all these points.

- **Obtain as many references as possible**
  The more references an organization consults, the greater the chance of seeing common trends.

- **Use a formalized survey process**
  Most reference checking is done via phone conversations and note-taking. Ideally, decision-makers will be able to do site visits, but these are insufficient by themselves. Instead, augment the reference interview process with a formalized written survey that contains an objective rating system. No matter how well coached a reference is, when asked to fill out a form, the company will tend to have fewer biases than during a conversation.

- **Use multiple interviewers**
  Decision-makers should not discount the fact that they have biases as well and may be leaning toward a particular vendor for subjective reasons. Organizations should have several people checking references.

Company Vision and Product Roadmap

A good working definition of vision and product roadmap as it relates to information security is "understanding tomorrow's problems and working to solve them today." Because of the pace of technology change and the almost daily emergence of new information security threats, it is important for an organization's email encryption partner to have vision. The company should have thought about what the next few years will look like, how new security threats will impact enterprises, and how it can add the most value to an organization. The email encryption partner should also have documented plans for addressing these emerging problems and be well on its way toward solving them.

Vision: Comprehensive Encryption or Comprehensive Messaging Security?

The organization should consider whether it will ultimately seek to leverage this partner as a single resource for all aspects of messaging security or potentially to provide leadership in the application of encryption across the enterprise. A "comprehensive encryption" vision is important to pursue for the following reasons:

- **Different skill sets are required**
  Although all partners should take a comprehensive view of the business requirements of email and the potential security risks, solving each risk requires a different skill set. For example, anti-virus and anti-spam control focus on malicious code and pattern research, heuristics algorithms, and signature updates. Tracking new instances of malicious code "in the wild" and incorporating this knowledge into customer notifications and signature updates is an extremely resource-intensive process and likely to prove a huge distraction for a solution provider focused on providing best-in-class encryption products.

- **Mature security sectors**
  Anti-virus is a mature product sector and spam control will soon be mature as well. There is little to be gained by reinventing the wheel in these sectors with an all-in-one vendor.

- **Need for manageable encryption for multiple uses**
  Although email encryption is a high priority, organizations should not focus on it to the

exclusion of other current or anticipated encryption needs. With so many possible applications of encryption, an organization is likely to want interoperability among these applications so that a user will have a single keypair to encrypt and decrypt sensitive data with all devices, no matter which application is transporting the data. There are many emerging applications for encryption and it will be advantageous to leverage an enterprise architecture across all of them. Most important, the architecture needs to logically support expansion into new areas in keeping with the "encryption tone" concept mentioned earlier.

Licensing

The nature of how software should be licensed is undergoing a transformation that may be an important consideration. Although software traditionally has been offered via a perpetual license, many vendors now sell their software on a subscription basis, with licensees able to use the software during the timeframe specified in the subscription. The rise in Application Service Providers (ASPs) has led many to predict that the subscription model will ultimately prevail; however, this prospect may have budget ramifications as well as an impact on how an organization's accounting department usually depreciates software. Organizations should purchase encryption solutions from vendors that provide software using the licensing model that best fits their business model and accounting methods:

- Perpetual license with annual technical support
- Subscription license
- Hosted or managed offerings

Writing RFPs

RFPs often yield unacceptable results for both the customer and the vendor, creating project delays, cost overruns, and hard feelings. Not only is the RFP used to procure the product, it is a key document used by project management resources when implementing the solution. This guide can be used as a scoping document to assist organizations in defining all the technical and business categories they must consider before choosing an enterprise encryption solution. Other recommendations include the following:

- **Clearly state mandatory requirements**
  One of the biggest frustrations organizations have is wading through RFP responses that are clearly inappropriate, but are submitted by hopeful vendors in language that hides inadequacies. Requirements should be explicitly stated to avoid this problem.

- **Specify measurable requirements**
  Rather than ask for "strong encryption," specifically define what that concept means for the enterprise.

- **Obtain detailed pricing**
  RFP responses may not match the organization's budget or can vary widely in price. Obtaining detailed component and per-seat licensing can help an organization

calculate an acceptable alternative solution without going back and forth extensively with the vendor.

- **Be thorough**
  Ensure that every section of the RFP is covered:

  - RFP Planning and Schedule
  - Administrative Requirements
  - Documentation of Existing Enterprise Email Architecture
  - Technical Requirements of an Encryption Solution
  - Services Requirements
  - Project Management Requirements
  - Qualifications & References
  - Project Plan
  - Pricing
  - Appendices of Diagrams

- **Conduct market research**
  Know who the top encryption players are in advance, as well as typical costs, to avoid surprises and to narrow the respondent list.

- **Define the outcome desired**
  By clearly stating the desired results, an organization can create a better RFP and more accurately list the milestones. For example, should the encryption solution initially be implemented in "learn mode," then gateway encryption rolled out for all, followed by more granular policy options?

- **Solicit input among stakeholders**
  Make sure security assurance, email administration, desktop support, network operations, and other relevant groups are involved in reviewing the RFP before it goes out to vendors.

- **Create a positive environment**
  Build a rapport with respondents based on mutual respect. Engage with the vendor of choice with the intention of creating an ongoing relationship whereby the vendor provides continual planning assistance and advance notice of future developments and products while the organization informs the vendor as its needs change and influences the vendor's product-related and strategic decisions.

Product Roadmap

Product development plans are key intellectual assets of a software company and should be guarded more closely than its financials. As a potential enterprise customer, however, an organization needs to understand how the encryption vendor's corporate vision is translated into tangible product plans and discover if those plans are in alignment with its future needs.

Chapter 6

Buyer's Checklist

What follows is a checklist of issues and questions that organizational decision-makers should address as they consider deployment of encryption solutions:

❑ Does the chosen architecture of the solution integrate with both the existing organization's and partners' email systems?

❑ How flexible are the solution's security policies?

❑ Is the solution compatible with other encryption systems?

❑ Does the solution provide policy-defined access to encrypted data even if the key owner is unable or unwilling to provide the private key?

❑ Does the solution support a secure standard document delivery format, such as gateway-to-recipient mode?

❑ Does the solution support a Webmail-style secure inbox for messages received by external users?

❑ Is the solution compatible with standard encryption algorithms?

❑ Does the solution integrate with anti-virus, anti-spam, anti-spyware and content filtering systems that comprise "email hygiene"?

❑ Do you want to deploy encryption at the client or server or both, and will the solution support your combination requirements?

❑ Will the solution support different combinations for different users in the organization? For example, can you deploy desktop-to-desktop encryption for legal counsel and gateway-to-gateway encryption for marketing staff?

❑ How easy is key management to administer?

❑ How scalable is the key management system?

❑ How well will the solution support growth and changes within your organization's email architecture?

❑ How well can the solution be leveraged by non-email applications that require encryption services?

❑ Will the solution support mobile devices? If so, which platforms does it support?

❑ Will the solution support shared storage encryption so administrators can easily assign group rights to encrypt or decrypt data?

❑ Does the solution provide full disk encryption?

❑ Does the solution support encrypting removable storage devices, such as USB flash drives?

❑ Will the solution encrypt instant messaging (IM) traffic?

❑ Will the solution encrypt databases?

❑ Does the solution support industry-standard Internet and encryption protocols?

❑ Is the solution a symmetric or asymmetric key system? (See "Encryption Protocols and Key Selection" later in this guide for more about these options.)

❑ Which encryption modes does the solution support: endpoint-to-endpoint, gateway-to-endpoint, gateway-to-gateway, and/or gateway-to-Web?

❑ Will the solution support automatic enrollment of users?

❑ Will the solution support automatic generation and management of certificates instead of requiring users to obtain and implement their own certificates?

❑ How frequently can keys be changed?

❑ Can keys be shredded?

❑ How vulnerable is the solution to data loss if the decryption key is inaccessible?

❑ Can keys be split?

❑ How easily can the solution be deployed?

❑ What reporting capabilities does the solution provide?

❑ Does the solution support existing logging and management tools?

❑ Does the solution provide a passive mode that generates logs containing information on which messages would have been encrypted and decrypted if policies were enforced?

❑ How well does the solution support existing and anticipated corporate policies?

❑ How financially viable is the encryption solution vendor?

❑ What is the encryption solution vendor's roadmap?

❑ What independent tests have been performed on the vendor's products?

(This page intentionally left blank)

Appendix 1

Osterman Research-Recommended PGP Products

PGP Corporation's solutions address all of the encryption requirements discussed in this document. Here is an overview of PGP Corporation's variety of solutions focused on encryption:

Endpoint-to-Endpoint

- **PGP Desktop Email**
  PGP Desktop Email provides enterprises with an automatic, transparent encryption solution for securing internal and external confidential email communications. With PGP Desktop Email, organizations can minimize the risk of a data breach and comply with partner and regulatory mandates for information security and privacy.

Gateway-to-Endpoint, Gateway-to-Gateway

- **PGP Universal Gateway Email**
  PGP Universal Gateway Email provides centrally managed, standards-based email encryption to secure email communications with customers and partners. By encrypting data at the gateway, PGP Universal Gateway Email ensures data is protected from unauthorized access in transit over the public Internet and at rest on a recipient's mail server. With PGP Universal Gateway Email, organizations can minimize the risk of a data breach and comply with partner and regulatory mandates for information security and privacy.

  PGP Universal Gateway Email integrates multiple delivery methods into a single product.

  - **PDF Messenger**
    New functionality for delivering encrypted PDFs that can be opened using a standard PDF reader such as Adobe Acrobat Reader

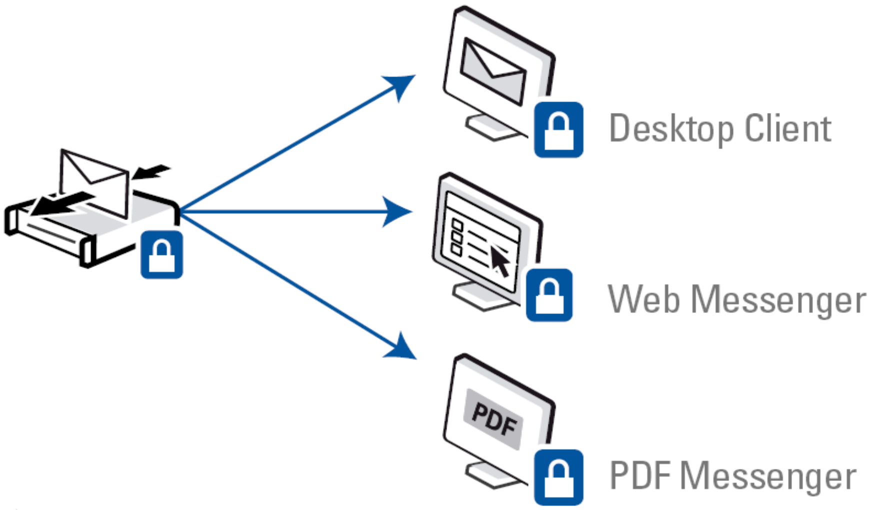
  - **Certified Delivery**
    Functionality that records or logs successful secure message delivery

  - **Web Messenger**
    A capability that enables message delivery through a Web email interface

Gateway-to-Web

- **PGP Universal Web Messenger** and **PDF Messenger** are features of PGP Universal Gateway Email that permits secure communications with external recipient who do not already have an email security solution. In cases where no recipient encryption key can be found, policy determines how to deliver a message securely using either PGP Universal Web Messenger or PDF Messenger. Using PGP Universal Web Messenger, PGP Universal Gateway Email retains the original secure message and sends an "in-the-clear" email message notifying the recipient that a secure message is available. The PGP Universal Web Messenger feature allows recipients to use their Web browser to create a secure SSL/TLS session and retrieve their message through a Webmail-like session served by PGP Universal Gateway Email.

Using PDF Messenger, PGP Universal Gateway Email delivers the messages as an encrypted PDF, as discussed above. The PDF Messenger feature allows recipients to use the existing Adobe Acrobat Reader client to decrypt and display the encrypted message.



Gateway-to-Recipient

- **PGP PDF Messenger**

  PGP PDF Messenger provides clientless email encryption for secure email communications with large groups of customers and partners. By encrypting data down to the individual recipient, PGP PDF Messenger ensures data is protected from unauthorized access in transit over the public Internet, at rest on a recipient's mail server, and at the endpoint. With PGP PDF Messenger, organizations can minimize the risk of a data breach and comply with partner and regulatory mandates for information security and privacy.

  PGP PDF Messenger secures email messages automatically as they leave the enterprise network according to highly configurable encryption rules, eliminating the need for client software or user intervention. Leveraging the broad adoption of PDF readers, PGP PDF Messenger enables enterprises to address regulatory requirements and data breach risks without requiring special software or using proprietary encrypted email attachments.

  PGP PDF Messenger is a PGP Encryption Platform–enabled application. The PGP Encryption Platform provides a strategic enterprise encryption framework for shared user management, policy, and provisioning, automated across multiple, integrated encryption applications. As a PGP Encryption Platform-enabled application, PGP PDF Messenger can be used with PGP Universal™ Server to manage existing policies, users, keys, and configurations, expediting deployment and policy enforcement. PGP PDF Messenger can also be used in combination with other PGP encryption applications to provide multiple layers of security.

Other Offerings

- **PGP Encryption Platform**
  The PGP Encryption Platform provides a strategic enterprise encryption framework for shared user and key management, policy, and provisioning automated across multiple, integrated encryption applications. Integrated PGP and third-party encryption applications enable organizations to deploy automated encryption as needed with the data security functions required to solve the business requirement. This data-centric approach protects data in motion and in transit anywhere, anytime.

- **PGP Universal Server**
  PGP Universal Server manages security policy across multiple applications to defend sensitive data and avoid the financial loss, legal ramifications, and brand damage resulting from a data breach. As the foundation of the PGP Encryption Platform architecture, PGP Universal Server manages PGP Encryption Platform–enabled applications that provide email, disk, and network file encryption. PGP Universal Server provides key management, policy enforcement, reporting and logging, and an extensible framework.

- **PGP Whole Disk Encryption**
  PGP Whole Disk Encryption provides enterprises with comprehensive, nonstop disk encryption, enabling quick, cost-effective protection for data on PCs, laptops, and removable media. The encrypted data is continuously safeguarded from unauthorized access, providing strong security for intellectual property, customer and partner data, and corporate brand equity.

- **PGP NetShare**
  PGP NetShare enables teams to securely share documents on file servers by automatically and transparently encrypting the files for fine-grained group access. This approach ensures that only authorized users can read or modify files, fulfilling partner and regulatory requirements for information partitioning and security.

- **PGP Command Line**
  PGP Command Line provides a new set of software tools for organizations that need to encrypt large amounts of batch information or secure backup processes. It enables users to insert PGP encryption and digital-signing functionality into existing automation scripts to ensure information is transmitted, stored, or backed up using strong PGP encryption.

- **PGP Support Package for BlackBerry**
  With PGP Support Package for BlackBerry, PGP-secured email messages are automatically encrypted, digitally signed, decrypted, and verified on BlackBerry devices. PGP Support Package for BlackBerry combines PGP email security with the

mobility and flexibility of BlackBerry devices and provides sender-to-recipient PGP security capabilities for wireless mobile users.

Appendix 2

Email Encryption Standards

- **S/MIME**
  Secure MIME (S/MIME) is a mature standard now in its third major revision and widely supported by virtually every mail client. The MIME standard was originally created to allow the conversion of various binary file formats such as image files to ASCII text suitable for inclusion with email messages. These attachments could then be handled automatically by email clients, allowing an email to contain an HTML-formatted page that includes images that are also sent as attachments with the email. S/MIME was designed so various portions of the encrypted message, such as the encrypted payload and the digital signature for that payload, could be sent as discrete items, allowing mail clients and the encryption program to parse the data more easily. For example, a gateway system can easily verify the signature of an X.509-signed message by calculating the data contained in the various S/MIME sections.

  With S/MIME, the certificate or encryption keys used to sign the data can be attached to an email message, making distribution of keys and certificates to first-time contacts much easier. S/MIME is covered by a variety of RFCs, including (but not limited to) RFC 2311, RFC 2312, RFC 2630, RFC 2631, RFC 2632, RFC 2633, RFC 2634, RFC 2785, RFC 2876, RFC 2984, RFC 3058, RFC 3114, RFC 3125, RFC 3126, RFC 3183, RFC 3185, RFC 3211, RFC 3217, RFC 3218, RFC 3274, RFC 3278, RFC 3369, RFC 3370, RFC 3394, RFC 3537, RFC 3560, RFC 3565, RFC 3657, RFC 3850, RFC 3851, RFC 3852, RFC 3854, RFC 3855, and RFC 4010.

Today, both S/MIME and OpenPGP enjoy widespread adoption within the industry. An apt analogy might be the two major graphics file formats supported by Web browsers. Both GIF and JPEG file types are widely used for varying reasons. A Web browser that excluded support for either of these graphics types would provide an insufficient Web surfing experience and, consequently, not become popularized. In the same way, designing an encryption architecture that excludes the use of either S/MIME or OpenPGP would prevent the solution from interoperating with a large number of existing encryption systems. This is a critical success factor in an enterprise encryption architecture: Without exception, it must support both OpenPGP and S/MIME.

- **OpenPGP**
  The OpenPGP standard is the reference for implementation of applications so that they can interoperate properly. The term "PGP" now refers to a specific company (PGP Corporation) and its implementation of the OpenPGP standard. OpenPGP is based primarily on the PGP 5.x release; however, going forward, OpenPGP allows extensions to be added. The OpenPGP standard covers four main areas:

  - Digital signatures
  - Encryption
  - Compression

- Radix-64 conversion

The first two items are self-explanatory. The third item, compression, allows for data to be compressed after signing but before encryption. Compression has the benefit of reducing message sizes and making certain types of cryptographic attacks harder; it is an optional component of OpenPGP. The fourth item, radix-64 conversion, is critical for transportation of encrypted OpenPGP messages via text-based protocols such as email using MIME. Radix-64 allows encrypted messages that are created by OpenPGP as arbitrary octets (8 bits) of data. These may appear as binary data to some systems and need to be converted to a 7-bit format (64-radix, also referred to as ASCII armored), which can easily be represented by standard ASCII text characters.

OpenPGP is supported by all PGP products, a number of other commercial products, and the Open Source implementation called GnuPGP (the program shipped by default with most Linux systems). OpenPGP has been officially recognized by the IETF and is detailed in RFC 2440.

- **PGP/MIME**
  The PGP/MIME standard is essentially an extension of the MIME standard. The PGP/MIME standard specifies three major additions to MIME:

  - application/pgp-encrypted
  - application/pgp-signature
  - application/pgp-keys

  These additions allow email clients and encryption programs to interact more easily with PGP-signed or encrypted email. For example, a gateway system can easily verify the signature of a PGP message by calculating the data contained in the MIME sections application/pgp-signature and application/pgp-encrypted. Additionally, key distribution is easier because keys can be attached to email and automatically identified and used by the remote client. PGP/MIME also allows data to be transferred using 8-bit encoding rather then 7-bit (radix-64, also referred to as "ASCII armored"), saving 12.5% of the message size (important when users encrypt and sent multi-megabyte files). PGP/MIME is widely supported by virtually all clients that also support MIME and S/MIME. PGP/MIME has been officially recognized by the IETF and is detailed in RFC 2015.

Encryption Protocols and Key Selection

When choosing an encryption scheme, organizations should first decide whether it should use a symmetric key or asymmetric key system. This critical decision must be made early because the capabilities inherent in each system will affect all other facets of the company's operations.

Symmetric Key Encryption

Until several decades ago, the only encryption systems available were based on symmetric keys:

- The simplest example of such a system is the Caesar cipher, where a string of text is taken and added to a repeating secret key, resulting in a new string of text. The cipher is named for Julius Caesar who replaced every A in messages to his generals with a D, every B with an E, and so on through the alphabet. Only someone who knew the "shift by 3" rule could decipher these messages.

- During World War II, the German Enigma machine used shared keys that were distributed among all parties and changed daily, which the Allies discovered using cryptanalysis on a regular basis.

- More recent symmetric key ciphers include the Data Encryption Standard (DES) and Advanced Encryption Standard (AES), which can use relatively long keys and are highly resistant to cryptoanalytical attacks. The main difficulty with these systems is that both ends communicating with a symmetric key encryption protocol must have a pre-shared secret key.

Symmetric key ciphers are used extensively and are ideal in connection-based situations where two systems connect and exchange data and then disconnect. Symmetric key ciphers also tend to be more efficient, requiring less processing power to encrypt and decrypt data. Today's powerful processors and encryption acceleration hardware makes this less of an issue, however. In most cases, a layer of asymmetric key encryption is often used on top of symmetric key encryption to provide a secure channel for the exchange of the symmetric encryption key.

Asymmetric Key Encryption

Asymmetric key encryption is based on a pair of encryption keys:

- **Public key**
  This key encrypts data and is distributed publicly.

- **Private key**
  This key decrypts the data and is kept secret by the owner of the keypair.

This process has several advantages:

- It allows anyone with the public key to encrypt data that only the holder of the private key can decrypt.

- It allows people with no preexisting connection or security arrangement to exchange messages securely.

Complementary to the encryption of data is the concept of "signing" of data, which communicates the fact that a unique entity has put its unique "stamp" on the data. The keypair is then used in the opposite manner from during encryption. In this scenario, the signing entity will take its private key to create a code unique to that private key and the contents of the data. This signature can be verified by anyone by using the signer's public key. The majority of asymmetric key encryption ciphers also support the signing of the public key by a trusted third party, testifying to its authenticity and to the data attached to the key, which often includes the owner's name, email address, and so on. This additional step allows keys to be distributed efficiently because the identity and authenticity of keys can easily be validated.

Critical Standards

Adherence to standards is not typically a difficult concept to sell to a CIO. Today's digital economy is able to function by leveraging several standard Internet protocols:

- HyperText Transfer Protocol (HTTP; Web browsing)
- Domain Name Service (DNS; domain names)
- Simple Mail Transport Protocol (SMTP; email)

All these protocols use the Transport Control Protocol/Internet Protocol (TCP/IP) as their transport protocol. It should come as no surprise that the foundation of an enterprise encryption solution is also adherence to standards. Choosing products based on current industry standards:

- Ensures interoperability with other products based on the same standards
- Maximizes investments in existing infrastructure technologies and products
- Provides the highest level of security

Most important, solutions that support the greatest number of standards provide the broadest reach in secure communications.

Encrypted email thrives when supporting several main de jure standards (those established as part of a formal standards certification process) as well as de facto standards (those that have become adopted by the majority of the market). Among the main de jure standards:

- OpenPGP
- S/MIME
- X.509
- SMTP
- FIPS 140-2
- IMAP
- POP
- LDAP
- Various PKI standards
- Cryptographic Token Interface (Cryptoki / PKCS #11), Department of Defense Common Access Card (DoD CAC), Homeland Security Presidential Directive 12 (HSPD-12)

Among the most important de facto standards:

- Microsoft's MAPI
- Lotus Notes
- Major handset operating systems

Because signatures create unique codes with respect to the data being signed, they are fundamental to the concept of non-repudiation. People need a method to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and the recipient cannot deny having received the message.

Key Management Issues

The primary issues with any encryption cipher or deployment are often administrative and relate to the amount of key management and administrative resources required to implement and support the chosen scheme. To ensure any form of encryption is done securely, the keys used to encrypt the data must be securely distributed to avoid the possibility of impersonation or "man-in-the-middle" attacks that might enable attackers to decrypt the data.

In symmetric key encryption systems, every party that wants to communicate securely with another party must have an encryption key. Thus, an office with 100 users wishing to communicate with each other would require 9,900 keypairs (100 x [100-1]), meaning that 9,900 symmetric keys would have to be created and distributed to the other party. As the number of users communicating increases, the number of keypairs grows. For 5,000 users, there would need to be 24,995,000 keypairs, and so on. Additionally, if a single user's system was compromised and the keys exposed, IT would need to create and distribute a new set of keys for that user and for everyone with whom the user communicates. IT would also need to coordinate with all external entities with which an organization wishes to communicate securely, creating even more scalability issues.

With asymmetric key encryption, every user creates a private and public keypair. Public keys typically are then signed by a trusted party and can be distributed over insecure channels such as a public Web server or email. This system requires two keys to be managed for each user:

- The private key is simply kept secret by the owner.

- The public key incurs some overhead in the signing process, after which the cost of distribution is minimal.

The asymmetric key encryption approach results in management of N*2 keys (where N is the number of users), a far more manageable situation than the N*(N-1) management required by symmetric key encryption.

THIS DOCUMENT IS PROVIDED "AS IS". ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.